Krishna B. Misra
Editor

Handbook of Performability Engineering

Springer

Handbook of Performability Engineering

Krishna B. Misra
Editor

Handbook of Performability Engineering

Springer

Professor Krishna B. Misra
Principal Consultant
RAMS Consultants
71 Vrindaban Vihar, Ajmer Road
Jaipur-302019 (Rajasthan)
India
kbmisra@gmail.com

ISBN 978-1-84800-130-5 e-ISBN 978-1-84800-131-2

DOI 10.1007/978-1-84800-131-2

British Library Cataloguing in Publication Data
The handbook of performability engineering
1. Reliability (Engineering)
I. Misra, Krishna B., 1943-
620'.0045
ISBN-13: 9781848001305

Library of Congress Control Number: 2008931851

© 2008 Springer-Verlag London Limited

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

The use of registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Cover design: eStudio Calamar S.L., Girona, Spain

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

This handbook is dedicated very fondly to
my grandson and to my lovely grandchildren
Meesha and Meera Trivedi,
Paridhi Misra,
Cyrus, Anushka and Xenia Chinoy,
and to their successive generations,
who will be the beneficiaries of the concepts
presented in this handbook
in sustaining humanity on this beautiful planet, Earth
and in preserving its environment for the future.

Foreword

The editor of the Handbook of Performability Engineering, Dr. Krishna B. Misra, a retired eminent professor of the Indian Institute of Technology, took to reliability nearly four decades ago and is a renowned scholar of reliability. Professor Misra was awarded a plaque by the IEEE Reliability Society in 1995 *"in recognition of his meritorious and outstanding contributions to reliability engineering and furthering of reliability engineering education and development in India"*. Upon his retirement in 2005 from IIT, Kharagpur, where he established the first ever postgraduate course on reliability engineering in India in 1982, and Reliability Engineering Centre in 1983, he launched the *International Journal of Performability Engineering* in 2005 and has since led the journal as its inaugural Editor-in-Chief.

Two years after successfully establishing the *International Journal of Performability Engineering,* Prof. Misra has now taken up the responsibility of editing the Handbook of Performability Engineering, which is being published by Springer. The timely publication of this handbook necessarily reflects the changing scenario of the 21st century's holistic view of designing, producing and using products, systems, or services which satisfy the performance requirements of a customer to the best possible extent.

The word "performability" was not commonly used or found in the reliability dictionary until its first use was made in 1978 by John Meyer in the context of performance (meaning reliability and maintainability) evaluation of aircraft control computers at NASA. However, Professor Misra has extended the use of word performability to reflect an amalgamation of reliability and other reliability-related performance attributes, such as quality, availability, maintainability, dependability, and sustainability. Therefore, performability can be considered as the best and most appropriate means to extend the meaning of effectiveness and overall performance of a modern complex and complicated system in which mechanical, electrical, and biological elements become increasingly harder to differentiate.

Having reviewed the contents of this voluminous handbook, and its contributed chapters, I find that it clearly covers the entire canvas of performability: quality, reliability, maintainability, safety, and sustainability. I understand that the motivation for this handbook came from the editorial that Dr. Misra wrote in the very first issue of the International Journal of Performability. The handbook addresses how today's systems need to be not only *dependable* (implying survivability and safety) but also *sustainable*. Modern systems need to be addressed in a practical way instead of simply as a mathematical abstract, often bearing no physical meaning at all. In fact, performability engineering not only aims at producing products, systems, and services that are dependable but also involves developing economically viable and safe processes of modern technologies, including clean production that entails minimal environmental pollution. Performability engineering extends the traditionally defined performance requirements to incorporate the modern notion of requiring optimal quantities of material and energy in order to yield safe

and reliable products that can be disposed of without causing any adverse effects on the environment at the end of their life cycle.

The chapters included in this handbook have undergone a thorough review and have been carefully devised. These chapters collectively address the issues related to performability engineering. I expect that the handbook will create an interest in performability and will bring about the intended interaction between various players of performability engineering.

I am glad to write the Foreword and firmly believe that this handbook will be widely used by practising engineers as well as serve as a guide to students and teachers with an interest in conducting research in the totality of performance requirements of the modern systems of practical use. I would like to congratulate Dr. Misra for taking the bold initiative of editing this historical volume.

July 24, 2007

Way Kuo
President of City University of Hong Kong
Editor-in-Chief, IEEE Transactions on Reliability

Prologue

Performability Engineering: Its Promise and Challenge

Performability engineering has as its scope the evaluation of all aspects of system performance. This encompasses the evaluation of the reliability of the system, its costs, its sustainability, its quality, its safety, its risk, and all of its performance outputs. In covering this broad scope, the objective is to provide a unified framework for comparing and integrating all aspects of system performance. This provides the manager and decision-maker with a complete, consistent picture of the system. This is the promise and exciting prospect of performability engineering.

The challenge involves unifying the diversity of the different disciplines that performability engineering covers. These disciplines cover reliability analysis, cost analysis, quality analysis, safety analysis, risk analysis, performance output analysis, not to mention data analysis, statistical analysis, and decision analysis. The challenge is to provide a unified framework for these different disciplines so that there is cohesiveness in the interfaces between the disciplines.

The first step in meeting this challenge is to provide a common portal through which workers in these diverse disciplines can contribute their ideas and work. This was implemented by the introduction of the International Journal of Performability Engineering, whose Editor-in-Chief is Professor Krishna B. Misra, who is also the inspiration and driver for the Handbook of Performability Engineering. This Handbook of Performability Engineering is another important step in addressing the challenge by presenting an integrated collection of chapters on the various disciplines and topics covered by performability engineering.

The chapters included in this handbook are diverse and represent the vitality of the different aspects of performability engineering. There are management-oriented chapters on the roles of reliability, safety, quality assurance, risk management, and performance management in the realm of performability management. There are chapters providing overview and the state-of-the-art on basic approaches being used in various disciplines. There are original technical contributions describing new methods and tools. Finally, there are chapters focusing on design and operational applications. The reader therefore has a veritable garden from which to feast from in impressive collection of chapters in the handbook.

In short, it is expected that this handbook will be found to be very useful by practicing engineers and researchers of the 21st century in pursuing this challenging and relevant area for sustainable development.

William Vesely, Ph.D.
Manager, Risk Assessment, Office of Safety and Mission Assurance
NASA Headquarters, 300 E Street SW,Washington, DC 20546

Preface

This handbook is unique in many respects. First of all, the title and the scope of subject matter is unique and is not to be found in a single volume in the existing literature. It is about a subject that is becoming very relevant and important in the 21st century. Secondly, the theme is unique and comprises a well-knitted theme of diverse yet related areas like quality, reliability, maintainability, safety, risk, environmental impacts, and sustainability. Thirdly, this handbook is about bringing together contributors of very diverse expertise, interests, and hail from different parts of the world to a common platform in executing a unifying and meaningful project. This initiative is expected to facilitate intense interaction between the experts from the diverse areas of performability engineering and break open the watertight compartments that exist today in an effort to present a holistic approach to performace assessment and design. It is also heartening to see that some of the contributors are founders of the areas that they represent. Therefore, the editor considers it a rewarding experience and a very encouraging step towards the realization of the objective for which this handbook is intended.

There are hundreds of books available on the subject of dependability and constituent areas such as quality, reliability, maintainability, safety, *etc.,* related to the performance of a product, system or a service. Dependability is primarily considered an aggregate of one or more of the attributes of survivability, like quality, reliability, maintainability, *etc*., and safety. However, these attributes are interrelated and reflect the level or grade of the product so designed and utilized, which is expressed through dependability. Nevertheless these attributes are very much influenced by the raw material, fabrication, technology, techniques, and manufacturing processes and their control, and also by the nature and the manner of usage. Currently, dependability and cost effectiveness are primarily seen as instruments for conducting international trade in the free market regime, thereby deciding the economic prosperity of a nation. This makes one realize that optimal design of a product, system, or service is one where one optimizes dependability with respect to costs incurred and sometimes with respect to other techno-economic constraints. This can at best be called partial optimization of the design of a product, system, or service. The material and energy requirements, waste generated, processes employed, and disposability are rarely considered for arriving at an optimal design or configuration of a product or a system.

With world resources declining, the cost of raw materials is likely to escalate spirally in the near future as mining becomes more and more costly and energy intensive due to grades of ore becoming poorer than before. To keep pace with the rising population, the increased volume of production is bound to affect the world environmental health further unless pollution prevention measures are vigorously pursued. At every stage of the life-cycle of a product, be it extraction of material, manufacturing, use, or disposal, energy and materials are required as inputs, and emissions (gaseous, solid effluents, or residues) are always associated with this, which influences the environmental health of our habitat. Therefore, the importance

of minimization of material and energy requirements along with the importance of control of effluents and waste management can hardly be emphasized enough while designing products and systems with acceptable levels of performance. Unless we consider all these factors together, we cannot call the design of products, systems, and services truly optimal from the engineering point of view.

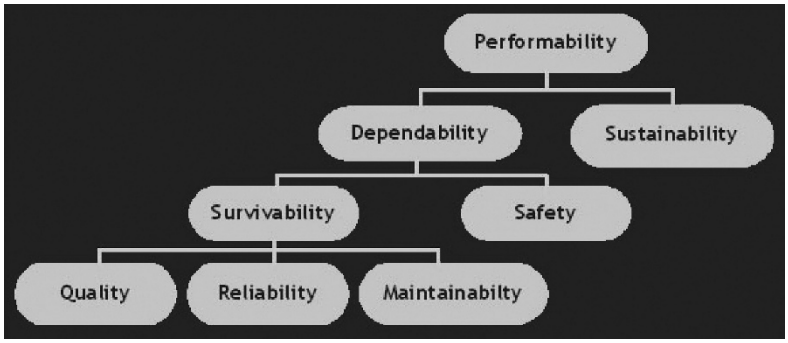
Certainly, these factors cannot be considered in isolation of each other. Therefore, emphasis has to be placed on a holistic view of the entire life cycle of activities of a product or system along with the associated cost of environmental preservation at each stage while maximizing the product performance. It must be emphasized here that to preserve our environment for our future generations, the internalization of the hidden costs of environment preservation will have to be accounted for, sooner or later, in order to be able to produce sustainable products in the long run. Open access resources can no longer be treated as freely available, unless we account for their restoration costs as well. In short, we can no longer rely solely on the criteria of dependability for optimizing the performance of a product, system, or service. We need to introduce and define a new performance criterion that will take a holistic view of the performance enhancement along with the associated environmental aspects.

Fortunately, we have the concept of sustainability that provides us with the framework to consider subjects like dematerialization, energy auditing, waste minimization, reuse and recycling, and other environmental considerations that can be of immense use in exploring means of clean production. The concepts of industrial ecology can be of great help in reducing the overall impact on the environment and to sustain development. Therefore, we have to explore ways of including dependability and sustainability in our criteria for the design of all future products, systems, and services, and to start with we need a term to represent all these activities.

In 1980, John Meyer introduced the term *performability* in the context of the performance evaluation of aircraft control computers for use by NASA. At the time this term was mainly used to reflect a composite attribute implying reliability and other associated attributes like availability, maintainability, *etc*., although dependability had been used at times to include a greater number of the attributes related to performance. Therefore, it was considered appropriate and logical to extend the meaning of this term to include attributes such as dependability and sustainability, rather than inventing a new term. Performability now would not only mean to include reliability, maintainability, or availability as was originally proposed, but also to include the whole gamut of attributes, like quality, reliability, maintainability, safety, and sustainability.

This handbook has been conceived to stimulate further thinking in this direction and to spur research and developmental effort in making sustainable products, systems, and services, which is the foremost need of the 21st century if humans are to survive and future generations are to have the same or better quality of life to prosper on this planet. The objective of this handbook is to introduce engineers, designers, producers, users, and researchers to visualize the interrelationships of all the performance attributes, to bring a synergetic interaction between various players of constituent areas of performability, and to exhort them to launch their activities in the direction of furthering performability engineering.

Today, there is hardly any book available on the market that deals with this subject in its entirety and provides a holistic perspective of the problem. Neither do the existing books on the subject of survivability and safety or dependability ever deliberate the issues related to sustainability. Nor do the books on the subject of sustainability and related areas touch upon problems of survivability and safety or dependability. For instance, while designing for survivability or dependability, internalization of environmental costs is not even mentioned, let alone considered. A truly optimal product design must balance out all the conflicting conditions imposed upon product development by the manufacturing processes. Obviously, the basic platform for addressing the inherently complex problems of this nature should emerge from the perspectives of performance, environment, and economics, as these products have to be produced in a competitive world market.



This handbook is primarily aimed at facilitating interactions and linkages between these diverse areas and helps promote the objective of designing, producing, operating, and using sustainable and dependable products, systems, and services.

Also with this handbook, a person intending to have introduction to performability engineering will not have to search extensively for relevant information to start his work. It is hoped that this handbook will offer a reader the necessary background in the subject just at one place. This is, therefore, the first book of its kind. It is also true that if we have to take to performability engineering as a profession, we need to create manpower in this discipline and introduce this subject for serious studies in the present day engineering curriculum. This handbook offers that opportunity to start with.

The handbook is organized in ten distinct sections as follows:

1. System design (7 chapters)
2. Engineering management (3 chapters)
3. Quality engineering and management (7 chapters)
4. Reliability engineering (18 chapters)
5. Reliability and risk methodology (4 chapters)
6. Risk management and safety (5 chapters)
7. Maintenance engineering and maintainability (5 chapters)
8. Sustainability and future technologies (9 chapters)
9. Performability applications (12 chapters)
10. Software engineering and applications (4 chapters)
11. Epilogue

The subject matter contained in the chapters has been selected to provide a balanced coverage of the entire spectrum of performability engineering. The chapters have been designed to provide up-to-date information on the subject being discussed. It is expected that this coverage will help achieve the objective for which this handbook is intended.

In spite of best efforts to make a cohesive presentation, there are bound to be lapses here and there in such a voluminous work; the editor takes the blame for all these shortcomings. However, if the handbook is able to create interest among the readers in performability engineering, it should be a matter of great achievement and pleasure to the editor. Eventually, it would prove to be a good idea that all engineers, irrespective of their areas of activity or discipline, are exposed to the subject of performability engineering to offer them with a wider vision of the requirement of sustainable and dependable products, systems, and services in the 21st century.

Krishna B. Misra

Acknowledgements

The editor would like to express his sincere thanks to all the contributors (99 in addition to the editor), who so generously and expeditiously came forward to share their ideas and work. I am deeply appreciative of their outstanding contributions, and it has been a tremendously satisfying experience to bring together such a large group of experts to produce a well-knitted theme consisting of diverse yet related areas in the form of the Handbook of Performability Engineering. The realization of this unique work of unprecedented scope and magnitude would have been impossible without the cooperation and counsel of many minds. The editor considers it his privilege to have worked with such a distinguished group of experts. The contributors, to whom the editor at times might have appeared to be unreasonable and more demanding but without which the handbook may not have seen the light of the day, deserve a great deal of appreciation.

In presenting the state-of-art, it is usually necessary to discuss and describe the work done by several authors and researchers and published in the literature. As it is not possible to list them all individually, the editor would like to record his appreciation and thanks *en bloc* to all those, whose works find a place of mention in this handbook.

The editor would like to thank Dr. Suprasad V. Amari of Relex Software Corporation, who incidentally has been the editor's student of reliability engineering, gave inputs at the several stages of conceiving the handbook, and also to Professor Hoang Pham of Rutgers University for encouraging and supporting the idea. My former student and colleague, Dr. Sanjay K. Chaturvedi, at the Reliability Engineering Centre, the Indian Institute of Technology, Kharagpur and postgraduate students, in particular, Mr. Rajshekhar Sankati and Mr. K. Kiran Pradeep deserve thanks for providing assistance whenever it was needed.

As in my past academic pursuits, my wife Veena has been a tremendous source of encouragement and strength. To her, I offer my deep gratitude and appreciation for her support in making this voluminous handbook a reality. Thanks are also due to my loving children, Vinita, Vivek, and Kavita, and to my daughter-in-law, Michelle, and sons-in-law, Rayomond Chinoy and Manoj Trivedi, who helped me on and off during the course of preparation of this handbook.

Finally, the editor would like to express his sincere thanks to Springer, UK and particularly to Dr. Anthony Doyle, Senior Editor in Engineering and to Mr. Simon Rees, Editorial Assistant in Engineering, who have been always prompt and courteous in responding to the several questions related to the production of this handbook. The production department of Springer and particularly Ms. Sorina Moosdorf deserve special mention in the production of the handbook and for the nice get up.

October 4, 2007 Krishna B. Misra

Contents

1 Performability Engineering: An Essential Concept in the 21st Century 1
Krishna B. Misra

1.1 Introduction 1
1.1.1 Fast Increasing Population 1
1.1.2 Limited World Resources 2
1.1.3 The Carrying Capacity of Earth 3
1.1.4 Environmental Consequences 3
1.2 Technology Can Help 4
1.3 Sustainability Principles 5
1.4 Sustainable Products and Systems 5
1.5 Economic and Performance Aspects 7
1.6 Futuristic System Designs 9
1.7 Performability 10
1.8 Performability Engineering 11
1.9 Conclusion 12
References 12

2 Engineering Design: A Systems Approach 13
Krishna B. Misra

2.1 Introduction 13
2.1.1 Analytic *Versus* Synthetic Thinking 14
2.2 The Concept of a System 14
2.2.1 Definition of a System 14
2.2.2 Classification of Systems 15
2.3 Characterization of a System 15
2.3.1 System Hierarchy 16
2.3.2 System Elements 16
2.3.3 System Inputs and Outputs 16
2.4 Design Characteristics 17

2.5 Engineering Design ... 18
2.5.1 Bottom-up Approach ... 18
2.5.2 Top-down Approach ... 18
2.5.3 Differences Between Two Approaches ... 19
2.6 The System Design Process ... 19
2.6.1 Main Steps of Design Process ... 20
2.6.2 Phases of System Design ... 21
2.6.3 Design Evaluation ... 22
2.6.4 Testing Designs ... 22
2.6.5 Final Design Documentation ... 23
2.7 User Interaction … ... 23
2.8 Conclusions ... 24
References ... 24

3 A Practitioner's View of Quality, Reliability and Safety ... 25
Patrick D.T. O'Connor

3.1 Introduction ... 25
3.1.1 The Costs of Quality, Reliability and Safety ... 25
3.1.2 Achievement Costs: "Optimum Quality" ... 26
3.1.3 Statistics and Engineering ... 28
3.1.4 Process Variation ... 29
3.2 Reliability ... 30
3.2.1 Quantifying Reliability ... 31
3.3 Testing ... 33
3.4 Safety ... 35
3.5 Quality, Reliability and Safety Standards ... 36
3.5.1 Quality ISO9000 ... 36
3.5.2 Reliability ... 38
3.5.3 Safety ... 38
3.6 Managing Quality, Reliability and Safety ... 39
3.6.1 Total Quality Management ... 39
3.6.2 "Six Sigma" ... 39
3.7 Conclusions ... 40
References ... 40

4 Product Design Optimization ... 41
Masataka Yoshimura

4.1 Introduction ... 41
4.2 Progressive Product Design Circumstances ... 42
4.3 Evaluative Criteria for Product Designs ... 43
4.3.1 Product Quality and Product Performance ... 43
4.3.2 Manufacturing Cost ... 44
4.3.3 Process Capability ... 44
4.3.4 Reliability and Safety ... 44
4.3.5 Natural Environment and Natural Resources ... 44
4.3.6 Mental Satisfaction Level ... 44
4.4 Fundamentals of Product Design Optimization ... 44

4.5 Strategies of Advanced Product Design Optimization 46
4.5.1 Significance of Concurrent Optimization 48
4.5.2 Fundamental Strategies of Design Optimization 49
4.6 Methodologies and Procedures for Product Design Optimization 50
4.7 Design Optimization for Creativity and Balance in Product Manufacturing 54
4.8 Conclusions 55
References 55

5 Constructing a Product Design for the Environmental Process 57
Daniel P. Fitzgerald, Jeffrey W. Herrmann, Peter A. Sandborn, Linda C. Schmidt and H. Gogoll Thornton

5.1 Introduction 57
5.2 A Decision-making View of Product Development Processes 58
5.2.1 Decision Production Systems 58
5.2.2 Improving Product Development Processes 59
5.3 Environmental Objectives 60
5.3.1 Practice Environmental Stewardship 60
5.3.2 Comply with Environmental Regulations 60
5.3.3 Address Customer Concerns 61
5.3.4 Mitigate Environmental Risks 61
5.3.5 Reduce Financial Liability 61
5.3.6 Reporting Environmental Performance 62
5.4 Product-level Environmental Metrics 62
5.4.1 Description of the Metrics 62
5.4.2 Scorecard Model 64
5.4.3 Guidelines and Checklist Document 64
5.5 The New DfE Process 65
5.5.1 Product Initiation Document 65
5.5.2 Conceptual Design Environmental Review 66
5.5.3 Detailed Design Environmental Review 66
5.5.4 Final Environmental Review 67
5.5.5 Post-launch Review 67
5.5.6 Feedback Loop 67
5.6 Analysis of the DfE Process 67
5.7 Conclusions 68
References 69

6 Dependability Considerations in the Design of a System 71
Krishna B. Misra

6.1 Introduction 71
6.2 Survivability 71
6.3 System Effectiveness 73
6.4 Attributes of System Effectiveness 74
6.4.1 Reliability and Mission Reliability 74
6.4.2 Operational Readiness and Availability 75
6.4.3 Design Adequacy 75
6.4.4 Reparability 75

6.4.5 Maintainability 75
6.4.6 Serviceability 75
6.4.7 Availability 76
6.4.8 Intrinsic Availability 76
6.4.9 Elements of Time 76
6.5 Life-cycle Costs (LCC) 77
6.6 System Worth 78
6.7 Safety 78
6.7.1 Plant Accidents 78
6.7.2 Design for Safety 80
References 80

7 Designing Engineering Systems for Sustainability 81
Peter Sandborn and Jessica Myers

7.1 Introduction 81
7.1.1 Sustainment-dominated Systems 82
7.1.2 Technology Sustainment Activities 84
7.2 Sparing and Availability 84
7.2.1 Item-level Sparing Analysis 84
7.2.2 Availability 87
7.2.3 System-level Sparing Analysis 88
7.2.4 Warranty Analysis 88
7.3 Technology Obsolescence 90
7.3.1 Electronic Part Obsolescence 91
7.3.2 Managing Electronic Part Obsolescence 91
7.3.3 Strategic Planning – Design Refresh Planning 93
7.3.4 Software Obsolescence 95
7.4 Technology Insertion 96
7.4.1 Technological Monitoring and Forecasting 96
7.4.2 Value Metrics and Viability 98
7.4.3 Roadmapping 100
7.5 Concluding Comments 101
References 101

8 The Management of Engineering 105
Patrick D.T. O'Connor

8.1 Introduction 105
8.1.1 Engineering is Different 106
8.1.2 Engineering in a Changing World 107
8.2 From Science to Engineering 107
8.2.1 Determinism 108
8.2.2 Variation 108
8.3 Engineering in Society 109
8.3.1 Education 109
8.3.2 "Green" Engineering 112
8.3.3 Safety 112
8.3.4 Business Trends 113

8.4 Conclusions 113
8.4.1 In Conclusion: Is Scientific Management Dead? 114
References 115

9 Engineering *Versus* Marketing: An Appraisal in a Global Economic Environment 117
Hwy-Chang Moon

9.1 Introduction 117
9.2 Creating Product Values with Low Cost and High Quality 118
9.2.1 "Consumer Tastes Are Becoming Homogenous" 119
9.2.2 "Consumers Are Willing to Sacrifice Personal Preference in Return for Lower Prices" 119
9.2.3 "Economies of Scale Are Significant with Standardization" 120
9.3 Strategic Implications of Global Standardization 120
9.4 The Dynamic Nature of the Global Strategy 121
9.5 A New Strategy for Dynamic Globalization 123
9.6 Conclusions 125
References 125

10 The Performance Economy: Business Models for the Functional Service Economy 127
Walter R. Stahel

10.1 Introduction 127
10.2 The Consequences of Traditional Linear Thought 129
10.3 Resource-use Policies Are Industrial Policies 129
10.4 The Problem of Oversupply 130
10.5 The Genesis of a Sustainable Cycle 132
10.6 The Factor Time – Creating Jobs at Home 133
10.7 Strategic and Organizational Changes 134
10.8 Obstacles, Opportunities, and Trends 136
10.9 New Metrics to Measure Success in the Performance Economy 136
10.10 Regionalization of the Economy 137
10.11 Conclusions 138
References 138

11 Cleaner Production and Industrial Ecology: A Dire Need for 21st Century Manufacturing 139
Leo Baas

11.1 Introduction 139
11.2 Different Levels of the Dissemination of Preventive Concepts 141
11.3 Practical Experiences and Types of Embeddedness 142
11.3.1 Cognitive Embeddedness 144
11.3.2 Cultural Embeddedness 145
11.3.3 Structural Embeddedness 145
11.3.4 Political Embeddedness 146
11.3.5 Spatial and Temporal Embeddedness 146
11.4 Industrial Ecology Programs in the Rotterdam Harbor Area 147
11.4.1 Phase I: The Development of Environmental Management Systems 147
11.4.2 Phase II: INES Project (1994–1997) 147

11.4.3 Phase III: INES-Mainport Project (1999–2002) 148
11.4.4 Phase IV: Inclusion in the Sustainable Rijnmond Program 149
11.5 Lessons Learned on the Introduction and Dissemination of Cleaner Production and Industrial Ecology 151
11.6 Conclusions and Recommendations 153
References 155

12 Quality Engineering and Management 157
Krishna B. Misra

12.1 Introduction 157
12.1.1 Definition 158
12.1.2 Quality and Reliability 159
12.2 Quality Control 159
12.2.1 Chronological Developments 160
12.2.2 Statistical Quality Control 161
12.2.3 Statistical Process Control 161
12.2.4 Engineering Process Control 162
12.2.5 Total Quality Control 162
12.3 Quality Planning 162
12.4 Quality Assurance 163
12.5 Quality Improvement 164
12.6 Quality Costs 164
12.7 Quality Management System 164
12.8 Total Quality Management 165
12.9 ISO Certification 166
12.10 Six Sigma 166
12.11 Product Life-cycle Management 168
12.12 Other Quality Related Initiatives 168
References 170

13 Quality Engineering: Control, Design and Optimization 171
Qianmei Feng and Kailash C. Kapur

13.1 Introduction 171
13.2 Quality and Quality Engineering 172
13.2.1 Quality 172
13.2.2 Quality Engineering 172
13.3 Quality Management Strategies and Programs 173
13.3.1 Principle-centred Quality Management 174
13.3.2 Quality Function Deployment 175
13.3.3 Six Sigma Process Improvement 176
13.3.4 Design for Six Sigma (DFSS) 177
13.4 Off-line Quality Engineering 177
13.4.1 Engineering Design Activities 177
13.4.2 Robust Design and Quality Engineering 178
13.5 On-line Quality Engineering 180
13.5.1 Acceptance Sampling and its Limitations 180
13.5.2 Inspection and Decisions on Optimum Specifications 181

13.5.3 Statistical Process Control 182
13.5.4 Process Adjustment with Feedback Control 183
13.6 Conclusions 183
References 184

14 Statistical Process Control 187
V.N.A. Naikan

14.1 Introduction 187
14.2 Control Charts 187
14.2.1 Causes of Process Variation 188
14.3 Control Charts for Variables 190
14.3.1 Control Charts for Mean and Range 190
14.3.2 Control Charts for Mean and Standard Deviation (*X, S*) 191
14.3.3 Control Charts for Single Units (X chart) 191
14.3.4 Cumulative Sum Control Chart (CUSUM) 192
14.3.5 Moving Average Control Charts 192
14.3.6 EWMA Control Charts 193
14.3.7 Trend Charts 193
14.3.8 Specification Limits on Control Charts 193
14.3.9 Multivariate Control Charts 193
14.4 Control Charts for Attributes 195
14.4.1 The *p* chart 195
14.4.2 The *np* chart 196
14.4.3 The *c* chart 196
14.4.4 The *u* chart 196
14.4.5 Control Chart for Demerits *per* Unit (*U* chart) 196
14.5 Engineering Process Control (EPC) 198
14.6 Process Capability Analysis 198
14.6.1 Process Capability Indices 198
References 199

15 Engineering Process Control: A Review 203
V.K. Butte and L.C. Tang

15.1 Introduction 203
15.1.1 Process Control in Product and Process Industries 203
15.1.2 The Need for Complementing EPC-SPC 204
15.1.3 Early Arguments Against Process Adjustments and Contradictions 205
15.2 Notation 206
15.3 Stochastic Models 206
15.3.1 Time Series Modeling for Process Disturbances 206
15.3.2 Stochastic Model Building 207
15.3.3 ARIMA (0 1 1): Integrated Moving Average 208
15.4 Optimal Feedback Controllers 209
15.4.1 Economic Aspects of EPC 211
15.4.2 Bounded Feedback Adjustment 212
15.4.3 Bounded Feedback Adjustment Short Production Runs 214
15.5 Setup Adjustment Problem 214

15.6 Run-to-run Process Control 215
15.6.1 EWMA Controllers 216
15.6.2 Double EWMA Controllers 217
15.6.3 Run-to-run Control for Short Production Runs 219
15.6.4 Related Research 219
15.7 SPC and EPC as Complementary Tools 219
References 221

16 Six Sigma: Status and Trends 225
U. Dinesh Kumar

16.1 Introduction 225
16.2 Management by Metrics 227
16.2.1 Yield 227
16.2.2 Defects *per* Million Opportunities (DPMO) 228
16.2.3 The Sigma Quality Level 228
16.3 Six Sigma Project Selection 228
16.4 DMAIC Methodology 229
16.4.1 DMAIC Case: Engineer Tank 230
16.5 Trends in Six Sigma 231
16.5.1 Design for Six Sigma 231
16.5.2 Lean Six Sigma 232
16.6 Conclusions 232
References 233

17 Computer Based Robust Engineering 235
Rajesh Jugulum and Jagmeet Singh

17.1 Introduction 235
17.1.1 Concepts of Robust Engineering 237
17.1.2 Simulation Based Experiments 238
17.2 Robust Software Testing 241
17.2.1 Introduction 241
17.2.2 Robust Engineering Methods for Software Testing 242
17.2.3 Case Study 243
References 244

18 Integrating a Continual Improvement Process with the Product Development Process 245
Vivek "Vic" Nanda

18.1 Introduction 245
18.2 Define a Quality Management System 245
18.2.1 Establish Management Commitment 245
18.2.2 Prepare a "Project" Plan 246
18.2.3 Define the Quality Policy 246
18.2.4 Establish a Process Baseline 246
18.2.5 Capture Process Assets 247
18.2.6 Establish a Metrics Program 247
18.2.7 Define the Continual Improvement Process 247
18.3 Deploy the Quality Management System 249

18.4 Continual Improvement 250
18.5 Conclusions 250
References 251

19 Reliability Engineering: A Perspective 253
Krishna B. Misra

19.1 Introduction 253
19.1.1 Definition 253
19.1.2 Some Hard Facts About Reliability 255
19.1.3 Strategy in Reliability Engineering 256
19.1.4 Failure-related Terminology 256
19.1.5 Genesis of Failures 258
19.1.6 Classification of Failures 260
19.2 Problems of Concern in Reliability Engineering 261
19.2.1 Reliability Is Built During the Design Phase 262
19.2.2 Failure Data 265
19.3 Reliability Prediction Methodology 266
19.3.1 Standards for Reliability Prediction 267
19.3.2 Prediction Procedures 271
19.3.3 Reliability Prediction for Mechanical and Structural Members 273
19.4 System Reliability Evaluation 274
19.4.1 Reliability Modeling 275
19.4.2 Structures of Modeling 276
19.4.3 Obtaining the Reliability Expression 277
19.4.4 Special Gadgets and Expert Systems 278
19.5 Alternative Approaches 279
19.6 Reliability Design Procedure 280
19.7 Reliability Testing 280
19.8 Reliability Growth 283
References 284

20 Tampered Failure Rate Load-sharing Systems: Status and Perspectives 291
Suprasad V. Amari, Krishna B. Misra, and Hoang Pham

20.1 Introduction 291
20.2 The Basics of Load-sharing Systems 293
20.2.1 The Load Pattern 293
20.2.2 The Load-sharing Rule 293
20.2.3 Load–Life Relationship 293
20.2.4 The Effects of Load History on Life 294
20.3 Load-sharing Models 295
20.3.1 Static Models 295
20.3.2 Time-dependent Models 296
20.3.3 Related Models 296
20.4 System Description 299
20.4.1 Load Distribution 299
20.4.2 The TFR Model 300
20.4.3 System Configuration 300

20.5 *k*-out-of-*n* Systems with Identical Components 300
20.5.1 Exponential Distribution 300
20.5.2 General Distribution 301
20.5.3 Examples 302
20.6 *k*-out-of-*n* Systems with Non-identical Components 303
20.6.1 Exponential Distributions 303
20.6.2 General Distributions 304
20.6.3 Further Examples 304
20.7 Conclusions 305
References 305

21 *O*(*kn*) Algorithms for Analyzing Repairable and Non-repairable k-out-of-n:G Systems 309
Suprasad V. Amari, Ming J. Zuo, and Glenn Dill

21.1 Introduction 309
21.2 Background 310
21.2.1 General Assumptions 310
21.2.2 Availability Measures 310
21.2.3 Motivation 311
21.3 Non-repairable *k*-out-of-*n* Systems 311
21.3.1 Identical Components 312
21.3.2 Non-identical Components 312
21.4 Repairable *k*-out-of-*n* Systems 314
21.4.1 Additional Assumptions 314
21.4.2 Identical Components 314
21.4.3 Non-identical Components 314
21.5 Some Special Cases 315
21.5.1 MTTF 315
21.5.2 MTTFF 316
21.5.3 Reliability with Repair 318
21.5.4 Suspended Animation 318
21.6 Conclusions and Future Work 319
References 319

22 Imperfect Coverage Models: Status and Trends 321
Suprasad V. Amari, Albert Myers, Antoine Rauzy, and Kishor Trivedi

22.1 Introduction 321
22.2 A Brief History of Solution Techniques 322
22.2.1 Early Combinatorial Approaches 323
22.2.2 State-Space Models 323
22.2.3 Behavioral Decomposition 323
22.2.4 The DDP Algorithm 323
22.2.5 Simple and Efficient Algorithm (SAE) 324
22.2.6 Multi-fault Models 324
22.3 Fault and Error Handling Models 324
22.4 Single-fault Models 327
22.4.1 Phase Type Discrete Time Models 327
22.4.2 General Discrete Time Models 327

22.4.3 The CAST Recovery Model 328
22.4.4 CTMC Models 328
22.4.5 The CARE III Basic Model 328
22.4.6 The CARE III Transient Fault Model 329
22.4.7 ARIES Models 329
22.4.8 HARP Models 329
22.5 Multi-fault Models 330
22.5.1 HARP Models 330
22.5.2 Exclusive Near-coincident Models 330
22.5.3 Extended Models 331
22.6 Markov Models for System Reliability 331
22.7 Combinatorial Method for System Reliability with Single-fault Models 333
22.7.1 Calculation of Component-state Probabilities 334
22.7.2 The DDP Algorithm 334
22.7.3 SEA 336
22.7.4 Some Generalizations 337
22.8 Combinatorial Method for System Reliability with Multi-fault Models 339
22.8.1 *k*-out-of-*n* Systems with Identical Components 340
22.8.2 *k*-out-of-*n* Systems with Non-identical Components 340
22.8.3 Modular Systems 341
22.8.4 General System Configurations 342
22.8.5 Some Generalizations 345
22.9 Optimal System Designs 345
22.10 Conclusions and Future Work 346
References 346

23 Reliability of Phased-mission Systems 349
Liudong Xing and Suprasad V. Amari

23.1 Introduction 349
23.2 Types of Phased-mission Systems 350
23.3 Analytical Modeling Techniques 351
23.3.1 Combinatorial Approaches 351
23.3.2 State Space Based Approaches 353
23.3.3 The Phase Modular Approach 355
23.4 BDD Based PMS Analysis 357
23.4.1 Traditional Phased-mission Systems 357
23.4.2 PMS with Imperfect Coverage 358
23.4.3 PMS with Modular Imperfect Coverage 362
23.4.4 PMS with Common-cause Failures 363
23.5 Conclusions 367
References 367

24 Reliability of Semi-Markov Systems in Discrete Time: Modeling and Estimation 369
Vlad Stefan Barbu and Nikolaos Limnios

24.1 Introduction 369
24.2 The Semi-Markov Setting 370
24.3 Reliability Modeling 373

24.3.1 State Space Split 373
24.3.2 Reliability 373
24.3.3 Availability 374
24.3.4 The Failure Rate 374
24.3.5 Mean Hitting Times 374
24.4 Reliability Estimation 375
24.4.1 Semi-Markov Estimation 375
24.4.2 Reliability Estimation 376
24.4.3 Availability Estimation 377
24.4.4 Failure Rate Estimation 377
24.4.5 Asymptotic Confidence Intervals 378
24.5 A Numerical Example 378
References 379

25 Binary Decision Diagrams for Reliability Studies 381
Antoine B. Rauzy

25.1 Introduction 381
25.2 Fault Trees, Event Trees and Binary Decision Diagrams 382
25.2.1 Fault Trees and Event Trees 382
25.2.2 Binary Decision Diagrams 383
25.2.3 Logical Operations 384
25.2.4 Variable Orderings and Complexity Issues 384
25.2.5 Zero-suppressed Binary Decision Diagrams 384
25.3 Minimal Cutsets 384
25.3.1 Preliminary Definitions 384
25.3.2 Prime Implicants 385
25.3.3 What Do Minimal Cutsets Characterize? 387
25.3.4 Decomposition Theorems 387
25.3.5 Cutoffs, p-BDD and Direct Computations 388
25.4 Probabilistic Assessments 388
25.4.1 Probability of Top (and Intermediate) Events 388
25.4.2 Importance Factors 389
25.4.3 Time Dependent Analyses 391
25.5 Assessment of Large Models 393
25.5.1 The MCS/ZBDD Approach 393
25.5.2 Heuristics and Strategies 394
25.6 Conclusions 394
References 395

26 Field Data Analysis for Repairable Systems: Status and Industry Trends 397
David Trindade and Swami Nathan

26.1 Introduction 397
26.2 Dangers of MTBF 398
26.2.1 The “Failure Rate” Confusion 399
26.3 Parametric Methods 401
26.4 Mean Cumulative Functions 402
26.4.1 Cumulative Plots 402

26.4.2 Mean Cumulative Function *Versus* Age 403
26.4.3 Identifying Anomalous Machines 404
26.4.4 Recurrence Rate *Versus* Age 404
26.5 Calendar Time Analysis 405
26.6 Failure Cause Plots 407
26.7 MCF Comparisons 408
26.7.1 Comparison by Location, Vintage or Application 408
26.7.2 Handling Left Censored Data 409
26.8 MCF Extensions 410
26.8.1 The Mean Cumulative Downtime Function 410
26.8.2 Mean Cumulative Cost Function 411
26.9 Conclusions 411
References 412

27 Reliability Degradation of Mechanical Components and Systems 413
Liyang Xie, and Zheng Wang

27.1 Introduction 413
27.2 Reliability Degradation Under Randomly Repeated Loading 414
27.2.1 The Conventional Component Reliability Model 414
27.2.2 The Equivalent Load and Its Probability Distribution 415
27.2.3 Time-dependent Reliability Model of Components 416
27.2.4 The System Reliability Model 420
27.2.5 The System Reliability Model Under Randomly Repeated Loads 420
27.2.6 The Time-dependent System Reliability Model 421
27.3 Residual Fatigue Life Distribution and Load Cycle-dependent Reliability Calculations 422
27.3.1 Experimental Investigation of Residual Fatigue Life 422
27.3.2 The Residual Life Distribution Model 424
27.3.3 Fatigue Failure Probability Under Variable Loading 426
27.4 Conclusions 427
References 428

28 New Models and Measures for Reliability of Multi-state Systems 431
Yung-Wen Liu, and Kailash C. Kapur

28.1 Introduction 431
28.2 Multi-state Reliability Models 432
28.2.1 Classification of States 432
28.2.2 Model Assumptions 433
28.3 Measures Based on the Cumulative Experience of the Customer 435
28.3.1 System Deterioration According to a Markov Process 436
28.3.2 System Deterioration According to a Non-homogeneous Markov Process 437
28.3.3 Dynamic Customer-center Reliability Measures for Multi-state Systems 439
28.4 Application of Multi-state Models 440
28.4.1 Infrastructure Applications – Multi-state Flow Network Reliability 441
28.4.2 Potential Application in Healthcare: Measure of Cancer Patient's Quality of Life 441
28.5 Conclusions 443
References 444

29 A Universal Generating Function in the Analysis of Multi-state Systems 447
Gregory Levitin

29.1 Introduction 447
29.2 The RBD Method for MSS 448
29.2.1 A Generic Model of Multi-state Systems 448
29.2.2 Universal Generating Function (*u*-function) Technique 449
29.2.3 Generalized RBD Method for Series-parallel MSS 450
29.3 Combination of Random Processes Methods and the UGF Technique 453
29.4 Combined Markov-UGF Technique for Analysis of Safety-critical Systems 458
29.4.1 Model of System Element 459
29.4.2 State Distribution of the Entire System 461
29.5 Conclusions 462
References 463

30 New Approaches for Reliability Design in Multistate Systems 465
Jose Emmanuel Ramirez-Marquez

30.1 Introduction 465
30.1.1 Binary RAP 465
30.1.2 Multistate RAP 466
30.1.3 Notation 467
30.1.4 Acronyms 468
30.1.5 Assumptions 468
30.2 General Series-parallel Reliability Computation 468
30.3 Algorithm for the Solution of Series-parallel RAP 468
30.4 Experimental Results 470
30.4.1 Binary System 470
30.4.2 Multistate System with Binary Capacitated Components 472
30.4.3 Multistate System with Multistate Components 473
References 475

31 New Approaches to System Analysis and Design: A Review 477
Hong-Zhong Huang and Liping He

31.1 Introduction 477
31.1.1 Definitions and Classifications of Uncertainty 478
31.1.2 Theories and Measures of Uncertainty 478
31.1.3 Uncertainty Encountered in Design 480
31.2 General Topics of Applications of Possibility Theory and Evidence Theory 480
31.2.1 Basic of Possibility Theory and Evidence Theory 480
31.2.2 Introduction to General Applications 481
31.3 Theoretical Developments in the Area of Reliability 481
31.3.1 Fuzzy Reliability 481
31.3.2 Imprecise Reliability 482
31.4 Computational Developments in the Reliability Area 484
31.4.1 Possibility-based Design Optimization (PBDO) 484
31.4.2 Evidence-based Design Optimization (EBDO) 486
31.4.3 Integration of Various Approaches to Design Optimization 487
31.4.4 Data Fusion Technology in Reliability Analysis 488

31.5 Performability Improvement on the Use of Possibility Theory and Evidence Theory 489
31.5.1 Quality and Reliability 490
31.5.2 Safety and Risk 492
31.5.3 Maintenance and Warranty 493
31.6 Developing Trends of Possibility and Evidence-based Methods 494
31.7 Conclusions 494
References 495

32 Optimal Reliability Design of a System 499
Bhupesh Lad, M.S. Kulkarni, and Krishna B. Misra

32.1 Introduction 499
32.2 Problem Description 501
32.3 Problem Formulation 503
32.3.1 Reliability Allocation Formulations 503
32.3.2 Redundancy Allocation Formulations 504
32.3.3 Reliability and Redundancy Allocation Formulations 504
32.3.4 Multi-objective Optimization Formulations 505
32.3.5 Problem Formulations for Multi-state Systems 505
32.3.6 Formulations for Repairable Systems 505
32.4 Solution Techniques 506
32.4.1 Exact Methods 507
32.4.2 Approximate Methods 509
32.4.3 Heuristics 510
32.4.4 Metaheuristics 511
32.4.5 Hybrid Heuristics 512
32.4.6 Multi-objective Optimization Techniques 513
32.5 Optimal Design for Repairable Systems 513
32.6 Conclusion 514
References 515

33 MIP: A Versatile Tool for Reliability Design of a System 521
S.K. Chaturvedi and Krishna B. Misra

33.1 Introduction 521
33.2 Redundancy Allocation Problem 522
33.2.1 An Overview 522
33.2.2 Redundancy Allocation Techniques: A Comparative Study 523
33.3 Algorithmic Steps to Solve Redundancy Allocation Problem 524
33.4 Applications of MIP to Various System Design Problems 525
33.4.1 Reliability Maximization Through Active Redundancy 525
33.4.2 System with Multiple Choices and Mixed Redundancies 527
33.4.3 Parametric Optimization 528
33.4.4 Optimal Design of Maintained Systems 528
33.4.5 Computer Communication Network Design with Linear/Nonlinear Constraints and Optimal Global Availability/Reliability 529
33.4.6 Multicriteria Redundancy Optimization 530
33.5 Conclusions 531
References 531

34 Reliability Demonstration in Product Validation Testing 533
Andre Kleyner

34.1 Introduction 533
34.2 Engineering Specifications Associated with Product Demonstration 533
34.3 Reliability Demonstration Techniques 535
34.3.1 Success Run Testing 535
34.3.2 Test to Failure 536
34.3.3 Chi-Squared Test Design – An Alternative Solution for Success Run Tests with Failures 538
34.4 Reducing the Cost of Reliability Demonstration 538
34.4.1 Validation Cost Model 538
34.4.2 Extended Life Testing 539
34.4.3 Other Validation Cost Reduction Techniques 540
34.5 Assumptions and Complexities of Reliability Demonstration 541
34.6 Conclusions 542
References 542

35 Quantitative Accelerated Life Testing and Data Analysis 543
Pantelis Vassiliou, Adamantios Mettas and Tarik El-Azzouzi

35.1 Introduction 543
35.2 Types of Accelerated Tests 543
35.2.1 Qualitative Tests 544
35.2.2 ESS and Burn-in 544
35.2.3 Quantitative Accelerated Tests 544
35.3 Understanding Accelerated Life Test Analysis 545
35.4 Life Distribution and Life-stress Models 546
35.4.1 Overview of the Analysis Steps 547
35.5 Parameter Estimation 548
35.6 Stress Loading 548
35.6.1 Time-independent (Constant) Stress 548
35.6.2 Time-dependent Stress 549
35.7 An Introduction to the Arrhenius Relationship 549
35.7.1 Acceleration Factor 551
35.7.2 Arrhenius Relationship Combined with a Life Distribution 551
35.7.3 Other Single Constant Stress Models 552
35.8 An Introduction to Two-stress Models 553
35.8.1 Temperature–Humidity Relationship Introduction 553
35.8.2 Temperature–Non-thermal Relationship Introduction 554
35.9 Advanced Concepts 555
35.9.1 Confidence Bounds 555
35.9.2 Multivariable Relationship and General Log-linear Model 555
35.9.3 Time-varying Stress Models 556
References 557

36 HALT and HASS Overview: The New Quality and Reliability Paradigm 559
Gregg K. Hobbs

36.1 Introduction 559
36.2 The Two Forms of HALT Currently in Use 560
36.2.1 Classical HALT Stress Application Sequence 560
36.2.2 Rapid HALT Stress Application Scheme 560
36.3 Why Perform HALT and HASS? 563
36.4 An Historical Review of Screening 566
36.5 The Phenomenon Involved and Why Things Fail 568
36.6 Equipment Required 570
36.7 The Bathtub Curve 571
36.8 Examples of Successes of HALT 572
36.9 Some General Comments on HALT and HASS 574
36.10 Conclusions 576
References 577

37 Modeling Count Data in Risk and Reliability Engineering 579
Seth D. Guikema and Jeremy P. Coffelt

37.1 Introduction 579
37.2 Classical Regression Models for Count Data 580
37.2.1 Ordinary Least Squares Regression (OLS) 580
37.2.2 Generalized Linear Models (GLMs) 581
37.2.3 Generalized Linear Mixed Models (GLMMs) 582
37.2.4 Zero-inflated Models 582
37.2.5 Generalized Additive Models (GAMs) 583
37.2.6 Multivariate Adaptive Regression Splines (MARS) 583
37.2.7 Model Fit Criteria 584
37.2.8 Example: Classical Regression for Power System Reliability 584
37.3 Bayesian Models for Count Data 586
37.3.1 Formulation of Priors 587
37.3.2 Bayesian Generalized Models 591
37.4 Conclusions 592
References 592

38 Fault Tree Analysis 595
Liudong Xing and Suprasad V. Amari

38.1 Introduction 595
38.2 A Comparison with Other Methods 596
38.2.1 Fault Tree *Versus* RBD 596
38.3 Fault Tree Construction 597
38.3.1 Important Definitions 597
38.3.2 Elements of Fault Trees 597
38.3.3 Construction Guidelines 597
38.3.4 Common Errors in Construction 598
38.4 Different Forms 598
38.4.1 Static Fault Trees 598
38.4.2 Dynamic Fault Trees 598

38.4.3 Noncoherent Fault Trees 600
38.5 Types of Fault Trees Analysis 601
38.5.1 Qualitative Analysis 601
38.5.2 Quantitative Analysis 602
38.6 Static FTA Techniques 602
38.6.1 Cutset Based Solutions 602
38.6.2 Binary Decision Diagrams 603
38.7 Dynamic FTA Techniques 607
38.7.1 Markov Chains 607
38.7.2 The Modular Approach 608
38.8 Noncoherent FTA Techniques 608
38.8.1 Prime Implicants 608
38.8.2 Importance Measures 609
38.8.3 Failure Frequency 610
38.9 Advanced Topics 611
38.9.1 Component Importance Analysis 611
38.9.2 Common Cause Failures 612
38.9.3 Dependent Failure 613
38.9.4 Disjoint Events 614
38.9.5 Multistate Systems 615
38.9.6 Phased-mission Systems 616
38.10 FTA Software Tools 617
References 617

39 Common Cause Failure Modeling: Status and Trends 621
Per Hokstad and Marvin Rausand

39.1 Introduction 621
39.1.1 Common Cause Failures 622
39.1.2 Explanation 622
39.2 Causes of CCF 623
39.2.1 Root Causes 623
39.2.2 Coupling Factors 624
39.2.3 The Beta-factor Model and its Generalizations 626
39.2.4 Plant Specific Beta-factors 627
39.2.5 Multiplicity of Failures 629
39.2.6 The Binomial Failure Rate Model and Its Extensions 630
39.2.7 The Multiple Greek Letter Model 631
39.2.8 The Multiple Beta-factor Model 631
39.3 Data Collection and Analysis 634
39.3.1 Some Data Sources 634
39.3.2 Parameter Estimation 635
39.3.3 Impact Vector and Mapping of Data 636
39.4 Concluding Remarks and Ideas for Further Research 637
References 638

40 A Methodology for Promoting Reliable Human–System Interaction 641
Joseph Sharit

40.1 Introduction 641
40.2 Methodology 644
40.2.1 Task Analysis 644
40.2.2 Checklist for Identifying Relevant Human Failure Modes 645
40.2.3 Human Failure Modes and Effects Analysis (HFMEA) 648
40.2.4 Human-failure HAZOP 648
40.2.5 Identifying Consequences and Assessing Their Criticality and Likelihood 649
40.2.6 Explanations of Human Failures 650
40.2.7 Addressing Dependencies 651
40.2.8 What-If Analysis 651
40.2.9 Design Interventions and Barriers 651
40.3 Summary 652
References 665

41 Risk Analysis and Management: An Introduction 667
Krishna B. Misra

41.1 Introduction 667
41.1.1 Preliminary Definitions 667
41.1.2 Technological Progress and Risk 668
41.1.3 Risk Perception 671
41.1.4 Risk Communication 672
41.2 Quantitative Risk Assessment 672
41.3 Probabilistic Risk Assessment 676
41.3.1 Possibilistic Approach to Risk Assessment 677
41.4 Risk Management 677
41.5 Risk Governance 678
References 678

42 Accidents Analysis of Complex Systems Based on System Control for Safety 683
Takehisa Kohda

42.1 Introduction 683
42.2 Accident Cause Analysis Based on a Safety Control 684
42.2.1 Safety from System Control Viewpoint 684
42.2.2 Accident Analysis Procedure 686
42.2.3 Illustrative Example 686
42.3 Accident Occurrence Condition Based on Control Functions for Safety 689
42.3.1 General Accident Occurrence Conditions 689
42.3.2 Occurrence of Disturbances 690
42.3.3 Safety Control Function Failure 690
42.3.4 Collision Accident Example 691
42.4 Conclusions 696
References 696

43 Probabilistic Risk Assessment 699
Mohammad Modarres

43.1 Introduction 699
43.1.1 Strength of PRA 699
43.2 Steps in Conducting a Probabilistic Risk Assessment 700
43.2.1 Objectives and Methodology 701
43.2.2 Familiarization and Information Assembly 701
43.2.3 Identification of Initiating Events 701
43.2.4 Sequences or Scenario Development 703
43.2.5 Logic Modeling 704
43.2.6 Failure Data Collection, Analysis and Performance Assessment 704
43.2.7 Quantification and Integration 706
43.2.8 Uncertainty Analysis 707
43.2.9 Sensitivity Analysis 708
43.2.10 Risk Ranking and Importance Analysis 708
43.2.11 Interpretation of Results 709
43.3 Compressed Natural Gas (CNG) Powered Buses: A PRA Case Study 710
43.3.1 Primary CNG Fire Hazards 710
43.3.2 The Probabilistic Risk Assessment Approach 710
43.3.3 System Description 711
43.3.4 Gas Release Scenarios 712
43.3.5 Fire Scenario Description 712
43.3.6 Consequence Determination 713
43.3.7 Fire Location 714
43.3.8 Risk Value Determination 714
43.3.9 Summary of PRA Results 714
43.3.10 Overall Risk Results 714
43.3.11 Uncertainty Analysis 715
43.3.12 Sensitivity and Importance Analysis 716
43.3.13 Case Study Conclusions 717
References 717

44 Risk Management 719
Terje Aven

44.1 Introduction 719
44.1.1 The Basis of Risk Management 720
44.1.2 Perspectives on Risk 722
44.1.3 Risk Analysis to Support Decisions 725
44.1.4 Challenges 725
44.2 Risk Management Principles 726
44.2.1 Economic and Decision Analysis Principles 726
44.2.2 The Cautionary and Precautionary Principles 729
44.2.3 Risk Acceptance and Decision Making 733
44.3 Recommendations 736
44.3.1 Research Challenges 739
References 740

45 Risk Governance: An Application of Analytical-deliberative Policy Making 743
Ortwin Renn

45.1 Introduction 743
45.2 Main Features of the IRGC Framework 743
45.3 The Core of the Framework: Risk Governance Phases 745
45.4 Stakeholder Involvement and Participation 749
45.5 Wider Governance Issues: Organizational Capacity and Regulatory Styles 750
45.6 Conclusions 753
Reference 754

46 Maintenance Engineering and Maintainability: An Introduction 755
Krishna B. Misra

46.1 Introduction 755
46.1.1 Maintenance System 755
46.1.2 Maintenance Philosophy 756
46.1.3 Maintenance Scope Changed with Time 757
46.2 Approaches to Maintenance 759
46.2.1 Preventive Maintenance 759
46.2.2 Predictive Maintenance 762
46.2.3 Failure-finding Maintenance 765
46.2.4 Corrective Maintenance 765
46.3 Reliability Centered Maintenance 768
46.4 Total Productive Maintenance 769
46.5 Computerized Maintenance Management System 771
References 772

47 System Maintenance: Trends in Management and Technology 773
Uday Kumar

47.1 Introduction 773
47.2 Why Does a Component or a System Fail and What Is the Role of Maintenance? 774
47.3 Trends in Management of the Maintenance Process 775
47.4 TPM Implementation 775
47.5 Application of Risk-based Decision Making in Maintenance 776
47.6 Outsourcing of Maintenance and Purchasing of the Required Functions 777
47.6.1 Contracting-out of the Maintenance Tasks 778
47.6.2 Outsourcing 778
47.6.3 Purchasing the Required Function: The Concept of Functional Products 780
47.6.4 Maintenance Performance Measurement 780
47.7 Trends in Maintenance Technology and Engineering 781
47.7.1 Design out and Design for Maintenance 781
47.7.2 Reliability 781
47.7.3 Maintainability 781
47.8 Condition Monitoring and Condition-based Maintenance Strategy 783
47.8.1 Sensor to Sensor (S2S) 783
47.8.2 Sensor to Business (S2B) 783

47.9 ICT Application in Maintenance: e-Maintenance 24-7 784
47.9.1 e-Maintenance Framework 785
47.10 Conclusions 786
References 786

48 Maintenance Models and Optimization 789
Lirong Cui

48.1 Introduction 789
48.2 Previous Contributions 791
48.3 Maintenance Models 793
48.4 Maintenance Policies 796
48.5 Maintenance Optimization and Techniques 799
48.6 Maintenance Miscellanea 800
48.7 Future Developments 802
References 803

49 Replacement and Preventive Maintenance Models 807
Toshio Nakagawa

49.1 Introduction 807
49.2 Replacement Models 808
49.2.1 Simple Replacement Models 808
49.2.2 Standard Replacement 809
49.2.3 Replacement for a Finite Interval 810
49.2.4 The Random Replacement Interval 810
49.2.5 Inspection with Replacement 812
49.2.6 The Cumulative Damage Model 813
49.2.7 The Parallel Redundant System 814
49.3 Preventive Maintenance Models 815
49.3.1 The Parallel Redundant System 815
49.3.2 The Two-unit System 816
49.3.3 The Modified Discrete Policy 816
49.3.4 Periodic and Sequential Policies 817
49.3.5 Imperfect Policies 818
49.4 Computer Systems 819
49.4.1 Intermittent Faults 820
49.4.2 Imperfect Maintenance 820
49.4.3 Optimum Restart 821
References 822

50 Effective Fault Detection and CBM Based on Oil Data Modeling and DPCA 825
Viliam Makis and Jianmou Wu

50.1 Introduction 825
50.2 Fault Detection Using MSPC,VAR Modeling and DPCA 827
50.2.1 Hotelling's T^2 Chart and PCA-based (T_A^2, Q) Charts 827
50.2.2 The Oil Data and the Selection of the In-control Portion 828
50.2.3 Multivariate Time Series Modeling of the Oil Data in the Healthy State 829

50.2.4 Dynamic PCA and the DPCA-based $(T^2_{4,t}, Q_t)$ Charts for the Oil Data 830
50.2.5 Performance Comparison of Fault Detection and Maintenance Cost 832
50.3 CBM Cost Modeling and Failure Prevention 834
50.3.1 The Proportional Hazards Model and the CBM Software EXAKT 834
50.3.2 Multivariate Time Series Modeling of the Oil Data 835
50.3.3 Application of DCPA to the Oil Data 836
50.3.4 CBM Model Building Using DPCA Covariates 837
50.3.5 Failure Prevention Performance and the Maintenance Cost Comparison 838
50.4 Conclusions 840
References 840

51 Sustainability: Motivation and Pathways for Implementation 843
Krishna B. Misra

51.1 Introduction 843
51.2 Environmental Risk Assessment 844
51.2.1 Hazard Identification 844
51.2.2 Dose-response Assessment 844
51.2.3 Exposure Assessment 845
51.2.4 Risk Characterization 845
51.3 Ecological Risk Assessment 845
51.4 Sustainability 846
51.4.1 Definition 847
51.4.2 The Social Dimension to Sustainability 847
51.4.3 Sustainability Assessment 848
51.4.4 Metrics of Sustainability 848
51.4.5 The Economics of Sustainability 850
51.4.6 Resistance to Sustainability 851
51.5 Pathways to Sustainability 852
51.6 Sustainable Future Technologies 853
51.6.1 Nanotechnology 853
51.6.2 Biotechnology 854
References 855

52 Corporate Sustainability: Some Challenges for Implementing and Teaching Organizational Risk Management in a Performability Context 857
Rod S. Barratt

52.1 Introduction 857
52.2 Pressure for Change 857
52.3 Internal Control 861
52.4 Risk Assessment and Management 862
52.5 Stakeholder Involvement 864
52.5.1 Perceptions of Risk 865
52.5.2 Stakeholder Dialog 866
52.6 Meeting Some Educational Challenges 871
52.7 Conclusion 874
References 874

53 Towards Sustainable Operations Management 875
Alison Bettley and Stephen Burnley

53.1 Introduction 875
53.2 Sustainability 876
53.3 Operations as a System to Deliver Stakeholder Value 879
53.4 Integration of Operations and Sustainability Management 883
53.4.1 Operations Strategy 884
53.4.2 Operations Design 889
53.4.3 Planning and Control 894
53.4.4 Improvement 896
53.6 Implications for Operations Management 898
53.7 Conclusions 899
References 900

54 Indicators for Assessing Sustainability Performance 905
P. Zhou and B.W. Ang

54.1 Introduction 905
54.2 Non-composite Indicators for Sustainability 907
54.3 Composite Indicators for Sustainability 907
54.4 Recent Methodological Developments in Constructing CSIs 909
54.4.1 MCDA Methods for Constructing CSIs 909
54.4.2 Data Envelopment Analysis Models for Constructing CSIs 911
54.4.3 An MCDA-DEA Approach to Constructing CSIs 912
54.5 An Illustrative Example 914
54.6 Conclusion 916
References 916

55 Sustainable Technology 919
Ronald Wennersten

55.1 Introduction 919
55.2 What Is Technology for? 920
55.3 The Linear Production System 921
55.4 Is Globalization a Solution? 921
55.5 Technology Lock-in 922
55.6 From Techno-centric Concerns to Socio-centric Concern 923
55.6.1 Changing the Focus 923
55.6.2 Towards a More Holistic View 924
55.7 Technology and Culture 925
55.8 Technology and Risk 926
55.9 Innovation and Funding of R&D 927
55.10 Engineering Education for Sustainable Development 928
55.11 Industrial Ecology – The Science of Sustainability 930
55.12 Conclusions 931
References 931

56 Biotechnology: Molecular Design in a Globalizing World 933
M.C.E. van Dam-Mieras

56.1 Introduction 933
56.2 What is Biotechnology? 933
56.3 The Importance of (Bio)Molecular Sciences 934
56.3.1 The "Omics" Research Domains 934
56.3.2 Techniques for Analysis and Separation of (Bio)Molecules 935
56.3.3 Bio-informatics 935
56.3.4 Biotechnology and Nanotechnology 935
56.4 Application of Biotechnology in Different Sectors of the Economy 935
56.4.1 Biotechnology and Healthcare 936
56.4.2 Biotechnology and Agriculture 936
56.4.3 Biotechnology and the Food Industry 936
56.4.4 Biotechnology and Industrial Production 937
56.5 Biotechnology and Sustainable Development 937
56.5.1 Sustainable Development and Globalization 937
56.5.2 Sustainable Development, Policy, and Responsibility 938
56.6 Innovations, Civil Society, and Global Space 939
56.6.1 Biotechnology and Governmental Policy 939
56.7 Biotechnology, Agriculture, and Regulations 940
56.8 Conclusions 941
References 941

57 Nanotechnology: A New Technological Revolution in the 21st Century 943
Ronald Wennersten, Jan Fidler and Spitsyna Anna

57.1 Introduction 943
57.2 Top-down and Bottom-up Designs 945
57.3 Applications of Nanotechnology 946
57.4 Applications in the Energy Sector 946
57.5 Environmental Applications 947
57.6 Other Areas of Applications 948
57.7 Market Prospects 949
57.8 Nanotechnology for Sustainability 950
57.9 Risks to the Environment and Human Health 951
57.10 Conclusions 952
References 952

58 An Overview of Reliability and Failure Modes Analysis of Microelectromechanical Systems (MEMs) 953
Zhibin Jiang and Yuanbo Li

58.1 Introduction 953
58.2 MEMS and Reliability 953
58.3 MEMS Failure Modes and Mechanisms Analysis 954
58.3.1 Stiction 955
58.3.2 Wear 956
58.3.3 Fracture 957
58.3.4 Crystallographic Defects 958

58.3.5 Creep 958
58.3.6 Degradation of Dielectrics 959
58.3.7 Environmentally Induced Failure 959
58.3.8 Electric-related Failures 960
58.3.9 Packaging Reliability 961
58.3.10 Other Failure Mechanisms 961
58.4 Conclusions 962
References 962

59 Amorphous Hydrogenated Carbon Nanofilm 967
Dechun Ba and Zeng Lin

59.1 Introduction 967
59.2 Deposition Methods 968
59.2.1 Ion Beams 968
59.2.2 Sputtering 968
59.2.3 PECVD 969
59.3 Deposition Mechanism of a-C:H 970
59.4 Bulk Properties of a-C:H 971
59.5 Electronic Applications 972
59.6 Mechanical and Other Properties 973
59.6.1 Elastic Properties 973
59.6.2 Hardness 973
59.6.3 Adhesion 974
59.6.4 Friction 974
59.6.5 Wear 975
59.6.6 Surface Properties 975
59.6.7 Biocompatible Coatings 975
59.6.8 Coatings of Magnetic Hard Disks 975
59.6.9 Surface Property Modification of Steel 975
References 979

60 Applications of Performability Engineering Concepts 985
Krishna B. Misra

60.1 Introduction 985
60.2 Areas of Applications 985
60.2.1 Healthcare Sector 985
60.2.2 Structural Engineering 986
60.2.3 Communications 986
60.2.4 Computing Systems 987
60.2.5 Fault Tolerant Systems 987
60.2.6 Prognostics and Health Monitoring 988
60.2.7 Maintenance of Infrastructures 989
60.2.8 Restructured Power Systems 990
60.2.9 PRA for Nuclear Power Plants 991
60.2.10 Problems in Software Engineering 993
60.2.11 Concluding Comments 994
References 994

61 Reliability in the Medical Device Industry 997
Vaishali Hegde

61.1 Introduction 997
61.2 Government (FDA) Control 999
61.3 Medical Device Classification 999
61.4 Reliability Programs 1000
61.4.1 The Concept Phase 1000
61.4.2 The Design Phase 1001
61.4.3 The Prototype Phase 1003
61.4.4 The Manufacturing Phase 1004
61.5 Reliability Testing 1005
61.5.1 The Development/Growth Test 1005
61.5.2 The Qualification Test 1005
61.5.3 The Acceptance Test 1005
61.5.4 The Performance Test 1005
61.5.5 Screening 1006
61.5.6 Sequential Testing 1006
61.6 MTBF Calculation Methods in Reliability Testing 1006
61.6.1 Time Terminated, Failed Items Replaced 1006
61.6.2 Time Terminated, Failed Items Not Replaced 1006
61.6.3 Failure Terminated, Failed Items Replaced 1007
61.6.4 Failure Terminated, Failed Items Not Replaced 1007
61.6.5 No Failures Observed 1007
61.7 Reliability Related Standards and Good Practices for Medical Devices 1007
References 1009

62 A Task-based Six Sigma Roadmap for Healthcare Services 1011
L.C. Tang, Shao-Wei Lam and Thong-Ngee Goh

62.1 Introduction 1011
62.2 Task Oriented Strategies of Six Sigma 1012
62.3 Six Sigma Roadmap for Healthcare 1014
62.3.1 The “Define” Phase 1015
62.3.2 The “Visualize” Phase 1017
62.3.3 The “Analyze” and “Optimize” Phases 1017
62.3.4 The “Verify” Phase 1018
62.4 Case Study of the Dispensing Process in a Pharmacy 1019
62.4.1 Sensitivity Analysis 1021
62.5 Conclusions 1022
References 1023

63 Status and Recent Trends in Reliability for Civil Engineering Problems 1025
Achintya Haldar

63.1 Introduction 1025
63.2 The Need for Reliability-based Design in Civil Engineering 1026
63.3 Changes in Design Philosophies – Design Requirements 1026
63.4 Available Analytical Methods – FORM/SORM, Simulation 1027
63.4.1 First-order Reliability Methods 1028

63.4.2 An Iterative Procedure for FORM 1031
63.4.3 Example 1033
63.5 Probabilistic Sensitivity Indexes 1035
63.6 Reliability Evaluation Using Simulation 1036
63.7 Reliability Evaluation Using FOSM, FORM and Simulation 1037
63.7.1 Example 1037
63.8 FORM for Implicit Limit State Functions – The Stochastic Finite Element Method 1039
63.9 Recent Trends in Reliability for Civil Engineering Problems 1040
63.10 Concluding Remarks 1044
References 1044

64 Performability Issues in Wireless Communication Network 1047
S. Soh, Suresh Rai, and R.R. Brooks

64.1 Introduction 1047
64.2 System Models 1048
64.2.1 Reliability Models and Assumptions 1048
64.2.2 System Communication Models and Reliability Measures 1049
64.2.3 Component Failure Models 1050
64.3 Performability Analysis and Improvement of WCN 1052
64.3.1 Example I: Computing Reliability and Expected Hop Count of WCN 1052
64.3.2 Example II: Mobile Network Analysis Using Probabilistic Connectivity Matrices 1056
64.3.3 Example III: Improving End-to-End Performability in *Ad Hoc* Networks 1063
64.3 Conclusions 1065
References 1065

65 Performability Modeling and Analysis of Grid Computing 1069
Yuan-Shun Dai, and Gregory Levitin

65.1 Introduction 1069
65.2 Grid Service Reliability and Performance 1070
65.2.1 Description of the Grid Computing 1070
65.2.2 Failure Analysis of Grid Service 1071
65.2.3 Grid Service Reliability and Performance 1072
65.2.4 Grid Service Time Distribution and Reliability/Performance Measures 1073
65.3 Star Topology Grid Architecture 1075
65.3.1 Universal Generating Function 1075
65.3.2 Illustrative Example 1077
65.4 Tree Topology Grid Architecture 1079
65.4.1 Algorithms for Determining the pmf of the Task Execution Time 1080
65.4.2 Illustrative Example 1082
65.4.3 Parameterization and Monitoring 1084
65.5 Conclusions 1085
References 1085

66 Status and Trends in the Performance Assessment of Fault Tolerant Systems 1087
John Kontoleon

66.1 Introduction 1087
66.2 Hardware Fault Tolerant Architectures and Techniques 1088

66.2.1 Passive Redundancy 1088
66.2.2 Dynamic and Hybrid Techniques 1089
66.2.3 Information Redundancy 1091
66.3 Software FT: Learning from Hardware 1091
66.3.1 Basic Issues: Diversity and Redundancy 1092
66.3.2 Space and Time Redundancy 1092
66.4 Global Fault Tolerance Issues 1094
66.4.1 Fault Tolerant Computer Networks 1095
66.4.2 Network Protocol-based Fault Tolerance 1095
66.4.3 Fault Tolerance Management 1098
66.5 Performance Evaluation: A RAM Case Study 1101
66.6 Conclusions and Future Trends 1103
References 1105

67 Prognostics and Health Monitoring of Electronics 1107
Nikhil Vichare, Brian Tuchband and Michael Pecht

67.1 Introduction 1107
67.2 Reliability and Prognostics 1108
67.3 PHM for Electronics 1108
67.4 PHM Concepts and Methods 1109
67.4.1 Fuses and Canaries 1109
67.4.2 Monitoring and Reasoning of Failure Precursors 1111
67.4.3 Monitoring Environmental and Usage Loads for Damage Modeling 1114
67.5 Implementation of PHM in a System 1117
67.6 Health Monitoring for Product Take-back and End-of-life Decisions 1118
67.7 Conclusions 1120
References 1120

68 RAMS Management of Railway Tracks 1123
Narve Lyngby, Per Hokstad, Jorn Vatn

68.1 Introduction 1123
68.2 Railway Tracks 1123
68.2.1 Railway Track Degradation 1125
68.2.2 Inspections and Interventions 1126
68.3 Degradation Modeling 1127
68.3.1 Stochastic Modeling 1127
68.3.2 Degradation in Local Time 1128
68.3.3 Degradation of Sections 1129
68.4 Methods for Optimizing Maintenance and Renewal 1131
68.4.1 Optimizing Point Maintenance 1131
68.4.2 Optimizing Section Maintenance and Renewal 1133
68.5 Case Studies on RAMS 1134
68.5.1 Optimizing Ultrasonic Inspection Intervals 1134
68.5.2 Optimizing Track Maintenance 1141
68.6 Conclusions and Future Challenges 1143
References 1143

69 Cost–Benefit Optimization Including Maintenance for Structures by a Renewal Model 1147
Rüdiger Rackwitz and Andreas Joanni

69.1 Introduction 1147
69.2 Preliminaries 1148
69.2.1 Failure Models for Deteriorating Components 1148
69.2.2 A Review of Renewal Theory 1150
69.2.3 Inspection and Repair 1151
69.3 Cost–Benefit Optimization 1152
69.3.1 General 1152
69.3.2 The Standard Case 1153
69.4 Preventive Maintenance 1154
69.4.1 Cost–Benefit Optimization for Systematic Age-dependent Repair 1154
69.4.2 Cost–Benefit Optimization Including Inspection and Repair 1156
69.5 Example 1158
69.6 Summary 1160
References 1160

70 Reliability and Price Assessment and the Associated Risk Control for Restructured Power Systems 1163
Y. Ding, Ming Zuo and Peng Wang

70.1 Introduction 1163
70.2 Reliability and Price Assessment of Restructured Power Systems with the Poolco Market Model 1167
70.2.1 Customer Response to Price Changes 1168
70.2.2 Formulation of the Nodal Price and the Nodal Reliability Problem 1168
70.2.3 System Studies 1170
70.3 Reliability and Price Assessment of Restructured Power Systems with the Hybrid Market Model 1170
70.3.1 Reliability and Cost Models for Market Participants 1170
70.3.2 A Model of Customer Responses 1172
70.3.3 Formulations of Reliability and Price Problems 1172
70.3.4 System Studies 1173
70.4 A Schema for Controlling Price Volatilities Based on Price Decomposition Techniques 1174
70.4.1 Price Decomposition Techniques 1174
70.4.2 The Proposed Schema 1175
References 1178

71 Probabilistic Risk Assessment for Nuclear Power Plants 1179
Peter Kafka

71.1 Introduction 1179
71.2 Essential Elements of PRA 1181
71.2.1 Identification of Scenarios 1183
71.2.2 System Reliability 1183
71.2.3 System Response 1183
70.2.4 Common Cause Failures 1184
70.2.5 Human Factors 1184
70.2.6 Software Reliability 1185

70.2.7 Uncertainties 1186
70.2.8 Probability Aggregation 1186
71.3 Today's Challenges 1187
71.3.1 The Risk Management Process 1187
71.3.2 Software Reliability 1189
71.3.3 Test and Maintenance and Induced Faults 1189
71.4 Outlook 1189
References 1190

72 Software Reliability and Fault-tolerant Systems: An Overview and Perspectives 1193
Hoang Pham

72.1 Introduction 1193
72.2 The Software Development Process 1195
72.3 Software Reliability Modeling 1196
72.3.1 A Generalized NHPP Model 1196
72.3.2 Application 1: The Real-time Control System 1199
72.4 Generalized Models with Environmental Factors 1199
72.4.1 Application 2: The Real-time Monitor Systems 1200
72.5 Fault-tolerant Software Systems 1201
72.5.1 The Recovery Block Scheme 1203
72.5.2 *N*-version Programming 1203
72.6 Cost Modeling 1204
72.6.1 The Gain Model with Random Field Environments 1204
72.6.2 Other Cost Models 1205
References 1206

73 Application of the Lognormal Distribution to Software Reliability Engineering 1209
Swapna S. Gokhale and Robert E. Mullen

73.1 Introduction 1209
73.2 Overview of the Lognormal 1210
73.3 Why Are Software Event Rates Lognormal? 1210
73.3.1 Graphical Operational Profile 1211
73.3.2 Multidimensional Operational Profiles 1211
73.3.3 Program Control Flow 1212
73.3.4 Sequences of Operations 1212
73.3.5 Queuing Network Models 1212
73.3.6 System State Vectors 1213
73.3.7 Fault Detection Process 1213
73.4 Lognormal Hypotheses 1213
73.4.1 Failure Rate Model 1213
73.4.2 Growth Model 1214
73.4.3 Occurrence Count Model 1214
73.4.4 Interpretation of Parameters 1215
73.5 Empirical Validation 1216
73.5.1 Failure Rate Model 1216
73.5.2 Growth Model 1218
73.5.3 Occurrence Count Model 1220
73.6 Future Research Directions 1221

73.7 Conclusions 1223
References 1223

74 Early-stage Software Product Quality Prediction Based on Process Measurement Data 1227
Shigeru Yamada

74.1 Introduction 1227
74.2 Quality Prediction Based On Quality Assurance Factors 1228
74.2.1 Data Analysis 1228
74.2.2 Correlation Analysis 1229
74.2.3 Principal Component Analysis 1229
74.2.4 Multiple Linear Regression 1230
74.2.5 The Effect of Quality Assurance Process Factors 1231
74.3 Quality Prediction Based on Management Factors 1231
74.3.1 Data Analysis 1231
74.3.2 Correlation Analysis 1232
74.3.3 Principal Component Analysis 1232
74.3.4 Multiple Linear Regression 1233
74.3.5 Effect of Management Process Factors 1234
74.3.6 Relationship Between Development Cost and Effort 1234
74.4 Relationship Between Product Quality and Development Cost 1235
74.5 Discriminant Analysis 1236
74.6 Conclusion 1236
References 1237

75 On the Development of Discrete Software Reliability Growth Models 1239
P.K. Kapur, P.C. Jha and V.B. Singh

75.1 Introduction 1239
75.2 Discrete Software Reliability Growth Models 1241
75.2.1 Discrete SRGM in a Perfect Debugging Environment 1242
75.2.2 Discrete SRGM with Testing Effort 1244
75.2.3 Modeling Faults of Different Severity 1245
75.2.4 Discrete Software Reliability Growth Models for Distributed Systems 1249
75.2.5 Discrete SRGM with Change Points 1251
75.3 Conclusion 1253
References 1254

76 Epilogue 1257
Krishna B. Misra

76.1 Mere Dependability Is Not Enough 1257
76.2 Sustainability: A Measure to Save the World from Further Deprivation 1258
76.3 Design for Performability: A Long-term Measure 1259
76.4 Parallelism between Biotechnology and Nanotechnology 1265
76.5 A Peep into the Future 1267
References 1268

About the Editor 1271
About the Contributors 1273
Index 1295

1

Performability Engineering: An Essential Concept in the 21st Century

Krishna B. Misra

RAMS Consultants, Jaipur, India

Abstract: The concept of performability is explained and the desirability of using this attribute in pursuing the design of engineering products, systems, and services is emphasized in order to meet the challenges of the 21st century. Today a new revolution is taking place where the leaders will be those nations that provide priority to the principles of sustainability in order to design, develop and use products, systems and services that are not only dependable but do not lead to disrupt the delicate ecological balance in nature. New materials, technologies and processes in consonance with environmental protection hold the key to future progress and prosperity.

1.1 Introduction

Over thousands of years, man has constantly innovated and contrived to exploit Earth's natural resources to improve his quality of life, well-being and prosperity. Whereas the last industrial revolution helped improve the living standard of man, it also caused immense damage to the environmental health of the Earth. Today another revolution is in the offing and the world is witnessing an unprecedented development in all scientific and technological fields. This can be attributed primarily to phenomenal advances made in the area of computer hardware and software, communications and information technology. It goes without saying that new areas like genetic engineering, biotechnology, nanotechnology hold the key to the development of sustainable products, systems and services in future. In fact all future technological pathways would aim to prevent and minimize, if not reverse the damage that was already done to the Earth's environment during the last industrial revolution.

1.1.1 The Fast Increasing Population

The rapid increase in the human population is a matter of concern for the people living on this planet since in the entire solar system Earth alone has a habitable atmosphere for sustaining life, which actually evolved thorough a series of delicate balances of several factors over billions of years; it took some 3.5 billion years before human life emerged from simple living cells, which themselves emerged through a unique sequence of combinations of molecules after the Earth was formed.

Since the appearance of *Homo Sapiens* on Earth, until 1900 the world population could only grow to a level of 1.6 billion people. However, by 1930, it had risen to two billion and by 1960 it had reached three billion. By 1975 it had risen to a level of four

billion, and by 1986 it was five billion; in 1999 it had already crossed the level of 6 billion. In fact, now we are adding more than 200,000 people every day. Today, we are about 6.5 billion people on Earth. Thus there has been an exponential growth in the last century as compared to the earlier centuries. The United Nations medium population projections show that the world population will reach the level of 8.9 billion by 2030 and is likely to level off at 14.5 billion by 2150. Also, even according to the U.N. Long-Range World Population Projections, the world population, under the most favorable conditions, is likely to reach a stable level of 11.5 billion by 2150. In any case, the increase in population even on the basis of most conservative estimates is likely to put tremendous pressure on the Earth's resources and will threaten the ecological balance that exists on Earth. Needless to say, every inhabitant of this planet needs to share the available resources on this planet and the Earth is the last habitat of humanity in the entire solar system as we have nowhere else to go.

Many planners think that populating other planets may be a solution to ease the population pressure on Earth. However, the technology to transport even a limited proportion of the population to any nearby planet where conditions may be favorable for humanity to survive, is non-existent and by the best technological forecasts, it cannot be developed at least for next 100–150 years. In fact by that time, we would have already done irreversible and irreparable damage to our planet.

Therefore, we have to find ways and means to sustain the human population on Earth without further damaging its environment and must even try to regenerate, if possible, its environmental health. It must dawn on all human beings living on this planet that we are living on an island in space, called Earth and that we cannot possibly escape living on it. The only recourse left is that we must mend our ways if we, and our future generations, regardless of their geographical location or nationalities, are to survive and flourish on this planet. Our problems are the problems of the planet Earth.

As the human population grows, there will be less for everyone in terms of food, clothing, materials and energy. People in the USA, who enjoy the benefits of a rich life style, might have to reconcile to being satisfied with less. Ideally, everyone on this Earth would like to maintain a wonderful lifestyle. With resources shrinking, the cost of raw materials is likely to escalate in a spiral fashion in future and the *per capita* share of world resources will also decrease. We have already witnessed this phenomenon in the case of oil prices, which have been steadily increasing over the past few decades and have more than doubled in the past few years. Likewise, other exhaustible resources are also likely to cost more in the near future.

1.1.2 Limited World Resources

The fast population growth of human beings has resulted in a fast depletion of resources on Earth. For resources of the Earth, whether they are renewable or non-renewable, if adequate care is not taken to control the rate of their use, there will always be a risk of degradation of the environment. Renewable resources can maintain themselves or can continuously be replenished, if managed properly and wisely. Food, crops animals, wildlife, forests along with solids, water and air belong to this category. We must not forget that the resources on Earth were not only meant for human beings alone but were also meant to sustain the rest of the living creatures on this planet. For this category of resources, the point of concern is not that we may run out of their supplies but that we may use them faster than they can be regenerated and if humans do not restrict to their equitable share of resources, other living beings or species on Earth will be endangered.

On the other hand, non-renewable resources like coal, oil, iron, aluminum, copper, tin, zinc, phosphates, *etc*., are exhaustible and can become depleted and their exploitation beyond sustainable levels may create severe adverse environmental effects threatening to cause irreparable damage to fragile eco-systems through which life on Earth is sustained.

There are several compulsions for using Earth's resources wisely, more efficiently, distributing them more equitably, reducing wastage and in fact reducing their overall consumption levels. The gap between developed nations and developing nations is widening. While writing these paragraphs, I have a newspaper item before me stating that Britons waste one third of all the food they buy (which is estimated at about 3 million tonnes), thereby wasting the money and energy used in producing it. On the other hand, there are undernourished people in Africa and Asia. Any kind of wastage either of materials, energy or food must be curbed. This is not only necessary for our survival and existence but also to have sustainable development so that human beings and their future generations can live and prosper without tension or wars over sharing the limited resources on this planet.

In any case, we have entered an era in which global prosperity will depend increasingly on using the Earth's resources wisely and more efficiently, distributing them more equitably, reducing wastage and in fact reducing their overall consumption levels. Unless we can accelerate this process, serious social tension is likely to arise, leading to wars and destruction of resources. The Gulf War is an example resulting from increased competition for the right of sharing scarce resources like oil. Eventually, the world might even be heading for an unforeseen catastrophe. The next scarce resource on the list may be water and sharing it may lead nations to strife.

1.1.3 The Carrying Capacity of Earth

The *carrying capacity* is defined as "The number of individuals of a given species that can be sustained indefinitely in a given space". This in the context of the number of human beings being sustained indefinitely on the planet Earth is called the *carrying capacity of Earth*. In other words, a population below the carrying capacity of the Earth can survive forever. We know that the Earth today has about 6.5 billion people. What we may want to know is how many people can survive on the Earth without damaging the Earth as the habitat of human beings. If we crowd the Earth too much, then it may affect the Earth's ability to support human beings indefinitely. Life will get worse and after a while, humans might start decreasing in number, or may even become extinct, as is happening with several other species.

On the other hand, if we find the right number of people and the right type of resources and energy to meet their requirements, then we will be able to support many people on Earth for a very long time – the humanity will be able to survive for thousands of years without compromising the standards of living. Of course, there are several controversial estimates for the carrying capacity of Earth. Some scientists put it at 40 billion and some put it merely at 2 billion – a level that we have already crossed, but what is certain is that if we do not bother about it, sooner or later we will have to face that impending disaster. If we conserve the Earth's resources, clean up pollution, and apply our present knowledge and technological advancement to finding less damaging ways of satisfying our needs, the carrying capacity can be improved. For instance, if we prevent pollution of water (also air and land) and clean up water that is already polluted, then we will be able to grow more food and more people can be supported. We know that the last industrial revolution improved the standard of living for some but damaged the pristine environment of several industrialized nations. All this happened since nobody bothered about pollution of free resources (we do not pay for preserving them) like air and water. Sustainable development would not allow that to happen again.

1.1.4 Environmental Consequences

On the other hand, the unprecedented technological developments during the last century have dealt a severe blow to the environmental health of the Earth; man's insatiable quest for a better quality of life coupled with economic disparities between people [1] has further changed the consumption pattern drastically and the choice of technologies. There has been more over-exploitation causing serious environmental consequences and wastage of resources during the past two decades than any time during the history of mankind. The depletion of ozone layer, CO_2 concentrations and pollution of rivers and water bodies including ground water

makes drinking water a valuable commodity. The winter of 2007 has been the warmest since 1880. Glaciers are receding and snow is melting. There are severe floods, forest fires and landslides in places least thought of earlier. These consequences flow from environmental degradation. In fact this phenomenon has led man to surpass the carrying capacity of Earth. The Brundland report [2] was an eye opener for all of us. In fact, realizing the gravity of the situation as early as 1992, more than 1600 scientists, including 102 Noble laureates collectively signed a Warning to Humanity, which reads as follows:

"No more than one or a few decades remain before the chance to avert the threats we confront, will be lost and the prospects for humanity immeasurably diminished… A new ethics is required – a new attitude towards discharging responsibility for caring for ourselves and for Earth… this ethics must motivate a great movement, convincing reluctant leaders, reluctant governments and reluctant people themselves to affect the needed changes".

However, due to the lack of political will and a clear understanding of the consequences of our inaction, not much has been done in the direction of taking some firm steps towards the implementation of resolutions made at several world meetings attended by world leaders. Developed countries and developing countries instead keep blaming each other for the present malaise and never come an agreement and precious time for humanity is being lost for ever.

1.2 Technology Can Help

Naturally, to keep pace with rising population, the increased volume of production to meet the demand is likely to affect the world environmental health further unless technology is put to use and pollution prevention measures are vigorously pursued. Therefore, the importance of the control of effluents and waste management along with minimization of energy and material requirements (dematerialization) requirements can hardly be emphasized while ensuring an acceptable level of performance of systems, products and services.

Technology can certainly help increase the carrying capacity in several ways, if we are able to improve upon the technology and use it wisely. For instance:

- Since we have a limited reserve of gasoline on the planet Earth, we need to build cars that will give better mileage. If each car uses less fuel, then we can serve more people with the same amount of gasoline.
- Also using newer catalytic converters, we can make vehicular emission, which contributes 25% of the world's total CO_2, which is the single major factor leading to global warming, completely free of gases causing air pollution and carbon loads.
- If we were to increase the number of telephones by using old-fashioned standard phones, we would need many, many kilometers of wire to connect all those phones and the copper for the wires will have to be mined and the process of mining uses a huge amount of fuel energy and would cause a considerable amount of pollution of land, water and air. On the other hand, if we use wireless cell phones, we do not need wires, and we can save all that fuel and pollution. Fortunately, this revolution has already taken place.
- If we use new genetically engineered plants that can be grown in dry climates and are resistant to disease, or with increased nutrition, we can grow the plants on new farms, without the use of pesticides, and produce a better crop. Of course, we will have to ensure that this happens without any risk to humans and that these new plants in themselves do not harm our environment.
- In fact, new sustainable technologies have the promise of reducing energy requirements of products and systems considerably. This has happened in the case of micro-miniaturization of electronic devices. A laptop today consumes negligibly less power than a computer of 1960, which used tubes and was highly inefficient and unreliable. After all Moore's law applies to electronic hardware development. Why will

this not happen if move over to the use of nano-devices?

Therefore, it is quite understandable that several possibilities exist for using technology to our advantage to prevent pollution and wastage of resources to help increase the carrying capacity of Earth.

1.3 Sustainability Principles

It is true that no development activity for the benefit of human beings can possibly be carried out without incurring a certain amount of risk. This risk may be in terms of environmental degradation in terms of pollution of land, water, air, depletion of resources, cost of replenishment or restoration to acceptable levels both during normal operating conditions and under the conditions of sudden hazardous releases on account of catastrophic failures or accidents. In the past, we have witnessed several technological (man-made) disasters, which had their origin in our underscoring the importance of ensuring the best level of system performance and its linkages to environmental risk.

There is a severe requirement of material conservation, waste minimization and energy efficient systems. Recycling and reuse must be given serious consideration if nonrenewable resource consumption is to be minimized or energy use associated with material extraction is to be conserved. Use of renewable energy sources has to become the order of the day. The same is true about the prevention of pollution of *free resources* like water and air, which are also required for sustaining life support system of the planet we live up on.

One of the important strategies of implementing sustainability is to prevent pollution (*rather than controlling* it) and this by itself cannot be viewed in isolation with the system performance. A better system performance would necessarily imply less environmental pollution on account of system longevity and optimum utilization of material and energy for limited resources scenario that governs the development of future systems. It is also naturally an economic proposition. In other words, sustainability depends very heavily on the performance characteristic of a system. Therefore, the objective of a system designer should be to incorporate the strategy of sustainability in all future system performance improvement programs and designs.

The key issues associated with the implementation of the sustainability characteristics of a system appear to revolve around:

- The need to conserve essential natural resources, minimize the use of materials, develop renewal energy sources and avoid overexploitation of vulnerable resource reserves.
- The need to minimize the use of processes and products that degrade or may degrade the environmental quality.
- The need to reduce the volume of waste produced by economic activities entering the environment. The quantum of waste is colossal. For example, every three months, enough aluminum is discarded in North America to rebuild the entire North American commercial airline fleet.
- The need to conserve and minimize the use of energy. For example, if recycled the energy requirement for aluminum is just 5% of the energy used in original production.
- The need to reduce or prevent activities that endanger the critical ecological processes on which life on this planet depends.

1.4 Sustainable Products and Systems

The sustainability principle requires that the products and systems use minimum material (dematerialization), and minimize the use of energy throughout their entire life cycle (extraction phase, manufacturing phase, use phase) and they should use non-hazardous materials and should be highly recyclable at the end of their life. Minimizing the use of matter minimizes the impact of the extraction phase and minimizes total material flows. Historically, the United States environmental activities have been driven by

regulation. They were focused more on the factory, on emissions from the factory. Consequently, R&D in the United States has focused very much on activities like the factory-eliminating CFCs, reducing the emissions of volatile organic compounds (VOCs), improving water quality and such types of issues. Whereas in Europe, environmental policies are being increasingly pursued to address the overall environmental impacts of a product over its entire life cycle right from raw materials extraction, product manufacturing, product use, and disposal or recycling.

The European Union's Integrated Product Policy (IPP), which seeks to stimulate demand for greener products and to promote greener design and production (Commission of the European Communities, 2001) is a step in that direction. European Union's WEEE directives also can be considered as a step in that direction. In Japan, much emphasis is being put on the environmental design of products and systems, driven both by the concern over scarce resources and as a business strategy. The emphasis is on extensive recycling of products and environmental attributes such as energy efficiency and the use of non-toxic materials. In Europe and Japan, increasing attention is being paid to materials flow analysis as a means of assessing resource efficacy and sustainability. Materials flow analysis, the calculation of flows of materials from cradle to grave, is being used to complement risk analysis and to provide insight into the challenges of sustainable use of resources. These developments indicate an international shift in emphasis from managing individual manufacturing wastes and emissions to managing the overall environmental impacts of industrial sectors and of products over their life cycles. In response, global industrial firms in the United States, Europe, and Japan, are beginning to apply these concepts to their products, manufacturing processes, and environmental programs. Since the 1970s, there is growing evidence to suggest that greater material efficiency, the use of better materials, and the growth of the service economy are contributing to the *dematerialization* of the economy.

The economic growth in developed countries is no longer accompanied by an increased consumption of basic materials. This dematerialization has been investigated for a range of materials including steel, plastics, paper, cement, and a number of metals. Also, as the sources of energy have shifted from wood and coal to petroleum, nuclear energy, and natural gas, the average amount of carbon per unit energy produced has declined, resulting in a *decarbonization* of world energy. These strategies will influence the way product and system designs are designed and manufactured in future.

In fact products, systems and services will be evaluated based on a life-cycle assessment of a product. A life-cycle assessment (LCA) evaluates the entire environmental impact of a product through its life cycle, including manufacturing, use and disposal. A great deal of work has been done to develop the technical foundations for LCA of products and processes, and to develop the databases necessary to support such assessments. The International Organization for Standardization (ISO) is working on formalizing LCA methods. Future products and systems would have to confirm to tenets of DfE (Design for Environment) methodologies.

The phenomenal advances made in information technology have built up great hopes in other technological pathways for sustainable development. Today, newer and smart materials that include composites, high strength plastics and biodegradable materials combined with material recycling and minimum effluent and waste-producing processes, the use of clean energy sources and ever-decreasing levels of energy requirement are some of the strategies that will govern the design and use of all future products, systems and services in the 21st century. New, renewable energy sources are likely to influence the design of future products and systems. It is expected that clean fusion technology will replace the present dirty fission technology in future, provided that the same is proved to be dependable, safe and sustainable.

As stated before, genetic engineering, biotechnology, nanotechnology and molecular manufacturing may provide immense possibilities to developing sustainable products, systems and services that may create minimum adverse effects

on environment and last long while using minimum material and energy requirements. All this would require new technological pathways to minimize if not reverse the damage that has already been done to the Earth's environment, if humanity is to survive on this planet.

Certainly, these factors cannot be considered in isolation of each other. Therefore, it is time to take a holistic view of the entire life cycle of activities of a product or system along with the associated cost of environmental preservation at each stage, while maximizing the product/system performance.

1.5 Economic and Performance Aspects

Classical economic theories that have treated nature as a bottomless well of resources and infinite sink for waste have to be discarded. Environmental costs, *i.e.*, the cost of preventing or controlling pollution and ecological disruption, must be internalized. In fact, it is our incapability to deal with the economic nature of environmental pollution that has been largely responsible in destroying the Earths' ecological systems. Many hidden environmental costs incurred on resource exploitation need to be passed on to the consumer or user.

To preserve our environment for future generations, the internalization of hidden costs of environment preservation will have to be accounted for, sooner or later, in order to be able to produce sustainable products in the long run. It is therefore logical to add these hidden costs to the cost of acquisitioning a product or a system.

Also, technological innovations are not without cost to the society. In fact, today leadership among the industrialized nations is judged by the amount of money a country spends on the R and D and by the number of personnel it employs for this effort. In the past, Japan was known as a nation that has turned technologies and know-how into the world's highest quality products. Now, the Chinese have excelled in the skill of making products that are known for being cheaper in cost and better in quality than their counterparts elsewhere in the world. They have invested very heavily in the development of industrial infrastructure over a period.

A recent survey shows that consumers are willing to pay up to 10% more to have an environmentally preferred product. But what does an environmentally preferred product mean, what characteristics of a product will a consumer pay more money for? It is known that consumers in Europe are more willing to pay a premium than consumers in the United States, but the definition of what attributes are important is still just at the beginning.

As of now, the performance of a product, system or a service is usually judged in terms of dependability, which can be called an aggregate of one or more of the attributes of survivability, like quality, reliability, maintainability, *etc*., and safety, of course, not overlooking the cost of physically realizing these attributes. These attributes are very much influenced by the design, raw material, fabrication, techniques and manufacturing processes and their control and, finally, by the usage. These attributes are interrelated and reflect the level or grade of the product so designed and utilized, which is expressed through dependability. In fact, as of now, dependability and cost effectiveness are primarily seen as instruments for conducting the international trade in the free market regime and thereby deciding the economic prosperity of a nation. Therefore, we can no longer rely solely on the criteria of dependability for optimizing the performance of a product, system or service. We need to introduce and define a new performance criterion that would take the sustainability aspect of developing a product or system into consideration in order to take a holistic view of the performance enhancement along with the remedial or preventive costs associated with environmental pollution.

The ever-increasing complexity of systems has further necessitated reliability of components and subsystems, the safety of human beings and the protection of our environment. Especially high-risk systems such as nuclear power plants and other chemical plants have warranted operational safety of the highest order. Besides economically endangering environmental safety or human life, costly projects such space probes can be

economically disastrous when such a system fails. Even on the basis of economic considerations, a designer is left with no option but to look for high reliability of systems as the cost of down time results in a crushing sum. For example, the power replacement cost when a moderate-sized nuclear plant is shut down may run over U.S. $80,000. The loss of several billion dollars besides the loss of human lives was involved in the total failure of the Challenger mission.

Another economic consideration that is important for developing future products and systems is to utilize obsolete products at the end of their life for recycling or reuse. If obsolete materials are not recycled, raw materials have to be processed afresh to make new products. This represents a colossal loss of resources as the energy, transport and environmental damage caused by these processes is large. In 1998, it was estimated that six million tonnes of electrical equipment waste causing a loss of resources in Europe was:

- 2.4 million tonnes of ferrous metal
- 1.2 million tonnes of plastic
- 652,000 tonnes of copper
- 336,000 tonnes of aluminum
- 336,000 tonnes of glass

besides the loss of heavy metals such as lead, mercury, *etc*. The production of all these raw materials and the goods made from them would have caused enormous environmental damage through mining, transport and energy use. In fact, recycling 1 kg of aluminium saves 8 kg of bauxite, 4 kg of chemical products and 14 kW of electricity. Therefore consideration of end-of-life treatment will soon become an integral part of product design.

Another major concern is the toxic nature of many substances such as arsenic, bromine, cadmium, lead, mercury and HCFCs, *etc*. Even in the consumer products' category, the number of refrigerators and freezers that are disposed of annually in the UK is 2.4 million units and these units contain gases like chlorofluorocarbons (CFCs) and hydro chlorofluorocarbons (HCFCs) used for cooling and insulation. Both are greenhouse gases, which when released into the atmosphere contribute to ozone layer depletion, leading to climatic changes. The European Council regulation No. 2037/2000 on substances that deplete ozone layer came into effect in October 2001.

Another example of household items is fluorescent tubes, which contain toxic heavy metals such as lead, mercury and cadmium and if these substances enter the human body they may damage liver, kidneys or brain. Mercury is a neurotoxin and can build up in the food chain. A four feet fluorescent tube may contain over 30 milligrams of mercury. The EC permissible limit for mercury in drinking water is one part per billion or 0.001 mg a liter. Here again, we have the ROHS EC directive (2002/95/EC) on hazardous substances.

In fact, end-of-life treatment will become the liability of the manufacturer and distributor of all products eventually. The WEEE directive of the European Union is the first step in this direction at least in the electrical and electronic sector. The WEEE directive (2002/96/EC) as passed by the European Community is aimed to prevent waste electrical and electronic equipment from ending up in landfills and to promote the level of recycling and reuse in the electrical and electronic sector. This directive requires all manufacturers and importers of electric and electronic equipment to meet the costs of collection, treatment and recovery of their waste electrical and electronic equipment at the end of their useful life.

The waste generated in this sector is not small either. For example, in a small country like Ireland, an estimated 35,000 to 82,000 tonnes of waste electrical and electronic equipment was generated in 2001. This amounted to 9 to 18 kg per person. Each year, more than 100 million computers are sold and over 1 million computers are disposed of in landfill sites. The rest are recycled for parts or material. Ecomicro – a recycling company in Bordeaux, France is reported to resort to recycling of components out of 1500 tonnes of obsolete or unusable computers annually. In fact, the market for refurbished computers has increased by 500% since 1996 but less than 20% of all discarded computers are recycled. Currently, a total of 40%,

which is 1.5 million printer cartridges, are recycled annually.

1.6 Futuristic System Designs

One of the ways of arresting environmental degradation is to discard old polluting technologies and production processes. The other way of slowing down the environmental degradation would be to prolong the life span of all products and systems so that we conserve energy and materials to satisfy our needs when reckoned over a given interval of time. In other words, the old principle *use and throw,* which was considered indispensable to keep the wheels of industry running and for economic prosperity of nations has eventually given way to the philosophy of reuse, recycle, and conservation if we do not intend to damage the life support system [3], of planet Earth. In short, we must be able to design highly reliable products and systems. Earlier reliability of products and systems was considered an economic compulsion to remain in business and to compete in the market but now it also an environmental compulsion

Other pathways to achieve sustainable products and systems and to minimize environmental impacts would be to use the concept of *industrial ecology,* which would entail clustering selected industries and have their *inputs* and *outputs* interlinked and mutually supported in order to preserve and conserve energy and materials including waste. We have also to work out methods of efficient energy generation and utilization, cleaner transportation, and improved materials. The use of biotechnology for improving products and cleanup process for taking care of effluents, extensive use of biodegradable materials and plastics would have to become quite common in future to prevent environmental degradation. Molecular manufacturing is being seen as clean process and a potential pathway for developing sustainable products and systems.

Several industrialized nations are taking a lead in the development of future products, processes, systems and services that are not only environmentally benign but have the advantage of economy and efficiency. Instead of mining; recycling, recovery and reuse are all becoming more and more common, as these are not only cost effective but less energy intensive and less polluting. Waste minimization, waste processing and safe disposal while conserving natural resources, the optimum and efficient use of energy including natural sources of energy, product and process, eco-friendly designs and improvement of performance of systems, for longevity and conservation of resources, are becoming increasingly important means of achieving sustainable products and systems.

Due to the existing fierce competition and improving technologies, modern systems are becoming more and more reliable than before. Today, we must recognize that unless we integrate the concept of economy reflected through material, resources and energy audit with performance audit reflected through quality, reliability, safety audits and finally with the environmental audit for sustainability, we would only be having wasteful and imperfect system designs. Therefore, it is time that we take the initiative in making system designers visualize the linkages or interdependence between environment, economy and performance.

Design for end-of-life requires manufacturers to reclaim responsibility for their products at the end-of-life. The alternatives to landfill or incineration include: maintenance, recycling for scrap material, and remanufacturing. This is shown in Figure 1.1.

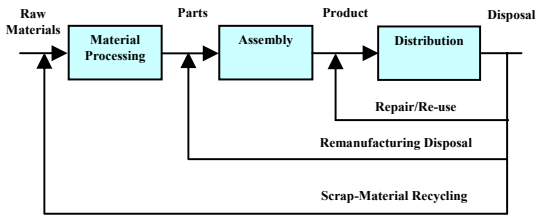


Figure 1.1. End-of-life options

Maintenance extends product life through individual upkeep or repair of specific failures. Remanufacturing is a production batch process of disassembly, cleaning, refurbishment and replacement of worn out parts, in defective or obsolete products. Scrap material recycling

involves separating a product into its constituent materials and reprocessing the material. Remanufacturing involves recycling at parts level as opposed to scrap material level. It is actually in effect recycling of materials while preserving value-added components. Remanufacturing also postpones the eventual degradation of the raw materials through contamination and molecular break down, which are the characteristics of scrap material recycling. Since remanufacturing saves 40–60% of the cost of manufacturing a completely new product and requires only 20% energy, several big companies are resorting to remanufacturing. Xerox is an example of this case. IBM has also established a facility in Endicott, New York as a reutilization and remanufacturing center. UNISYS and Hewlett Packard also use this strategy. It must, however, be stated that remanufacturing is not suitable for all types of products; it is appropriate only for those products that are technologically mature and where a large fraction of the product can be used after refurbishment.

It should be mentioned here that a designer must account for the various costs associated with recycling and remanufacturing including the first cost, recycling cost, and the cost of failure during disassembly and reassembly. The first cost is the cost of manufacturing and the first assembly. Recycling cost includes the cost of extracting material or cost of separating parts of different materials. Both maintenance and remanufacturing involve disassembly and reassembly and part reuse and failures can occur during these phases. Therefore, the consequences of the above failures are weighted by their probabilities of occurrence. For example, rivets and welds are usually destroyed during the disassembly. Another part of the cost includes the cost of a part being damaged during assembly or disassembly. Cost also includes the cost of damage caused to a part when a fastener is extracted. Maintenance costs are the costs associated with disassembly or assembly, whereas the remanufacturing cost is the total cost under all the mentioned heads.

While modeling for reliability, an analyst will have consider the fact that for a product or system with brand new components, we usually assume that the population size is constant and has the same probability density function *f(x)*. In remanufactured systems, part failure results in replacement of a part of the same type or different type. The remaining system remains unchanged or is reconfigured to accommodate the replaced part. Thus there are two different failure density functions to consider. Also the age distributions of each of the part populations are tracked to determine the reliability of the composite system population.

In short, prudence in designing systems that have less environmental consequences is the necessity of today. Longer life or durability with less pollution is also economically beneficial in the long run and would yield minimum life-cycle costs. The criterion of sustainability for judging the performance of system would imply less pollution, optimum utilization of materials and energy, waste minimization and a longer life for the system and above all minimum risks to our life support system. This would also be an economic proposition as *sustainability* is interlinked with other performance attributes.

1.7 Performability

In search of a simple, suitable and appropriate term for reflecting this new concept, several terms defined from time to time were explored but none was found more appropriate than the term *performability*. In 1980, John Meyer [4] introduced the term *performability* in the context of evaluation of highly reliable aircraft control computers for use by NASA. Originally, Meyer [4] used this term mainly to reflect attributes like reliability and other associated performance attributes like availability, maintainability, *etc*. However, this reflected only partially the performance measures that we now would like the word to mean. Also, since that time dependability has been used to include more attributes related to performance. Therefore, it was considered logical and appropriate to extend the meaning of performability to include attributes like dependability and sustainability.

Thus, the definition of the term *performability* has been widened to include sustainability in the context of the changed scenario of the 21st century

in order to reflect a holistic view of designing, producing and using products, systems or services, which will satisfy the performance requirements of a customer to the best possible extent and are not only dependable (implying survivability and safety) but are also sustainable.

1.8 Performability Engineering

Performance engineering can be defined as the entire engineering effort that goes into improving the performance of a system that not only ensures high quality, reliability, maintainability and safety but is also sustainable.

Implicit with this definition is not only the high performance of a system but also its minimum life-cycle costs. Performance engineering addresses sustainability along with other factors like quality, reliability, maintainability, and safety. We cannot separate environmental problems from the economics of clean production and clean technologies. Likewise, improved performance should necessarily imply less environmental pollution, less material and energy requirements, waste minimization, and finally conservation and efficient utilization of available resources, which in turn result in minimum life-cycle costs. These problems are best tackled at the design stage of a system.

When an aggregate attribute such as *performability* reflects a designer's entire effort in achieving sustainability for a dependable product, we could call this effort *performability engineering*, which in other words is meant to reflect the entire engineering effort of a producer to achieve the performability of a product, system or service, which in fact can be called improving 3-S, namely, survivability, safety and sustainability. This concept is depicted in Figure 1.2. It may be emphasized here that the usual definition of dependability ignores the accompanying environmental consequences while creating products, systems and services. It is evident that in order to produce a truly optimal design economically, consideration sustainability should not be overlooked. These attributes are very much influenced by the design, raw materials, fabrication, techniques and manufacturing processes. They are interrelated and reflect the level or grade of the product so designed and utilized which is expressed through dependability.

The life-cycle activities of a product or system are depicted in Figure 1.3. Performability takes a holistic view of various activities and processes and takes stock of what is being produced and what is being wasted. We conserve and economize materials, energy, avoid waste to optimize a product or system's design over its entire life cycle.

In fact, performability engineering not only aims at producing products, systems and services that are dependable but involves developing economically viable and safe processes (clean production and clean technologies) that entail minimal environmental pollution, require

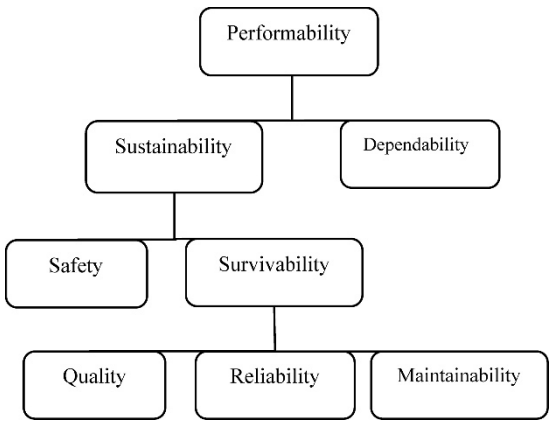


Figure 1.2. Implication of performability

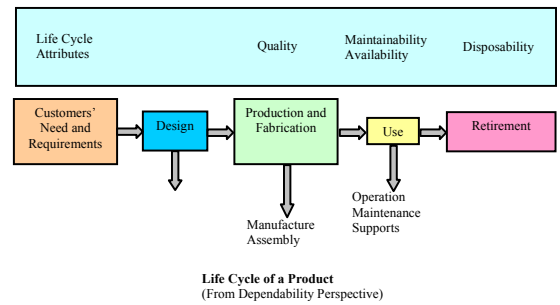


Figure 1.3. Life-cycle activities

minimum quantities of raw material and energy and yield safe products of acceptable quality and reliability that can be disposed of at the end of their life without causing any adverse effects on the environment. The WEEE directives of the European Community are a step this direction.

This would also necessitate the efficient use of natural resources and the use of non-waste technologies, which would ensure that all raw materials and energy are used in a most rational and integrated way to curb all kinds of wastages while maximizing the performance.

Obviously, less material and energy consumption, either through dematerialization, reuse or recycling or through proper treatment (clean up technology), would lead to a lesser degree of environmental degradation. Similarly, a better design would result in prolonging the life span of a product and hence would ensure less adverse effects on the environment over a given period of time. In other words, we must integrate the entire life cycle of activities of survivability with that of environmental cycle considerations to improve the product or system performance within the technological barriers with minimum cost.

At every stage of the life cycle of a product, be it extraction of material, manufacturing, use or disposal, energy and materials are required as inputs and emissions (gaseous, solid effluents or residues) and these influence environmental health of our planet.

Unless we consider all these factors, we cannot call the design of products, systems and services truly optimal from an engineering point of view. This necessitates bringing synergetic interaction between the constituent areas of performability.

1.9 Conclusion

Long-term product, system or service development strategies necessitate the consideration of performance attributes like performability, which takes a holistic view of the entire life-cycle activities and their influence on our environment and in fact on our own existence and that of future generations on this planet. Truly optimal design should necessarily consider sustainability along with dependability as the design criteria for all future products, systems and services.

References

[1] Misra KB (Ed.). Clean production: Environmental and economic perspectives. Springer, Berlin, 1996.

[2] Westman WE. Ecology, impact assessment, and environmental planning. John Wiley, New York, 1985.

[3] Report of the world commission on environment and development: The Brundtland report. Our common future: 1989.

[4] Meyer JF. On evaluating the performability of degradable computing systems, IEEE Transactions on Computers; 1980: 29(8): 720–731.

2

Engineering Design: A Systems Approach

Krishna B. Misra

RAMS Consultants, Jaipur, India

Abstract: The purpose of this chapter is not to deal with all the aspects of design of an engineering system, but to discuss the design process using the systems approach, which the design department or section of a manufacturing concern, particularly in the electronics, aerospace, machine tool sector and the producers of consumer goods such as automobiles, office equipment, and household appliances and in many other areas, can use. For a manufacturer, the *research function* helps develop new products or useful design modifications to an existing product range and *development activity*, which is basically an engineering function aimed at converting the research concept into a viable product, is known as an R&D activity and sometimes it may be associated with design engineering as a project design and development function.

2.1 Introduction

The subject of system design has been dealt and discussed with in great detail ever since the dawn of the system age around 1940. The purpose of this chapter is to provide a broader outline of a scientific approach to the planning, design, development, manufacture and evaluation of engineering systems. It is basically aimed at realizing a coherent total system to achieve a specified objective subject to physical, environmental, state-of-the art techno-economic constraints. Any other approach may prove costly and untenable.

Historically, two approaches have been helpful in understanding the world around us. The first is called *reductionism* and is based on the assumption that everything can be reduced, decomposed, or disassembled to simple indivisible parts. Reductionism is basically an analytical approach and involves disassembling of what is to be explained down to independent and indivisible parts of which it is composed; and offers the explanation of the whole by aggregating the explanations of the behaviour of these indivisible parts.

The other approach is that of the *mechanism,* in which all phenomena are explained by using a cause and effect relationship. An event or a thing is considered to be the *cause* of another event or thing (called the *effect*) and a cause is sufficient to explain its effect and nothing else is required. It employs what is known as c*losed-system* thinking in which the search for causes is environment free and the laws for the phenomena are formulated in laboratories so as to exclude environmental effects. It is *mechanization* that brought about the *industrial revolution,* which in effect helped substitute men by machines in order reduce physical labour. However, with the decline of the machine age, a concept came into existence that heralded the dawn of the system age, which

considers all objects and events, and all of their experiences, are parts of a larger whole. This concept is better known as *expansionism* and provides another way of viewing things around us; a way that is different from reductionism but compatible with it. However, this does not mean that there are no parts, but that focus is on the whole. It shifts the focus from ultimate elements to a whole with interrelated parts-to-systems.

2.1.1 Analytic Versus Synthetic Thinking

In the *analytic* approach that was associated with reductionism, an explanation of the whole was derived from explanations of its parts, whereas the systems approach has provided us with a *synthetic* mode of thinking and in this approach, one is more interested in putting things together rather than in tearing them apart analytically. In fact, *analytic thinking* can be considered as an *outside-in approach* whereas *synthetic thinking* is an *inside-out* approach of thinking.

The synthetic mode of thinking [1], when applied to physical problems is known as the *systems approach* and is based on the fact that even if each part of a system performs as well as possible, the system as a whole may not perform as well as possible. This follows from the observation that the sum of the functioning of the parts is quite often not equal to the functioning of the whole. Therefore, the synthetic mode seeks to overcome the often-observed predisposition to perfect details and ignore system outcomes.

All man-made artefacts, including products, equipment and processes are often termed *technical systems*. Engineering activities such as analysis and design for man-made or technical systems are not an end in them and may be viewed as means for satisfying human needs. Therefore, modern engineering has two aspects. One aspect addresses itself to materials and forces of nature whereas the other addresses itself to the needs of people. Successful accomplishment of engineering objectives requires a combination of technical specialties and expertise. Engineering in the systems approach necessarily has to be teamwork, where the involved individuals are aware of the relationships between the specialties, economic considerations, and ecological, political, and social factors. Today, engineering decisions require serious consideration of all these factors right in the early stage of system design and development as these decisions have a definite impact subsequently. Conversely, these factors usually impose constraints on the design process. Thus, technical aspects not only include the basic knowledge of the concerned specialties of engineering but also the knowledge of the context of the system being developed.

2.2 The Concept of a System

The word "*system*" has a very wide connotation. Broadly speaking, we have a wide variety of systems around us. Several of them have been created by man to satisfy his needs while others exist in nature. *Natural systems* are those that came into existence through natural processes whereas *man-made systems* are those in which human beings intervene through components, attributes, or relationships. Examples of man-made systems are highways, railways, waterways, marine and air transport, space projects, chemical plants, nuclear plants, electrical power generation, distribution and utilization, housing and office complexes, mining and oil extraction, *etc*. Even in the context of nanotechnology [2], nanosystems are systems and the principles of system engineering naturally apply to them. Solid mechanics, system dynamics, mechanisms and control theory are all relevant to nanotechnology and all enable technologies in future. Therefore, the word system may connote anything ranging from simple, artificial or composite, physical systems to conceptual, static and dynamic systems or even organizational and information systems. However, man-made systems are invariably imbedded into the nature [3], therefore interfaces exist between man-made systems and natural systems, and man-made systems in turn influence natural systems.

2.2.1 Definition of a System

A system can be defined as an aggregation of parts or elements, connected in some form of interaction

or interdependence to form a complex or unitary whole. In other words, *a system is a set of mutually related elements or parts assembled together in some specified order to perform an intended function*. Not only do we have systems that are assemblies of hardwired units but we also have abstract systems such as the education system, the social system, the monitory system, a scheme of procedures, *etc*. Not every set of items, facts, methods or procedures is a system. A random collection of items cannot be called a system because of the absence of purpose and unit's functional relationship. At most, it can be called a set of objects but not a system. This is a very broad definition and allows anything from a power system down to an incandescent lamp to be classified as a system provided a system must have an objective or a function to perform

2.2.2 Classification of Systems

In order to provide a better understanding of the systems that we shall be concerned with, it would not be out of place to mention here the broad classification of systems. Physical systems are those that manifest themselves in some physical form while conceptual systems are those, where the attributes of components are represented by symbols, ideas, plans, concepts and hypotheses. A physical system occupies physical space whereas conceptual systems are organizations of ideas. Conceptual systems often play an important role in the operations of physical systems in the real world. A static system has a structure without any activity whereas a dynamic system constitutes structural arrangement with some activity. Many systems may not be classified in this broad category because they may lack the notion used here. For example, a highway is a static system yet it constitutes of components, attributes and relation of dynamic systems.

A closed system is one that does not interact significantly with its environment and it exhibits the characteristics of equilibrium resulting from the internal rigidity that maintains the system in spite of influences from the environment. In contrast, an open system allows information, energy and matter to cross its boundaries. Open systems interact with their environment. They display steady state characteristics whereas in a dynamic interaction of systems, the elements adjust to the changes in the environment. Both closed and open systems exhibit the property of entropy, which may be defined as the degree of disorganization in a system and uses the term analogously to thermodynamics. Actually, entropy is the energy not available for work when energy transformation takes place from one form to the other.

In a large variety of natural or man-made systems, the inputs, processes and the outputs are described mostly in statistical terms and uncertainty exists in both the number of inputs and their distribution over time. Therefore, these features can be best described in terms of probability distributions and the system operation is known to be probabilistic.

Many of the existing systems today in the sphere of energy, transportation, information, computer communication, production, *etc.,* are all artificial or man-made. However, they can influence or be influenced by natural systems at the same time and can also be composite.

As far as this handbook is concerned, we shall deal exclusively with engineering systems. However, the system concepts and analyses presented here may be applicable to any other category of systems as well. The scope of engineering systems itself is so vast that no generalization is possible to handle such systems. However, one specific feature of engineering systems, unambiguously and strikingly, is that they are all man-made and both their elements and the system as a whole can be called products. Nevertheless, man's presence in an engineering system and his role in its functioning, may change from system to system. In any case, man shall always be regarded as an element of the system. Secondly, an engineering system must be trustworthy and dependable otherwise it cannot serve the purpose it was intended.

2.3 Characterization of a System

Most of the engineering systems today belong to the category of *complex* systems. Although such a

distinction between simple and complex systems is totally arbitrary, the degree of complexity of a system relates to the number of elements, their physical dimensions, multiplicity of links or connections of the constituent elements within the system, multiple functions, *etc*. The complexity of a system can be best defined based on the complexity of its structure and the functions performed by the system.

2.3.1 System Hierarchy

A system is a top-down approach and has basically three levels of hierarchy [4], *i.e., systems, subsystems* and *components*. In such a hierarchy, a *component* is defined as the lowest level of hierarchy in a system and is a basic functional unit of a system. Components, in the system definition should be regarded as those units of the system, which can be assumed indivisible in context of the problem being considered at hand. Sometimes we may use the word *element* (the fundamental unit) to mean a component. The assembly of components connected to produce a functional unit is designated as a *subsystem*. It is the next higher level of hierarchy in a system, after the component. Finally, an assembly of subsystems connected functionally to achieve an objective is called a *system*. It is the highest level of hierarchy in the concept of a system.

Sometimes terms like *element*, *product*, *unit*, *equipment, etc*., are also used interchangeably to mean a system, a subsystem or even a component depending upon the context of level of system hierarchy.

2.3.2 System Elements

Regardless of the level of hierarchy of a system, it always comprises *items*, *attributes* and *relationships* to accomplish a function, where:

- *Items* are the operational parts of a system consisting of input, process and output;
- *Attributes* are the properties of the items or components of a system that are discernible,
- *Relationships* are the links between items and attributes.

Therefore, a system can be considered as a set of interrelated items or units working together to accomplish some common objective, purpose or goal. The purposeful action performed by a system is called as its *function*. Once the objective of a system is defined, system items can be selected to provide the intended output for each specified set of inputs. The objective also makes it possible to establish a measure of effectiveness, which indicates how well the system will perform.

A system usually involves transformation of material, energy or information, which in turn involves *input*, *process* and *output*. In fact, a system that converts material, energy or information involves structural components, operating components and flow components. Standard components are usually the static parts.

A system has [5] its limits and boundaries. Any thing outside the boundaries of a system is called its *environmen*t and no system can ever remain isolated from it. Materials, energy or information must pass through the boundaries as an *input* to the system whereas material, energy or information that passes from the system to the environment is called its *output*. However, the constraints imposed on the system limit its operation and define the boundary within which it has to operate. In turn, the system imposes constraints on the operation of its subsystems and consequently on its components. Therefore, at all levels of the system hierarchy, there are inputs and outputs. The output of one item can be input to another. Inputs can be physical entities like materials, stresses or even information.

2.3.3 System Inputs and Outputs

An input to a system can be defined as any stimulus, or any factor whose change will invoke some kind of response from the system.

Usually, we have three groups of inputs, namely,

- *Component parameters,*
- *Operating condition parameters,*
- *External inputs.*

The component parameters are those variables that are generally determined by the hardware design, whereas the operating condition parameters

determine the state of the system in terms of operating conditions and environmental parameters, and the external inputs are the inputs, such as power supply voltage, input signal voltage, *etc*.

An input applied to the system will result in a response, which depends on the system condition and the input. This result is called the output of the system. Here again, we may have the following subdivisions:

- Primary outputs,
- Secondary outputs.

For example, primary outputs could be the power output of an amplifier or the output voltage of a stabilized power supply, whereas the secondary outputs may be regarded as the power dissipated in components, the voltage across a capacitor, noise or vibrations generated, *etc*.

2.4 Design Characteristics

Engineering design is a function that usually employs established practices to produce hardware specifications for the solution of a given problem. The design should be *functional* and must be one which, when translated into hardware, will satisfactorily perform the functions for which it was designed. The design should be *reliable*, which means when the design is translated into hardware, it must not only function but also continue to meet the full-range functional requirements over the required period of time throughout the specified range of environments. If the system is maintainable and its maintenance is anticipated, the design must provide adequately for *maintainability.*

The design must be *producible* and should be economically produced by the available production facilities and supplies. The design must be *timely* and should be completed and released within the established time schedule, which may be established either by a contract, or by the deadlines dictated by compulsions of change of model, or by competitors. The design must be *competitive* and *saleable*. However, the factors involved in saleability vary widely and may include *cost*, *special features*, *appearance*, and several other factors.

As far as possible, a designer should employ proven design techniques. When design objectives cannot be met by proven and familiar design practices, the designer is expected to employ new methods, borrow design techniques from other industries, or use available new *state-of-the-art* materials and processes. Since designers are generally supposed to be creative, it is often difficult for them to resist trying something new even though a technique of proven effectiveness and reliability exists. It is the responsibility of management to establish a system that makes it easier for a designer to use proven design than to try unproven design. Also as all system objectives cannot be met to the fullest extent in a design, the designer should be encouraged to attempt a trade-off between the set of important objectives.

By specifying unusually tight tolerances or use of exotic materials, a designer may be able to increase reliability but generally at the expense of producibility. Sometimes, a designer may be tempted to take chances with lowered reliability design without demonstrating its ability to function under the worst scenario of environment and ageing, so that the design is released on schedule. Some of these compromises and trade-offs are unavoidable. The management has the necessary information and responsibility to make decisions in this respect. However, the designer must disclose the fact that trade-offs have been made and the reasons for making these decisions to the reliability section and to the management.

To accomplish a system design, the design management must set clear-cut design objectives. These design objectives may be either imposed by the user or by the general management, or they may be developed within the design organization for submission to and acceptance (with or without modification) by the general management.

The design process necessitates a very high degree of creativeness, technological insight, and flexibility. At the initial stage, several activities like brainstorming, consultations, literature search, interviewing, systems engineering, and so on, are carried out. In the feasibility study, a designer must apply his mind and all his experience and creativity him in proposing a number of plausible solutions. Once the feasibility study has been completed, the

design has advanced to a point where a number of *alternative solutions are available for further study.* This marks the beginning of *the preliminary design phase*.

The first step in the preliminary design phase likewise depends upon the designer, who is to choose for further study the most promising configuration or topology from the feasibility analysis. Having done this, the rest of the preliminary design is carried out without changing the system configuration or topology. The designer has to choose the specifications and component parameters such that the best possible alternative within the limitations of a fixed topology results, duly considering component parameter variations and conditions of use including environmental effects.

The last phase of the design process is the *detailed design phase*, which brings the design to detailed part specifications, assembly drawings, testing of prototypes, *etc*. Following this phase, we come to the point where we may be planning for production and subsequently follow up with other stages such as distribution, utilized servicing, and retirement of the product of system.

2.5 Engineering Design

Basically, there are two main approaches in engineering design, *viz.,* the bottom-up and top-down approaches. In the case of bottom-up design, physical realizability in terms of known elements is assured, whereas the top-down design process ends with the system elements as its functional entities. Their physical realizability may not be guaranteed. In the top-down approach, the requirements are always satisfied at every step of the design process because it is an inherent part of the methodology, whereas in the bottom-up approach the methodology provides no assurance that that finally would happen.

2.5.1 Bottom-up Approach

Traditional engineering design is basically a *bottom-up approach*, where one starts with a set of known elements and creates a product or a system by *synthesizing* a set of specific system elements. It is also very rare that the functional requirements are met right in the first instance unless the system is quite simple. After determining the system's performance and deviations from what is desired, these elements and/or their configuration may be changed again and again till the desired performance is assured and the system objective is met. The process is known as the *bottom-up process* and is iterative in nature. Of course, the number of iterations naturally would depend on the complexity of the system being designed and the experience and creativity of a designer.

2.5.2 Top-down Approach

A more general methodology to engineering design is provided using the systems approach, which is actually based on a *top-down approach* to the design. There are two main features of the top-down process. First, the process is applicable to any part of the system. Starting with the system as a whole, repeated application of this process to various levels of system hierarchy will result in partitioning of the system into smaller and smaller *elements*, better known as *subsystems* and *components*. Second, the process is self-consistent. External properties of the whole system, as described by the inputs and outputs and relations between parts, must be reproduced by the external properties of the set of interacting elements.

The top-down approach also recognizes that general functions are available in transforming inputs into outputs and a designer abstracts from the particular case to the underlying generic case, and represents the genetic case by several interacting functional elements. The use of functional elements is the essential feature of the systems approach compared with systems integration in convention design. A particular functional element is applicable to a whole class of systems. Consequently, only a few such elements are required to realize many real systems.

Lastly, it may be emphasized that a systems approach is not intended to replace bottom-up design totally. Every end product incorporates physical objects working together to meet the desired objective. At any point in the design process there must be a transition from the

functional to the physical. Thus almost all engineering designs may gainfully employ both methodologies. However, the first to be employed is supposed to be the systems approach, which will reduce the system complexity by decomposing it into its constituent elements and then bottom-up design can be used to realize the design elements physically.

2.5.3 Differences Between Two Approaches

The systems approach lays emphasis on the following aspects of engineering design:

1. The systems approach views the system as a whole, whereas conventional engineering designs have always covered the design of various system components but the necessary overview and understanding of how these system components effectively fit together is not outright obvious.
2. Emphasis in the past was primarily placed on the design and system acquisition activities, without considering their impact on production, operations, maintenance, support, and disposal. If one is to adequately identify the risks associated with the upfront decision-making process, these should be based on life-cycle considerations. The systems approach considers a *life-cycle orientation* that views all phases of the system's life, *i.e.,* system design and development, production and/or construction, distribution, operation, maintenance and support, retirement, phase-out, and disposal.
3. In the systems approach, emphasis is put on providing the initial *definition of system requirements* and on the specific design criteria followed by analysis to ensure the effectiveness of early decision making in the entire design process. The actual system requirements are well defined and specified, and the tractability of these requirements right from the system level downwards are transparent. In fact, in earlier designs, this type of early analysis in many new systems was always practically non-existent. The lack of defining such an early "baseline" often resulted in greater design efforts downstream, which subsequently often resulted in expensive system modifications.
4. *The systems approach necessitates an interdisciplinary team approach* throughout the design and development process. This ensures that all design objectives are addressed in an effective and efficient way.

Last but not least, the systems approach involves the use of appropriate technologies and management principles in a synergetic manner and its application requires a focus on the process, along with a *thought process* that should lead to better system designs.

2.6 The System Design Process

To design a system is to synthesize it. This requires selecting known elements and putting them into a new configuration. A design alternative is an arrangement to realize the system objective. Evaluation is a prediction of how good the design alternative would be if it were accepted for implementation. System design evaluation generally precedes the system analysis, which in turn, is preceded by synthesis. In fact analysis, evaluation and synthesis are followed in a cyclic order till the objective of system design is met. In order to make system design cost-effective and competitive, system design evaluation should be carried out as an essential technical activity within the design process. However, it should not be pursued in isolation. System design evaluation should necessarily be carried out regularly as an assurance of continuous design improvement. As one proceeds from the top-down approach in the early phases of system design and development, there is also a follow-on "bottom-up" procedure at the same time. During the latter phases of the preliminary and detail design and development phase, subsystems or components are combined, assembled, and integrated into the specified system configuration. This, in turn, leads to the iterative process of system evaluation. Inherent within the systems engineering process is always a provision for constant feedback and necessary corrective action.

2.6.1 Main Steps of Design Process

The designer's approach to design is basically the same whether it is design of a component or a part, a subsystem, or a system, and the difference lies only in in the degree with which the task is carried out. The following is the sequence of steps that are commonly executed during the design:

1. Develop one or more design concepts that satisfy the design objective.
2. Carry out the feasibility analysis of the various possible design concepts using personal experience or by theoretical analysis and simulation, or by experimentation and testing, or by combinations of these.
3. Choose the design concept that meets all of the design objectives. Apportion reliability or any other performance goal requirements at all levels down to the part level of system hierarchy.
4. Prepare preliminary specifications and drawings.
5. Based on preliminary drawings and specifications, pass on the design for fabrication and production and procurement of development hardware to be used for feasibility and evaluation testing of the hardware.
6. Plan qualification test requirements and participate in planning production test and inspection requirements.
7. Participate in the preparation of prototype and qualification testing, taking whatever corrective design action is found to be necessary.
8. Prepare the final design. It is at this point that the review of set of designed objectives is necessary.
9. Review and approve those portions of the design that are not created by the design section.
10. Release the completed design, after ensuring that the objectives of design and other required approvals, for manufacturing or fabrication or for the user's disposition as applicable, have been achieved.

The designer has several tasks to perform even after the design is released. Two of these functions, design-configuration control and design-change control, are closely related. All design-change requests must be fully and carefully reviewed for impact on design objectives such as inherent reliability as well as for other impacts. As the design approaches completion, design-change control must come under the direct control of top management, because it is difficult to stop most design organizations from making changes. Design-configuration control relates to the control of requirements for a specific model type of hardware, serial number or production block.

There are two approaches for executing the first two phases of the design, *viz.,* the feasibility study and the preliminary system design and the most common and realistic approach based on the foregoing practice of design is outlined in Figure 2.1(a), where the configuration is fixed at the discretion of the designer and formal optimization is subsequently applied only to this design. While choosing the most promising design from the feasibility study, a designer usually makes some rough calculation of the expected performance of the system. Needless to say, a comparison of designs can only be valid if each design has been optimized according to the same criterion. If the designs are acceptable, there is no point in comparing an optimized design to one that has not been optimized, as there is little to gain by comparing two non-optimized designs.

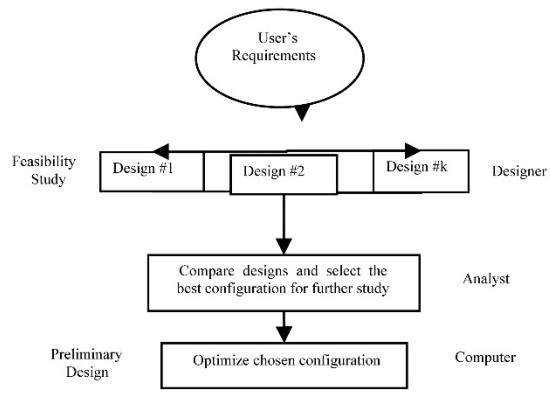


Figure 2.1(a). Common practice for system design

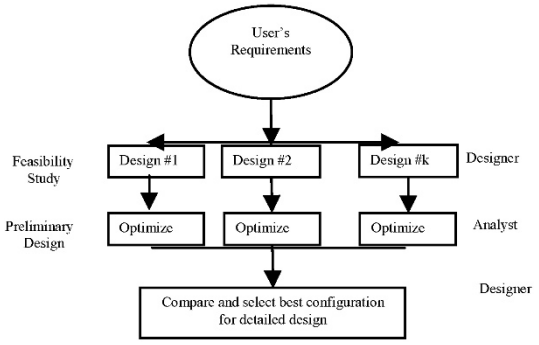


Figure 2.1(b). Ideal process for system design

Figure 2.1(b) shows the idealized structure for the first two phases of the design process. It would be unrealistic to consider this structure at all, if the design were not achieved through a computer optimization. It is, however, necessary to appreciate that the optimization of different design configurations can be quite time consuming; the designer must in each case prepare the specific actions for consideration.

It should be mentioned here that in either case the final design configuration is realized through the interaction of designer and analyst and very often we will need to do some iterations as the results of the preliminary design may sometimes provide ideas for minor changes in the design configuration.

2.6.2 Phases of System Design

Basically, any system design [6] evolves through the following phases of development:

- Conceptual Design
- Preliminary System Design
- Detail Design and Development
- System Test and Evaluation

2.6.2.1 Conceptual Design

This is the first phase in a system design and development process. Conceptual design is the foundation on which the life-cycle phases of the remaining stages of system design, *viz.,* preliminary system design, detail design and development, and system test and evaluation, are based.

Conceptual design evolves from:

- Functional definition of the system based on an identified need of the system and the requirements of the customer.
- Establishment of design criteria.

Therefore, system design is a process that starts with the need and definition of user requirements to a fully developed system configuration that is ready for production and delivery for subsequent use. To identify need, we must identify the deficiencies in the present design involving the customer if necessary; in fact, the customer should be associated with the design team throughout the design from start to end.

Once we have established the need, it is necessary to identify a possible design approach that can be pursued to meet that need and we can assess various approaches in terms of performance, effectiveness, maintenance, logistic support and economic criteria and select the best alternative. At this stage the possible technology can also be selected and the operational requirements of the system in terms of deployment, mission profile, utilization, environment of use and performance and effectiveness related parameters, *etc.,* can be developed. Maintenance and logistic support [7] for the system can also be designed at this stage. Having accomplished this, system specifications can be developed and a review of the conceptual design can be undertaken.

2.6.2.2 Preliminary System Design

This phase of design translates the system level requirements obtained from the conceptual design phase into subsystem level requirements and below for developing a system configuration. It also extends functional analysis and requirements allocation from the baseline, to the depth that is needed to identify specific requirements for hardware, software, man-power, facilities, logistic support, and other related resources. Subsystem functional analysis is basically an iterative process and decomposes requirements from the system level to the subsystem level and if desired to the components level if it is necessary to describe functional interfaces and identifying resource

needs adequately. These resources may be in the form of hardware, software, people, facilities, data, or their combinations. Also allocation of resources along with statement of maximum or minimum specifications of all important parameters is done in this phase. A system design review is again undertaken to ensure that the overall requirements are being met and the results of the functional analysis and allocation process, the trade-off studies, the design approach selected, *etc*., are reviewed for compliance with the initially set requirements. All deviations are recorded, and the necessary corrective measures as considered appropriate are initiated. Results from this phase support detail design and development.

2.6.2.3 Detail Design and Development

The design requirements at this stage are derived from the system specifications and evolve through applicable lower-levels specifications. These specifications include appropriate design-dependent parameters, technical performance measures and associated design-to criteria for characteristics that must be incorporated into the design of system, subsystems and components. This is achieved by the requirements allocation process. Design requirements for each system element are specified through the process of allocation and the identification of detailed performance and effectiveness parameters for each element in the functional analysis *(i.e.,* input–output factors, metrics, *etc*.). Given this information, a designer can decide whether to meet the requirement by an item that is commercially available and for which multiple suppliers are available or by modifying an existing commercially available item off-the-shelf or by designing, developing and producing a new item to meet the specific requirement. Detail design documentation is an essential part of detail design phase and generates a database for the purpose of information processing, storage and retrieval so that it can be used during the testing and is also available for future designs. At this stage, the design may be evaluated through the fabrication of a prototype model or using a physical working model. Detail design review is undertaken generally after the detail design has been completed, but before the release of firm design data to initiate production and/or fabrication. The objective is to establish a good "*product baseline*". Such a review is conducted to verify the adequacy and producibility of the design. The design is then "frozen" at this point, and manufacturing methods, schedules and costs are re-evaluated for final approval and the product or system design may go for testing and evaluation. This baseline design should also be evaluated for environmental impact, social acceptability, *etc*.

2.6.3 Design Evaluation

The objective of design evaluation is to establish the *baseline* against which a particular design configuration can be evaluated. The whole idea of evaluation is that the functions that the system must perform to satisfy a specific user need should be assessed along with the expectations in terms of effectiveness, costs, time, frequency and any other factors. However, the functional requirements starting at the *system level* are ultimately expected to determine the characteristics that should be incorporated within the design of the system and its subsystems and components. The ultimate objective is to assess requirements at each level of system hierarchy in terms of hardware, software, facilities, people and data.

System evaluation is a continuous process and is undertaken starting with the conceptual design, and extends to the operational use and support phase, and concludes only when the system is retired. The objective of system evaluation is to determine (through a combination of prediction, analysis and measurement activities) true system characteristics and to ensure that the system successfully fulfils its intended purpose or mission.

2.6.4 Testing Designs

The test plan for testing a system may vary depending on the system requirements; however, a general outline of test plan is expected to include the following:

- The definition and schedule of all test equipment and details of organization, administration, and control responsibilities.
- The definition of test conditions including maintenance and logistic support.
- The description of test plans for each type of testing.
- A description of the formal test phase.
- The description of conditions and provisions for the retest phase.
- The test documentation.

The basic test plan serves as a valuable reference and indicates what is to be accomplished, the requirements for testing, the schedule for the processing of equipment and materials for test support, and data collection and reporting methods and so on. All this information is useful in developing an information feedback subsystem, in providing historical data that may be useful in the design and development of new systems in future of the same type or having similar function.
Also testing is done at each stage of design to ensure that the design is progressing in the intended direction and goal. For example, *feasibility testing* is done by the designer to prove the design concept and to choose the most promising concept from several possible design concepts. *Evaluation testing* is done to test early hardware in the operating and environmental conditions for which it was designed. Test procedures and test results are documented. Hardware, test equipment, and test procedures can be modified, if conditions require this. *Qualification testing* is done for formal proofing of the design against the design specifications. Corrective design action in the form of hardware redesign is taken if test results indicate the necessity for such design modifications.

2.6.5 Final Design Documentation

As is common with engineering design, the final design documentation usually includes the following:

- *Specifications:* These list the performance requirements, specify environmental conditions, establish system performance goals, and specify the basic logistic requirements.
- *Drawings:* These include coordination drawings, correlation drawings, production drawings procurement drawings, and drawings of special test equipments.
- *Parameters:* These documents detail the functional parameters with their tolerances starting at the operational-use end and working backwards to the supplier. Tolerances are tightened at each major step so that there is room for some functional parameters drift or degradation with time and transportation. These adjusted tolerances are called “funnels of tolerance”, with the small end of the funnel at the suppliers and the large end of the funnel at the users.

The design section usually produces the design documentation in consultation and approval of the product assurance department.

2.7 User Interaction

As we have seen in the earlier sections, the design begins with the specifications of more-or-less well-defined system requirements, and “users require-ments”, which made the basis of a search for acceptable design solutions in a feasibility study acceptable in terms of both physical and economic soundness.

The user must be kept fully informed of the system limitations and the conditions of use for which it was intended. However, these must be agreed upon between the designer and the user. If the user has some special requirements to meet, they must be defined, in the system’s specifications, the exact conditions under which the system is intended to operate. Furthermore, the user must ensure that the system is subsequently operated within those conditions for the sake of the safety of the system. It is also necessary during system operation to invest in a sound user-training program and back it up with the assessment of actual conditions of use. This is expected to assist the designer to anticipate actual environments and adverse conditions during system operation, so that

the designer makes due allowance for them and the possibility of failure is not overlooked. On the other hand, the designer can take the initiative to apprise the user of the conditions and environments of use that the designer expects the system may happen be operated in and the user must be given every opportunity to match this use of the system to the designer's anticipation.

The designer must receive adequate feedback of the in-service behaviour of the system design from the user. This feedback of field experience will let the designer know about the possible deficiencies in the existing design, so that remedial measures can be taken. It will also help designer to remove those deficiencies from future system designs.

In short, matching of the design to the requirements of the user in its intended environment requires intense and good communication between the designer and the user.

2.8 Conclusions

This chapter has discussed the basic design procedure generally followed for engineering systems design. It is observed that the systems approach is convenient and tractable as compared to the bottom-up approach that was commonly followed earlier. This will become more apparent from the subsequent chapters presented in this handbook.

References

[1] Ackoff R.L., Redesigning the Future, John Wiley, New York, 1974.

[2] Drexler K. Eric, Molecular manufacturing: A future technology for cleaner production, Chapter 33 in Clean Production: Environmental and Economic Perspectives (Ed. K.B. Misra), Springer, Berlin, 1996, 783–798.

[3] Misra, K.B. (Ed.), Clean Production: Environmental and Economic Perspectives, Springer, Berlin, 1996.

[4] Misra, K.B., Reliability Analysis and Prediction: A Methodology Oriented Treatment, Elsevier Science, Amsterdam, 1992

[5] Becker Peter W., Design of Systems and Circuits, Mc Graw-Hill, New York, 1977.

[6] Blanchard Benjamin S. and Fabrycky Wolter J., Systems Engineering and Analysis, Prentice Hall, London, 1998.

[7] Misra, K.B. (Ed.), New Trends in System Reliability Evaluation, Elsevier Science, Amsterdam, 1993.

3

A Practitioner's View of Quality, Reliability and Safety[1]

Patrick D.T. O'Connor

Consultant
62 Whitney Drive, Stevenage, Hertfordshire SG1 4BJ UK

Abstract: The closely related topics of quality, reliability and safety are discussed in the context of modern technology, economics and society. Practical experiences are related to illustrate some of the key points.

3.1 Introduction

If the people involved in design and production of a new product never made mistakes, and there was no variation of any feature (dimensions, parameters, strength, *etc.*) or in the environment that the product would have to endure, then it would be relatively easy to design and manufacture products which would all be correct and which would not fail in use. Of course, engineering reality is seldom like this. Engineering designers must take account of variation, and also of the wear and degradation imposed by use and time. Production people must try to minimize the effects of process variations on quality, yield, reliability and costs. Maintenance people and users must work to keep the products serviceable.

The more that variation can be reduced and quality and reliability improved, the greater will be the benefits to the manufacturer and the user. Fewer failures during development will reduce development costs (redesign, re-test, delays, *etc.*). Less variation and fewer failures in production will reduce production costs (rework, scrap, work in progress, investigations, *etc.*). Finally, the reliability in service will be improved, resulting in enhanced reputation and thus increased sales, lower warranty costs, and greater profit opportunities. Throughout, the managers and engineers who would otherwise be busy dealing with failures would be freed to concentrate on new and improved products.

The modern world demands that products and services are safe. Ensuring the safety of engineering designs, production, use and maintenance presents great challenges to management of all of these functions.

3.1.1 The Costs of Quality, Reliability and Safety

There are two aspects to the quality, reliability and safety cost picture. By far the largest, in nearly all cases, are the costs of failure. Failures generate

[1] This chapter is based in part on the author's book The New Management of Engineering [1]

costs during development, during production and in service.

The further downstream in the process that causes of failures are discovered the greater is the cost impact, both in terms of the effect of the failure and to remove the cause, in nearly all cases.[2] Problems that cause failures or rejection after the product has been delivered add to the costs of warranty or service, and can also influence the product's reputation and sales. These internal and external costs of failures obviously depend upon the rates of occurrence.

Some of these costs, for example the cost of a re-design and re-test to correct a problem, the costs of production rework and scrap, and warranty repair costs are relatively easy to identify and quantify. These can be thought of as the direct failure costs. There are also indirect costs, for example management time involved in dealing with failures, staff morale, factory space needed for repairs, documentation, the extra test and measurement equipment needed for diagnosis and repair, the effects of delays in entering the market, delivery delays, and the effects on product reputation and therefore on future sales. Deming [2] called these the "hidden factory", the cost of which usually exceeds the profit margin on the products concerned. In extreme cases failures can lead to product recalls, and litigation and damages if injury or death is caused. The indirect costs can be difficult to identify and quantify, but they are often much greater than the direct costs. It is important to note that failure costs begin soon after initial design and continue throughout the life of the product, over many accounting periods, and even beyond to future products. For a new product they are impossible to predict with confidence.

Obviously, we should have a strategy for identifying and minimizing these costs and risks. The strategy must be in place at the earliest stages of the project and it must extend through the life cycle. A sensible first step is to make a determined attempt to forecast the likely range of failure costs.

Of course these figures can never be exact, nor can they all be stated with certainty. For example, the cost of the extra testing can be stated precisely, but how can we be sure that it will reduce the failure proportion to 5%? Also, they are based on projections into the future. Therefore they might not be convincing to financial people, particularly if their horizon is this year's figures.

We must overcome these problems by obtaining agreement on the input values and performing the analyses. Modern business software, particularly life cycle cost programs, enable the analysis to be performed in great detail. Company and project management must take the long-term view. Finally, the expected benefits in terms of reduced failures must be taken on trust. They cannot be guaranteed or proven, but overwhelming evidence exists to show that quality and reliability can be improved dramatically with relatively small but carefully managed up-front effort.

3.1.2 Achievement Costs: "Optimum Quality"

In order to create reliable designs and products it is necessary to expend effort and resources. Better final designs are the result of greater care, more effort on training, use of better materials and processes, more effective testing, and use of the results to drive design improvement (product and processes). Better quality products are the result of greater care and skill, and more effective inspection and test. It seems plausible that there is an optimum level of effort that should be expended on quality and reliability, beyond which further effort would be counter-productive.

Ideally, we should seek to optimize the expenditure on preventing causes of failures, in relation to the costs that would arise otherwise. The conventional approach to this problem has been to apply the concept of the "optimum cost of quality". It is argued that, in order to prevent failures, the "prevention costs" would have to be increased. If these rising costs could be compared with the

[2] The "Times Ten Rule" is often quoted: there will be a factor of 10 increase in costs for each further stage that a failure occurs. For example, a failure cause that is found during design might cost $100 to correct. The same failure found during development test might cost $1000 to correct, in production $10,000, and in service $100,000. Several cases show that this factor can be too low, with actual cost multipliers of 40 to 100 times being reported, and sometimes much higher if failures in service have serious consequences, such as product recall or causing injury or death.

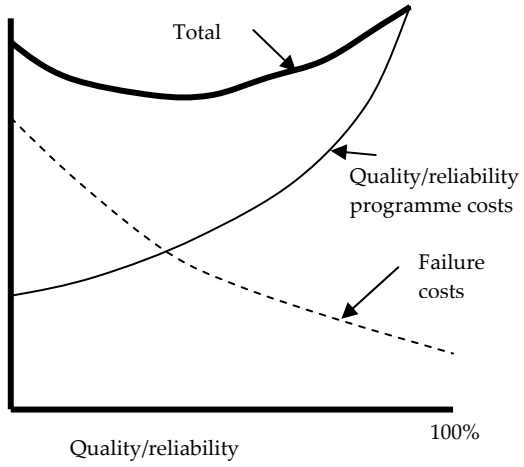


Figure 3.1. Quality and reliability costs – A traditional view

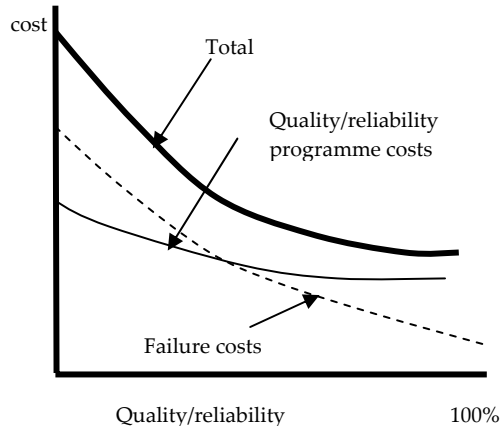


Figure 3.2. Quality and reliability costs – A modern view

falling costs of reduced failures, an optimum point would be found, at which the total "cost of quality" would be minimal (see Figure 3.1). Note that the "quality/reliability" scale of the abscissa is indicative, 100% representing no failures in production or use). The concept of the "optimum cost of quality" or "optimum quality level" at which this changeover occurs is embedded in much teaching and thinking about quality and reliability. Actually identifying the point in quantitative terms is highly uncertain. Nevertheless, the concept has often been used as a justification for sticking with the *status quo*. The idea of an optimum quality somewhat lower than perfection can be a powerful deterrent to improvement. Since the "optimum" point is so uncertain, it is tempting to believe that it is the status quo: what we are achieving now is as good as we can get. For example, on a missile system 90% reliability was accepted as being "optimum" for many years, because this was the specified level, which was eventually achieved.

It was Deming who explained the fallacious nature of the "optimum cost of quality"[3]. The minimum total cost of failures occurs when they approach zero, not at some finite, determinable figure. The argument that achieving high quality necessarily entails high costs is dismissed by considering the causes of individual failures, rather than generalized measures such as reliability or failure rate. At any point on the curve of quality/reliability *versus* cost, certain failures occur. Deming explained that, if action is taken to prevent the recurrence of these, there would nearly always be an overall saving in costs, not an increase. It is difficult to imagine a type of failure whose prevention will cost more than the consequences of doing nothing. Therefore the curve of cost *versus* failures moves downwards as quality is increased, and not upwards (see Figure 3.2). The missile example quoted above provided a striking confirmation of this when it was determined that better control of electronic parts and assembly quality, at no increased cost, resulted in reliability improvement to over 95%.

The truth of the logic taught by Deming has been dramatically exposed by the companies that have taken it to heart. The original title of Deming's book was *Quality, Productivity and Competitive Position*, thus emphasizing the strong positive correlation of all three factors. This realization has been at the core of the success of the Japanese and other companies that have set new standards and expectations for quality and reliability, in markets such as cars, machine tools, electronics and many others, while at the same

[3] Actually, Deming's arguments were presented in the context of production. This insight was probably the most important single idea that drove the Japanese post-war industrial revolution. He did not explicitly include the effects of reliability in service. Of course, if these are included the case is strengthened even more.

time reducing their costs of development and production. The concepts follow inevitably from the principles of management taught by Peter Drucker [3], requiring a completely integrated team approach to the product, rather than the functional approach of "scientific" management. The talents and motivations of everyone on the team must be devoted to improving all aspects of quality. This approach to quality has been called "total quality management" (TQM).

A major problem in this context is the fact that design, development and production costs involved can usually be estimated with reasonable accuracy, and they occur in the near future. However, the savings in failure costs are usually much more uncertain and they arise further ahead in time, often beyond the present financial plans and budgets.

3.1.3 Statistics and Engineering

The "normal" (or Gaussian) distribution is the probability function that most closely describes the great majority of natural variation, such as people's heights and IQs and monthly rainfall. It also describes quite well many variables encountered in engineering, such as dimensions of machined parts, component parameter values, and times to failure due to material fatigue. The "normal" distribution is therefore widely used by statisticians and others and it is taught in all basic statistics courses and textbooks. Therefore it could be a reasonable starting point for application to variation in engineering.

Whilst statistical methods can be very powerful, economic, and effective in engineering applications, they must be used in the knowledge that variation in engineering is in important ways different from variation in most natural processes. The natural processes whose effects are manifested in, for example, people's heights, are numerous and complex. Many different sources of variation contribute to the overall height variation observed. When many distributed variables contribute to an overall effect, the overall effect tends to be normally distributed. If we know the parameters of the underlying distributions (means, standard deviations), and if there are no interactions or we know what the interaction effects are, we can calculate the parameters of the overall distribution. These properties are also true of engineering or other non-natural processes which are continuous and in control: that is, if they are subject only to random variation.

Natural variation rarely changes with time: the distributions of people's heights and life expectancies and of rainfall patterns are much the same today as they were years ago, and we can realistically assume that they will remain so for the foreseeable future. Therefore any statistical analysis of such phenomena can be used to forecast the future, as is done, for example, by insurance actuaries. However, these conditions often do not apply in engineering. For example:

- A component supplier might make a small change in a process, which results in a large change (better or worse) in reliability. Therefore past data cannot be used to forecast future reliability using purely statistical methods. The change might be deliberate or accidental, known or unknown.
- Components might be selected according to criteria such as dimensions or other measured parameters. This can invalidate the normal distribution assumption on which much of the statistical method is based. This might or might not be important in assessing the results.
- A process of parameter might vary in time, continuously or cyclically, so that statistics derived at one time might not be relevant at others.
- Variation is often deterministic by nature, for example spring deflection as a function of force, and it would not always be appropriate to apply statistical techniques to this sort of situation.
- Variation in engineering can arise from factors that defy mathematical treatment. For example, a thermostat might fail causing a process to vary in a different way to that determined by earlier measurements, or an operator or test technician might make a mistake.

- Variation can be non-linear, not only continuous. For example, a parameter such as a voltage level may vary over a range, but could also go to zero, or a system might enter a resonant condition.

These points highlight the fact that variation in engineering is caused to a large extent by people, as designers, makers, operators, and maintainers. The behavior and performance of people is not as amenable to mathematical analysis and forecasting as is, say, the response of an engine to air inlet temperature or even weather patterns to ocean temperatures. Therefore the human element must always be considered, and statistical analysis must not be relied on without appropriate allowance being made for the effects of motivation, training and management, and the many other factors that can influence performance, cost, quality and reliability.

Finally, it is most important to bear in mind, in any application of statistical methods to problems in science and engineering, that ultimately all cause-and-effect relationships have explanations, in scientific theory, engineering design, process or human behavior, *etc.* Statistical techniques can be useful in helping us to understand and control engineering situations. However, they do not by themselves provide explanations. We must always seek to understand causes of variation, since only then can we really be in control.

3.1.4 Process Variation

All engineering processes create variation in their outputs. These variations are the results of all of the separate variables that influence the process, such as backlash and wear in machine tool gears and bearings, tool wear, material properties, vibration and temperatures. A simple electrical resistor trimming process will produce variation due to measurement inaccuracy, probe contact resistance variation, *etc.* In any manufacturing process it is obviously desirable to minimize variation of the product. There are two basic ways in which this can be achieved: we can operate the process, measure the output, and reject (or re-process if possible) all items that fall outside the allowed tolerance. Alternatively, we can reduce the variation of the process so that it produces only good products. In practice both methods are used, but it must be preferable to make only good products if possible. We will discuss the economic and management implications of these two approaches later, but let us assume that we will try to make all products within tolerance.

First of all, we must ensure that the process is inherently capable of maintaining the accuracy and precision required. "Accuracy" is the ability to keep the process on target: it determines the average, or mean, value of the output. "Precision" relates to the ability to make every product as close to target as possible: it determines the spread, or standard deviation, of the process. Having selected or designed a process that is capable of achieving the accuracy and precision required, we must then control it so that variation does not exceed the capability. A process is considered to be "in control" if the only variation is that which occurs randomly within the capability of the process. There must be no non-random trends or fluctuations, and the mean and spread must remain constant. If a process is capable and it is kept in control, in principle no out-of-tolerance products should result. This is the basic principle of "statistical process control" (SPC).

The assumption of statistical normality in engineering applications was discussed earlier. No manufacturing process can be truly "normal" in this sense for the simple reason that there are always practical limits to the process. By contrast, the mathematical normal distribution function extends to plus and minus infinity, which is clearly absurd for any real process, even natural ones. Therefore it makes little sense to extrapolate far either way beyond the mean. Also, even if engineering processes seem to follow the normal distribution close to either side of the mean, say to plus or minus 1 or 2 standard deviations (90% to 95% of the population), the pattern of variation at the extremes does not usually follow the normal distribution, due to the effects of process limits, measurements, *etc.* There is little point, therefore, in applying conventional statistical methods to analyze and forecast at these extremes.

The principles of SPC were first explained by W.A. Shewhart in 1931. He explained the nature of

variation in engineering processes and how it should be controlled. Shewhart divided variation into two categories. "Special cause" or "assignable" variation is any variation whose cause can be identified, and therefore reduced or eliminated. "Common cause" or "random" variation is that which remains after all special causes have been identified and removed: it is the economically irreducible variation left in the process.

Control charts can be used to monitor any production process once the process is in control, and if the numbers being produced are large enough to justify using the method. Many modern production tools, such as machining centers and gauges, include software that automatically generates control charts. They are one of the most important and effective tools for monitoring and improving production quality, and they should always be used, at the workplace, by the people running the process.

Shewhart pointed out the importance of control charts for process improvement. However, in much of industry they have been used mainly for monitoring, and not as part of an active improvement process. Also, an undue amount of attention has been given to the statistical aspects, so that books and teaching have tended to emphasize statistical refinement at the expense of practical utility, and the method is often perceived as being a specialists' tool rather than an aid to the process.

It was Deming, who had worked with Shewhart, who explained to Japanese industrialists the power of control charts for process improvement. This went together with his teaching that productivity and competitiveness are continuously enhanced as quality is improved, in contrast the traditional view that an "optimum" quality level existed beyond which further improvement was not cost effective. Later, Taguchi also took up this point in relation to design and used it as one of the justifications for the application of statistical experiments to optimize product and process designs. Statistical experiments, performed as part of an integrated approach to product and process design, can provide the most rational and most cost-effective basis for selecting initial control limits. In particular, the Taguchi method is compatible with modern concepts of statistical process control in production since it points the way to minimizing the variation of responses, rather than just optimizing the mean value. The explicit treatment of control and noise factors is an effective way of achieving this, and is a realistic approach for most engineering applications.

The control chart's use for process improvement is not based upon statistics. Instead, operators are taught to look for patterns that indicate "special causes" of variation. All process variation is caused by something, and the distinction between "common cause" and "special cause" lies only in the attitude to improvement. Any perceived trend or regular fluctuation can be further investigated to determine whether it represents a cause that can be eliminated or reduced.

Deming and Ishikawa taught Japanese production managers, supervisors, and workers how to interpret control charts and use them for process improvement. They also taught the use of other simple methods, such as Pareto charts and other graphical techniques, and Ishikawa developed the cause-and-effect diagram, an effective method for structuring and recording the efforts to determine causes of problems and variation. All of these methods (the "seven tools of quality") are used by the "quality circles", small groups of workers meeting during working time to determine and recommend ways of improving the processes they work on. Quality circles are the best known manifestation of Drucker's emphasis on people at the workplace being the most effective at generating improvements. The truth and effectiveness of these ideas have been dramatically demonstrated by many modern companies in highly competitive industries. Survival and growth in manufacturing industries depends as much on the fluent application of modern production quality management and methods as on product innovation and design.

3.2 Reliability

If quality can be thought of as the excellence of a product at the time it is delivered to the customer,

reliability is used in the engineering context to describe the ability of a product to work without failure during its expected time in use. A product's reliability therefore depends upon how well it is designed to withstand the conditions under which it will be used, the quality of manufacture, and, if appropriate, how well it is used and maintained.

Engineering products can fail in service for many reasons. These include:

- Variation of parameters and dimensions, leading to weakening, component mismatch, incorrect fits, vibration, *etc.* Design and manufacturing to minimize variation and its effects have been discussed earlier.
- Overstress, when an applied stress exceeds the strength of a component. Examples are mechanical overstress leading to fracture or bending of a beam or electrical overstress leading to local melting of an integrated circuit transistor or breakdown of the dielectric of a capacitor.
- Wear out, which is the result of time-dependent mechanisms such as material fatigue, wear, corrosion, insulation deterioration, *etc.*, which progressively reduce the strength of the component so that it can no longer withstand the stress applied.

There are of course many other causes of failure, such as electromagnetic interference in electronic systems, backlash in mechanical drives, stiction and friction leading to incorrect operation of mechanisms, leaks, excessive vibration, and intermittent electrical connections. Failures are not always unambiguous, like a light bulb failure, but may be open to subjective interpretation, such as a noisy gearbox, a fluctuating pressure regulator or an incorrectly diagnosed symptom in an electronic system.

Designers can in principle, and should in practice, ensure that their product designs will not fail under any expected conditions of variation, stress, wear out or for any other reason. The designers do not control variation in production, but, as explained earlier, they can ensure, together with the production people, that the effects of variations on performance and reliability are minimized and that appropriate tolerances and controls are designed into the production processes. Designers can prevent overstress failure if they understand the stresses that can be applied and ensure that adequate safety margins and protection are provided. They can protect against wear out failures by understanding the mechanisms and environments involved and by ensuring that the time to failure exceeds the expected life of the product by providing protection and, when appropriate, by designing a suitable inspection and maintenance plan. Finally, they can protect against all of the other causes of failure by knowing how they occur and by attention to detail to prevent them.

3.2.1 Quantifying Reliability

Since reliability is often expressed as a probability, the subject has attracted the attention of statisticians. Reliability can be expressed in other ways, for example as the mean time between failures (MTBF) for a repairable system, or mean time to failure (MTTF) for a non-repairable item, or the inverse of these, the failure rate or hazard rate. (Note that these measures imply that failures occur at a constant average rate: this is a convenient assumption that simplifies the mathematics, but which might bear little relation to reality).

Statistical methods for measuring, analyzing and predicting reliability have been developed and taught to the extent that many engineers view reliability engineering as being a specialist topic, based largely on statistics. This is also manifest in the fact that most books, articles and conference papers on the subject relate to the statistical aspects and that nearly all university teaching of reliability is performed by mathematics, not by engineering faculties.

As we have discussed earlier, the application of statistics to engineering is subject to practical aspects that seriously limit the extent to which statistical models can credibly represent the practical engineering situation, and particularly as a basis for forecasting the future. Since the cause of nearly every failure of a product in service is ultimately traceable to a person making a mistake, it is quite wrong and misleading to associate

reliability with the design or the product, as though reliability were a physical characteristic like mass or power. The mass and power of an engineering product are determined by physical and chemical laws, which limit what a particular design can achieve. Every product built to that design would have the same mass and power, subject of course to small variations due to production variation. However, nature places no such constraints on reliability. We can make any product as reliable as we want or need to, and the only constraints are our knowledge, skill and effort. It therefore follows that a measurement of reliability is only a statement of history. However, any attempt to use this information to predict future reliability must be conditioned by the answers to questions like these:

- What were the causes of the failures? Were the causes poor quality of some components, poor assembly control, or design features that led to their being overstressed? (Note that if the first two causes predominate, repair should lead to fewer failures in future, but if the problem is mainly due to design, repair will not improve reliability.)
- When the components failed and were replaced, were the new ones better than the ones that failed? Were the repairs performed correctly?
- Will future production of the same design use the same quality of components and of assembly? (Of course if failures have occurred action should have been taken to prevent recurrence).
- If the information on reliability is to be used to predict the reliability of another system that uses similar components, do we know that the application will be identical in terms of stress, duty cycles, environment, test, *etc.* and, if not, do we know how to relate the old data to the new application?

These are not the only relevant questions, but they illustrate the problem of quantifying reliability. In the great majority of cases the questions cannot be answered or the answers are negative. Yet we can confidently say that every 280 KΩ 1% resistor will have a resistance of 280 KΩ, plus or minus 2.8 KΩ, and will handle up to its rated power in watts. The difference is that reliability measurements and predictions are based on perceptions, human performance and a huge range of variables, whilst parameter measurements and predictions are based on science.

To most engineers these comments might seem obvious and superfluous. However, measurements and predictions of reliability are made using just such approaches and the methods are described in standards and stipulated in contracts, particularly in fields such as military and telecommunication systems. For example, the U.S. Military Handbook for predicting the reliability of electronic systems (Military Handbook 217) provides detailed mathematical "models" for electronic component failure rates, so that one can "predict" the failure rate contribution per million hours of, say, a chip capacitor while being launched from a cannon, to an accuracy of four significant figures! Other organizations have published similar "data", and similar sources exist for non-electronic items. The ISO standards on dependability and safety stipulate the use of these methods. Reliability prediction "models" have even been proposed for software, for which there are no time-related phenomena that can cause failure. These methods are all in conflict with the fundamental principle that engineering must be based on logic (*i.e.,* commonsense) and on science.

Statistical inference methods have also been applied to reliability "demonstration". The concept seems simple: test the product under representative conditions, for a suitable length of time, count the failures and calculate the reliability (*e.g.,* MTBF). Then apply standard statistical tests to determine if the reliability demonstrated meets the requirement, to a specified level of statistical confidence. However, statistical "sequential" reliability demonstration tests do not reflect practical reality. For example, if a product is tested and fails 10 times in 10 000 hours its demonstrated "best estimate" of MTBF would be 1000 hours. However, if five of the causes can be corrected, is the MTBF now 2000 hours? What about the failures that might occur in future, or to different units, that did not occur in the tests? Will the product be more or less reliable as it becomes older? Is it considered more

reliable if it has few failures but the effects of the failures are very expensive or catastrophic?

The correct way to deal with failures is not merely to count them, but to determine the causes and correct them. The correct way to predict reliability is to decide what level is necessary and the extent of the commitment to achieving it. For example, a manufacturer of TV sets discovered that competitors' equivalent sets were about four times as reliable, measured as average repairs per warranty year. They realized that to compete they had to, at least, match the competitors' performance, so that became the reliability prediction for their new product. Note that the prediction is then top down, not from component level upwards. This is much more realistic, since it takes account of all possible causes of failure, not just failures of components. The prediction is top down also in the sense that it is management-driven, which is of course necessary because failures are generated primarily by people, not by components.

Reliability engineering methods and management are described in detail in my book *Practical Reliability Engineering* [4], which has been updated to take account of technology changes, new methods and other developments.

3.3 Testing

Testing is usually the most expensive and time-consuming part of engineering development programs. Paradoxically, most development testing should in principle be unnecessary, since it is performed primarily to confirm that the design works as intended, or to show up what features need to be changed in order to make it work. If we could have complete faith in the design process we could greatly reduce the need for testing. There are some products where in fact no testing is carried out: civil engineering structures and buildings are not tested (though many such designs are now analyzed using CAE simulations) partly because of the impracticability of building and testing prototypes, but also because the designs are relatively simple and conservative. However, nearly all engineering designs must be tested. Unfortunately, this is seldom done as effectively as it could be. Here are some examples from my experience:

- A project director, managing the development of a military system that involved novel technologies and high risk of failure, stated that there would be no environmental testing because "our engineers are paid to get their designs right".
- Railway systems, particularly new locomotives and trains, were subjected to minimal development testing in comparison with systems of equivalent complexity and risk in other industries, such as cars, aircraft, and military systems. The reasons were not based upon any logic, but entirely on tradition. For most of its history, rail vehicle engineering has consisted of relatively proven technology, applied by a small number of famous designers. Also, there was nowhere to test a new train except on the rails with all the other traffic. This limited testing tradition suddenly came unstuck from about the 1980's when rail vehicle design belatedly but rapidly included a range of advanced technologies, such as AC electric traction, air conditioning, digital system controls, passenger information systems, *etc.* Some rail vehicle suppliers are now building test tracks and environmental test facilities
- A large diesel engine was selected to power a new diesel-electric freight locomotive. The engine was a well-proven machine, with previous applications in ship propulsion, power generation, *etc.* To provide assurance for the rail application, one engine was subjected to a "standard type test", involving 150 hours continuous running at maximum rated power. It passed the test. However, in rail service it proved to be very unreliable, suffering from severe cracking of the cylinder block. The problem was that the previous experience involved long duration running under steady and mostly low-stress conditions, which are totally different to the very variable, often high-stress, rail application. Also, in the previous applications,

and in the "type test", the coolant supply was large enough to ensure that it was always cool on entry to the engine, but the locomotive coolant tank was much smaller, so that the inlet temperature was very variable. The combination of variable duty cycles and variable coolant temperature led to early fatigue induced cracking of the block.

- A contract for the development of a complex new military system included a requirement that the reliability be demonstrated in a formal test before the design could be approved for production. The test criterion was that no more than 26 failures were to occur in 500 test hours, in the specified test conditions. When questioned, the customer "reliability expert" accepted that the test criterion would not be achieved if 27 minor failures occurred, but would be achieved with 25 major failures.
- A new airline passenger entertainment system was developed and sold, for installation in a fleet of new aircraft. Reliability was considered to be a critical performance requirement, since failure of any seat installations would lead to passenger complaints. A test program was implemented. However, cost and time constraints resulted in inadequate testing and problems detected not being corrected. Reliability was so poor when the system was installed and put into service that it eventually had to be removed, and the project terminated.
- A manufacturer of electronics systems submitted samples of all production batches to long-duration test at 40 °C. When asked why, the Quality Manager replied "to measure the reliability". Further questioning revealed that the systems had been in world wide service for some time, that in-service reliability performance was well known from maintenance and utilization records, and that the testing had not generated any problems that were not already known. So I said: "but you know the reliability, this test is very expensive and delays delivery, so why not stop doing it?" Months later they were still doing it. Apparently the reason was that their written company procedures said it had to be done, and changing the procedures was too difficult!
- The US Military Standard for testing microcircuits (MIL-STD-883) required that components must be tested at high temperature (125 °C) for 168 hours. This requirement was later copied into other national and international standards. The reason for choosing this unnecessarily long and expensive test time? There are 168 hours in a week!
- Among the sparse examples of recent books on aspects of testing, one makes no mention of accelerated tests and another actually condemns the idea of testing production electronics hardware at stresses higher than might be experienced in service.
- Some "experts" argued that systems that relied on software for safety-critical functions such as aircraft flight controls could never be considered to be safe, because it is not possible to prove by mathematical analysis or testing that failures will *never* occur. (We cannot prove that for pilots or mechanical controls either, but software does not make the mistakes humans make, and mechanical controls do break.)
- A military system, in service with different forces, displayed much worse reliability in army than in air force use. Investigation of the causes revealed that the army were following their traditional procedure of testing the whole system every day, whilst the air force's procedure was to test only if problems were reported. (How often do you test your TV?)
- No one seems to be able to report a completed engineering development project where too much testing had been performed. Nearly all engineering projects could have benefited from more testing, and wiser testing.

The main reason for insufficient or inappropriate testing seems to be that engineers have not developed a consistent philosophy and methodology for this essential activity. Testing is not taught as part of most engineering curricula, and academics seem to be unaware of the importance of testing, or even sometimes of its existence as a project activity.

Specialist areas are taught, for example fatigue testing to mechanical engineers and digital circuit testing to electronics engineers. However, a wide range is untaught, particularly multidisciplinary, systems and management aspects. Engineering training tends to emphasize design. Testing (and manufacturing) are topics that attract less attention, and they do not have the "glamour" of research and design. This is reflected in the generally lower esteem, status and salaries of engineers working in test and manufacturing. In some countries the near-disappearance of technician and apprentice training as routes to recognized engineering qualification has greatly reinforced this unfortunate trend. Engineering industry suffers shortages of talented engineers in these key areas. As a result, designs are often inadequately tested in development and products are inadequately tested in manufacture and maintenance. This creates high costs throughout the product cycle, damages competitiveness, and can lead to hazards.

If the design team possesses all the knowledge and resources (CAE, time, *etc.*) necessary to create correct designs, and the project leader has faith in this knowledge, then the need for testing can be reduced. Furthermore, what testing is performed will be less likely to show design errors, so the total design effort will be reduced. The point to be stressed here is that the potential improvements in engineering productivity that can in principle be achieved by harnessing the innate ability of people to learn, and then to use their knowledge to reduce the need for product test and redesign is enormous. Nevertheless, despite the most determined attempts to minimize the need for test by team organization, training, analysis and simulation, most engineering product development must involve considerable testing. Design, test, redesign and re-test proceed iteratively and in parallel, at different levels and in different locations.

Therefore development testing must be managed as an integral aspect of the whole product process. Design and test must be closely integrated from the earliest stages, and designers should be active participants in the analysis and testing of their designs. Suppliers' test programs and methods must also be managed as part of the overall project.

Testing is also an integral part of the manufacturing processes, and often of maintenance. Therefore the methods to be applied must be designed and tested during the preceding phases. Design teams should be aware of the relevant technologies and methods.

Whilst development and manufacturing testing is expensive, insufficient or inadequate testing can be far more costly later, often by orders of magnitude. Therefore the test program must be planned and financed as a long-term investment, not merely as a short-term cost. This can be a difficult concept to sell, particularly as so many organizations are driven by short-term financial measures like end-of-year profits, dividends and stock options. Engineering as well as commercial experience and judgment must be applied to the difficult and uncertain business of test. Managers at all levels and in all contributing functions must appreciate the concept that test is an investment which must be planned, and which can generate very large returns. *Test adds value***.**

The New Management of Engineering [1] is the only book on engineering management (to the best of my knowledge) that discusses the subject. My book *Test Engineering* [5] is the only book that provides an overview of test methods, economics and management.

3.4 Safety

Engineering products can cause hazards during operation or maintenance and if they fail. Safety incidents can obviously impact the reputation of a product and of the supplier. They can also generate very high costs, in product recalls, re-design and re-test. More significantly, they can lead to litigation and very high financial penalties.

Design, development, manufacture and maintenance of engineering products must obviously seek to minimize the possibility of hazards. The methods that can be applied are mostly the same as for assuring reliability, so these should be extended as appropriate.

Increasingly, engineers are being required to "prove" the safety of new products and systems, particularly in applications such as public transport and large installations that present potential hazards, *e.g.,* chemical plant and nuclear power stations. These formal, detailed statements are sometimes called "safety cases". The proof must be based on analysis of all potential modes of failure, including human failure, and of their consequences. The techniques used include failure modes, effects and criticality analysis and fault tree analysis, as used for reliability analysis as well as other techniques. The objective is to show that the probability of a single event or of a combination of multiple events that could cause defined hazards is acceptably low. The criteria for acceptability are usually laid down by the regulating authorities, and are typically for a probability not exceeding 10^{-8} per year for an accident causing loss of life. In order to "prove" such probabilities it is necessary to know or to agree what figures should be applied to all of the contributing events. We have discussed the incredibility of predicting reliability. Predicting hazard probabilities of this order is of course quite unrealistic. Any data on past events are likely to be only of historic significance, since action will almost certainly have been taken to prevent recurrence. Applying such probabilities to human actions or errors is similarly of extremely doubtful credibility. Also, accidents, particularly major ones, are usually the result of unforeseen events not considered in the hazard analyses.

It is of course essential that the hazard potentials of such systems are fully analyzed and minimized. However, it is equally important to apply commonsense to reduce the tendency to over-complicate the analysis. There is no value to be gained by attempting to quantify an analysis beyond the precision and credibility of the inputs. If the expected probability range of expected events is considered to be known to within an order of magnitude, it is absurd to present analyses that show the combined probability to a precision of several significant figures. It is also absurd to perform highly complex analyses when the causes and consequences can be sufficiently accurately estimated by much simpler methods. Such analyses can generate misguided trust in their thoroughness and accuracy, when in fact their complexity and implied precision can result in oversights and make them difficult to interpret or query. The KISS principle ("*keep it simple, stupid"*) applies to safety analysis just as much as it does to design.

3.5 Quality, Reliability and Safety Standards

3.5.1 Quality: ISO9000

The international standard for quality systems, IS09000, has been developed to provide a framework for assessing the extent to which an organization (a company, business unit or provider of goods or services) meets criteria related to the system for assuring quality of the goods or services provided. The concept was developed from the US. Military Standard for quality, MIL-Q-9858, which was introduced in the 1950s as a means of assuring the quality of products built for the U.S. military services. Most industrial nations have adopted ISO9000 in place of their previous quality standards.

The original aim of supplier certification was to provide assurance that the suppliers of equipment operated documented systems, and maintained and complied with written procedures for aspects such as fault detection and correction, calibration, control of subcontractors and segregation of defective items. They had to maintain a "Quality Manual", to describe the organization and responsibilities for quality. It is relatively easy to appreciate the motivation of large government procurement agencies to impose such standards on their suppliers. However, the approach has not been effective, despite the very high costs involved.

The major difference between the ISO standards and their defense-related predecessors is not in their content, but in the way that they are

applied. The suppliers of defense equipment were assessed against the standards by their customers, and successful assessment was necessary in order for a company to be entitled to be considered for contracts. By contrast, the IS09000 approach relies on "third-party" assessment: certain organizations are "accredited" by their national quality accreditation body, entitling them to assess companies and other organizations and to issue registration certificates. The justification given for third-party assessment is that it removes the need for every customer to perform his own assessment of suppliers. A supplier's registration indicates to all his customers that his quality system complies with the standard, and he is relieved of the burden of being subjected to separate assessments ("audits") by all of his customers, who might furthermore have varying requirements. To an increasing extent, purchasing organizations such as companies, government bodies and national and local government agencies are demanding that their suppliers must be registered[4]. Many organizations perceive the need to obtain registration in order to comply with these requirements when stipulated by their customers. They also perceive that registration will be helpful in presenting a quality image and in improving their quality systems.

IS09000 does not specifically address the quality of products and services. It describes, in very general and rather vague terms, the "system" that should be in place to assure quality. In principle, there is nothing in the standard to prevent an organization from producing poor quality goods or services, so long as procedures are followed and problems are documented. Obviously an organization with an effective quality system would normally be more likely to take corrective action and improve processes and service than would one that is disorganized. However, the fact of registration cannot be taken as assurance of quality. It is often stated that registered organizations can, and sometimes do, produce "well-documented rubbish". An alarming number of purchasing and quality managers, in industry and in the public sector, seem to be unaware of this fundamental limitation of the standards.

The effort and expense that must be expended to obtain and maintain registration tend to engender the attitude that the optimal standards of quality have been achieved. The publicity that typically goes with initial registration supports this. The objectives of the organization, and particularly of the staff directly involved in registration, are directed at the maintenance of procedures and audits to ensure that people work to them. It becomes more important to work to procedures than to develop better ways of doing things. Third-party assessment is at the heart of the IS09000 approach, but the total quality philosophy demands close partnership between the purchaser and his suppliers. A matter as essential as quality cannot be safely left to be assessed by third parties, who are unlikely to have the appropriate specialist knowledge and who cannot be members of the joint supplier-purchaser team.

Defenders of IS09000 say that the total quality approach is too severe for most organizations, and that IS09000 can provide a "foundation" for a total quality effort. However, the foremost teachers of modern quality management all argue against this view. They point out that any organization can adopt the total quality philosophy, that it will lead to far greater benefits than registration to the standards and at much lower costs. The IS09000 approach, and the whole system of accreditation, assessment and registration, together with the attendant bureaucracy and growth of a sub-industry of consultants and others who live parasitically on the system, is fundamentally at variance with the principles of the new management. It shows how easily the discredited "scientific" approach to management can be re-asserted by people and organizations with inappropriate motivation and understanding, especially when vested interests are involved.

ISO9000 has always been controversial, generating heated arguments in quality management circles. In an effort to cater for much of the criticism, ISO9000:2000 was issued. However, whilst this mitigates some of the weaknesses of the earlier version (for example, it includes a requirement for improvements to be pursued), the

[4] The European Community "CE Mark" regulations encourage registration. However, it is not true, as is sometimes claimed, that having ISO9000 registration is a necessary condition for affixing a CE Mark.

fundamental problems remain. Special versions of the standard have been developed by some industry sectors, notably automotive (ISO/TS16949:2002, replacing QS9000), commercial aviation (AS9000) and telecommunications (TL9000).

It is notable that the ISO9000 approach is very little used in Japan or by many of the best performing engineering companies elsewhere in the world, all of whom set far higher standards, related to the actual quality of the products and services provided and to continual improvement. They do not rely on "third-party" assessment of suppliers.

The correct response to IS09000 and related industry standards is to ignore them, either as the basis for internal quality management or for assessing or selecting suppliers, unless they are mandated by customers whose importance justifies the expense and management distraction involved. If registration is considered to be necessary it is important that a total quality approach is put in place first. Compliance with the IS09000 requirements will then be straightforward and the tendency to consider achievement of registration as the final goal will be avoided.

3.5.2 Reliability

U.S. Military Standard 785 is the original standard on reliability programs. It described the tasks that should be performed and the management of reliability programs. It referred to several other military standards that cover, for example, reliability prediction, reliability testing, *etc.*[5] U.K. Defence Standards 00-40 and 00-41 are similar to MIL-STD-785, but include details of methods. Non-military standards for reliability include British Standard BS5760 and the range of international standards in the IS0603000 family. Whilst these do include varying amounts of practical guidance, much of the material over-emphasizes quantitative aspects such as reliability prediction and demonstration and "systems" approaches similar to those of IS09000.

3.5.3 Safety

International, national and industry regulations and standards have been created for general and for specific aspects of safety of engineering products. Managers must be aware of what regulations and standards are applicable to the projects for which they carry responsibility and they must ensure compliance. For example, the European CE Mark Directive is primarily related to safety, medical equipment must comply with US FDA regulations, and there are strict regulations for aviation equipment, high voltage electrical equipment, *etc.*

A recent development has been the "safety case", which is a document that must be prepared by the supplier and accepted by the customer. The safety case describes the hazards that might be presented and the ways by which they will be avoided or mitigated. The approach is applied in fields such as rail, power, process plant, *etc.*, particularly when government approval is required. The safety case approach tends to be bureaucratic and "systems" based, rather like the ISO9000 approach to quality, and its effect on the safety of the UK railway system has not been encouraging.

An important new standard as far as engineering management is concerned is ISO/IEC61508, which is concerned with the safety of systems that include electronics and software. Nowadays, not many do not. The standard is without any practical value or merit. The methods described are inconsistent with accepted industry practices, and many of them are known only to specialist academics, presumably including the members of the drafting committee. The issuing of the standard is leading to a growth of bureaucracy, auditors and consultants, and increased costs. It is unlikely to generate any improvements in safety, for the same reasons that ISO9000 does not improve quality. Nevertheless, managers need to be aware of its applicability and how best to deal with it. It must not be ignored.

[5] The US DoD withdrew nearly all of these standards in 1995.

3.6 Managing Quality, Reliability and Safety

3.6.1 Total Quality Management

Engineering project managers must take the lead on quality, reliability and safety, since all aspects of design, development, production and support are links that determine the levels achieved. Quality and reliability are critical contributors to development time and costs, production costs and project success. Safety hazards can present very high business risks. By delegating responsibility for these aspects the project manager hands over control of some of the most significant determinants of success or failure. He must therefore manage quality, reliability and safety, at the same time making the best use of specialists assigned to the project. The project manager must understand the full effects, in particular the relationships to competitiveness and costs. He must ensure that all engineers on the project are dedicated to excellence, and that they are trained and supported so that failures and hazards are avoided whenever practicable and corrected whenever found.

All engineers are quality, reliability and safety engineers. However, not all are trained and experienced in design analysis methods like failure modes and effects analysis, the relevant statistical and other analysis techniques, test methods, *etc.* Therefore some specialization is often appropriate. A small specialist group can also provide the focus for development of methods, internal support and consultancy and training. However, it is essential that the engineers performing quality, reliability and safety work on projects are integrated into the project teams, just like all the other contributors. It is unfortunate that, partly because of the perception that quality and reliability use statistical methods that most engineers find unfamiliar, and partly because many of the people (engineers and statisticians) engaged in this work have exaggerated the statistical aspects, quality and reliability effort is often sidelined and given low priority.

Depending upon the type of project, the hazard risks involved and the contract or regulatory requirements, safety aspects could be managed separately from quality and reliability. However, there should be close collaboration, since many of the analysis and test methods are complementary.

Management of the quality and reliability function should be combined to ensure that the product benefits from an integrated approach to all of the factors discussed earlier. The combination of quality and reliability responsibilities should be applied centrally, as well as on projects. However, some companies separate the roles of quality and reliability. They consider reliability to be related to design and development, and quality to production. This separation of functions can be justified in organizations and in projects in which design and development work predominates, or when production is undertaken elsewhere, for example by "outsource" subcontractors. However, it is nearly always preferable to combine the functions. A combined approach can be a powerful glue to encourage cooperation between design and production engineers, whereas separation can foster uncoordinated attitudes and approaches. A combined approach can also foster an integrated approach to training, of both quality and reliability specialists and of other engineers in quality and reliability topics. Since quality of design and of production are so integrally related to productivity, costs and reliability, many of the world's most competitive engineering companies combine the functions, and many use the term "quality" to encompass the integrated function. Sometimes the expression "off-line quality" is used to describe all of the work related to quality and reliability before production starts, and "on-line quality" to refer to related work after the start of production. This top-down, integrated approach to managing quality has been called total quality management (TQM).

3.6.2 "Six Sigma"

The "six sigma" approach was originally developed in the USA by the Motorola company. It has spread to many other companies, mainly in the USA, particularly after its much-publicized application by GE under Jack Welch. It is based on the idea that if a process that is variable can be controlled so that all of its output that is within

plus or minus six standard deviations of the statistical distribution will be within specification, then only about one in a million times will it produce a "defective" output. This assumes that the output is statistically "normally" distributed, as discussed earlier; this is of course, highly unlikely, especially at such extremes. The approach is supported by the use of statistical analysis tools to identify causes of variation and to implement improvements.

The main differences between six sigma and the quality circles approach is that six sigma is run by specialists, not by the people running the processes. Some of the analytical methods used are more advanced, including ANOVA and Taguchi. The trained six sigma people are given titles like "black belts", and it is their job to find problems and generate solutions. The whole operation is driven from the top, and is directed at achieving stated targets for measurable cost savings. External consultants are often involved in training and in execution.

Six Sigma has been credited with generating significant improvements and savings. However, it is expensive. The management approach is "scientific", so it is arguable that the quality circles approach is a more effective philosophy.

3.7 Conclusions

Proper care and attention to quality, reliability and safety in design, development, production and maintenance, far from being unrealistic and expensive, are in nearly all cases practicable and highly cost effective. Reliability is a major determinant of a product's reputation and cost in service, and small differences in the reliability of competing products can greatly influence market share and profitability. If the reliability of a new product is perceived to be below expectations, or less than required by contract, serious losses or cancellation can result. Just as Deming pointed out the fallacy of an "optimum" level of production quality less than perfection, so design and development for any level of reliability less than 100% is wasteful and uncompetitive.

Note that we are discussing the probability of no failures within the expected life and environment. The designer is not expected to cater for gross overstress or inadequate maintenance, though of course the design must include margins of safety related to the criticality of failure and the likely variations in stress and strength. The creation of a reliable design is nearly always more economical than creating a design that fails in service. Furthermore, it is usually extremely difficult and expensive to improve the reliability of a product after it has been delivered, particularly if the failures are due to design shortcomings.

Designing, developing, and manufacturing modern products and systems to be reliable is therefore crucially important. The principles of reliability engineering are, however, inherently simple. Good engineering leads to good products.

Finally, it must be emphasized: well-managed effort and expenditure on quality, reliability and safety will always prove to be an excellent investment.

References

[1] O'Connor PDT. The new management of engineering. http://www.lulu.com, 2004.
[2] Deming WE. Out of the crisis. MIT University Press, Cambridge, 1986.
[3] Drucker PF. The practice of management. Heinemann, Portsmouth, NH, 1955.
[4] O'Connor PDT. Practical reliability engineering. 4th edition, Wiley, 2002. http://www.patoconnor.co.uk/practicalreliability.htm
[5] O'Connor PDT. Test engineering. Wiley, New York, 2001.

4

Product Design Optimization

Masataka Yoshimura

Optimum System Design Engineering Laboratory
Graduate School of Engineering, Mechanical Engineering Division
Kyoto University, Kyoto, Japan

Abstract: This chapter describes product design processes in product manufacturing from a technological point of view pertaining to optimization. The importance of optimization techniques for present and future product manufacturing is clarified and fundamental strategies for product design optimization are discussed, based on concurrent engineering concepts. The details of advanced optimization methodologies using hierarchical multiobjective optimizations are then explained, and a comprehensive applied example of a machine-tool optimization is provided.

4.1 Introduction

The product-manufacturing paradigm has seen profound changes during the past 100 years, as the mass production of a relatively small range of products was replaced by a job-shop type of production capable of manufacturing a large variety of products. Currently, job-shop manufacturing, in which customers select the most preferable products from a variety of products that makers prepare in advance, is giving way to a manufacturing paradigm that supports making products to order. Prompt response to customer needs is required, spurring the development of methods capable of delivering products that offer high performance, high quality and low cost, produced within a product development time that is as short as possible.

Relatively new is an increasing public awareness of the consequences of widespread product manufacturing. Its potential for causing serious harm to natural environments and the depletion of precious natural resources has made it mandatory to consider product life-cycle issues, the recycling of parts or raw materials, and manufacturing operations at all levels. Furthermore, leading product manufacturers must now also consider the mental and physical satisfaction of their customers as they live and work with their products, so design methodologies that can more closely tailor product characteristics to suit the emotional and mental requirements of particular people are necessary.

The foregoing product environments and pressures imply that product manufacturing is increasingly competitive, and the difference between business success and failure often depends on what would seem to be small design or manufacturing details. To satisfy and balance all of the foregoing factors as much as possible during the design and development of various products,

the use of sophisticated optimization techniques is indispensable, despite the complexity of the task and the difficulties encountered when dealing with requirements that include numerous characteristics having conflicting interrelationships.

In what follows, product design circumstances are first clarified, and practical methodologies for obtaining the most preferable design solutions are then presented.

4.2 Progressive Product Design Circumstances

The primary goals of advanced product manufacturing are to develop and manufacture essential products that fulfill lifestyle needs to the highest degree possible, and auxiliary products that make our living more comfortable, efficient and satisfying. Figure 4.1 illustrates examples of products associated with high standards of living. The manufacturing of all products depends on various levels of technologies. In the Stone Age, early people crafted spears and stone tools so that they could kill and process game, gather edible plants, and live as securely as they were able. Such items were developed to fit human hands and operated at a correspondingly human scale.

Over centuries and millennia of gradual human progress, innumerable kinds of products have been manufactured. The most advanced products of today are associated with high standards of living,

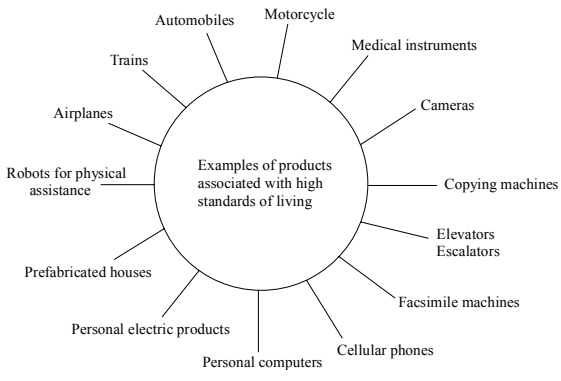


Figure 4.1. Examples of products associated with high standards of living

such as vehicles for transportation, electronic equipment for communication, business and leisure, and products for recreation and amusement. This tremendous variety of products and their associated technologies encompass a wide range of scales, from manipulation on an atomic scale, exploiting quantum effects, to monumental enterprises such as the creation of dams or a megalopolis, with the scale of the human body roughly at the center. In the course of progress, more efficient airplanes and trains are designed and built to transport increasing numbers of people to their destinations in shorter times, advanced power plants aim to provide a more stable infrastructure, and buildings of increasing scale that incorporate more sophisticated control of materials and climate aim to provide higher levels of comfort.

When considering the impact of human activity upon the natural environment and planet as a whole, it is clear that such extremely large scales really should be included in product development and design processes. On the other hand, it seems that an unbalanced degree of attention is focused on smaller scales, as shown by products for personal use that are increasingly miniaturized to provide greater convenience, utility and comfort. The realm of nanotechnology is receiving increasing publicity, as research uncovers ways to incorporate features at the scale of billionths of a meter in practical, everyday products that aim to satisfy requirements for lighter weight, superior function, and higher density of parts. Moreover, some areas of research focus on atomic and molecular scales, where certain discoveries have already lead to important breakthroughs that soon have profound social impact.

Thus, the scale of current product manufacturing covers a range from atoms and molecules, to household products, cars, trains and planes, skyscrapers, space stations, and even monumental earthworks. Since the design, manufacturing, sale and use over time of consumer products is almost always associated with rising standards of living, it is vital to preserve a strong awareness of human scales, which lie approximately at the center between the very large and the very small. Product manufacturing that ignores human needs and

desires, that is, manufacturing that concentrates too strongly on one particular scale at the expense of the human scale, may turn out to be uncomfortable or even harmful. The design and production of successful products almost always requires an astute examination of the relationships of scale between such objects, the surroundings in which they will be used, and the people who make them a part of their lives.

There are two major kinds of products, as follows:

(1) Products that ordinary customers buy and use.
(2) Industrial products used to manufacture products categorized in (1) above.

Figure 4.2 shows the relationship between customers and the manufacturers of consumer products and the industrial machines used to produce the products. The behavior of customers as they "vote with their wallets" naturally influences the demand for certain products, which in turn affects product manufacturers and supporting industries. As retail sales increase, certain manufacturers flourish and business activity radiates to other manufacturers and business sectors according to the specifics required for the production of the given products. The need to design and develop increasingly useful, attractive and sophisticated consumer products provides a fundamental stimulus for development and improvement in the manufacturing realm.

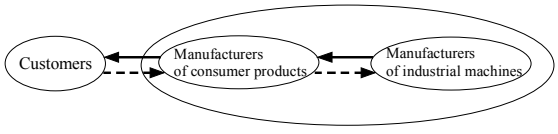


Figure 4.2. Relationship between customers and manufacturers of consumer products and industrial machines

Figure 4.3 shows a generalized manufacturing flow, which is usually the same for both consumer products and industrial machines.

Generalized manufacturing flow begins with market research and proceeds through product development, product design, product manufacturing, and ultimate sale of the goods.

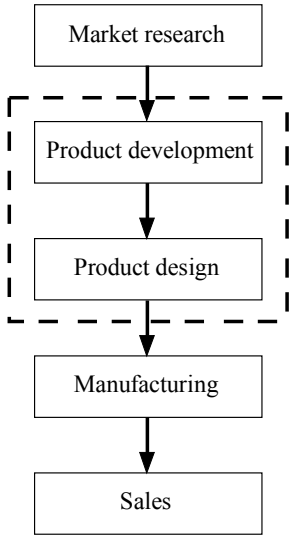


Figure 4.3. Conventional product manufacturing flow

4.3 Evaluation Criteria for Product Designs

In order to obtain optimum product design solutions, criteria for product manufacturing should first be defined, with the specifics depending on the particular nature of the product. The most fundamental criteria are described below.

4.3.1 Product Quality and Product Performance

The aim of product manufacturing is to produce products that fulfill their functions, required performances, qualities, and characteristics. The criteria first described below pertain to product qualities, which can be classified into two types: design qualities and manufacturing qualities. Design qualities correspond to values that customers require for the product, and in the case of industrial machines such as machine-tools and industrial robots, these are the accuracies, efficiency, operational energy requirements and similar performance aspects. In the case of automobiles, drivability, acceleration and braking performance, fuel economy, comfort, versatility, aesthetic value, and so on, would be considered.

On the other hand, manufacturing qualities pertain to the manufacturing processes used when producing products that incorporate desired design qualities. In the case of machine-tools, such qualities would correspond to dimensional variances, surface roughness, processing accuracy, and so on. To ensure a satisfactory level of product quality, manufacturers must evaluate whether or not their products achieve designated design specifications. Here, variations during manufacturing processes are therefore the principal evaluation factors.

Qualities that customers require in the products they seek to acquire are often labeled as being aspects of product performance. For example, accuracies when considered as a product performance correspond to certain levels of precision when the product is used for work or to accomplish its objective. Efficiencies are often evaluated by the time required to complete an objective task or sequence of operations, and a product that can accomplish work more quickly is said to have higher efficiency.

4.3.2 Manufacturing Cost

The next important criterion in product design is the total manufacturing cost, the sum of the various costs required to actually manufacture the product. The material cost of structural members and components, machining costs, casting and forging costs, powder metallurgy costs, the cost of welding, assembly, and so on, are all included in the manufacturing cost. Examples of other costs that are included in the total product cost include labor expenses, and overhead, advertising, and so on.

4.3.3 Process Capability

Process capability pertains to the maintenance of uniform qualities during the manufacturing process, and is evaluated by measuring variations in the attributes of manufactured work-pieces.

4.3.4 Reliability and Safety

The reliability and safety of products are extremely important criteria in product designs. Whenever a product fails significantly, much effort is devoted to determining the causes and how to prevent future occurrences of similar trouble. The need to adequately consider such issues when products are designed would seem to be common sense, but this is not always the case. Safety evaluations place utmost stress on the prevention of harm or injury to human beings. On the other hand, evaluations of reliability mostly focus on the regular accomplishment of product functions.

4.3.5 Natural Environment and Natural Resources

Product manufacturing has a tremendous influence on natural environments and has led to a number of catastrophes as well as shortages or exhaustion of natural resources. In response to these concerns, consideration of product life-cycles and the recycling of products and material have become indispensable aspects of responsible product designs.

One of the criteria in product life-cycle designs is given as follows:

$$\Phi = \frac{Satisfaction\ \ level\ for\ society\ as\ a\ whole}{Total\ damage\ to\ global\ environments} \tag{4.1}$$

That is, the ratio of satisfaction levels due to the successful realization of product functions over the consequential impact and damage to natural environments should be maximized to preserve the long-term viability of economical societies and establish truly sustainable lifestyles.

4.3.6 Mental Satisfaction Level

Currently, products offering high performances and qualities at reasonable costs are the norm rather than the exception. Given this situation, qualities related to mental factors such as aesthetic characteristics are becoming distinguishing factors that both encourage and respond to customer discrimination.

4.4 Fundamentals of Product Design Optimization

A basic optimization problem is formulated by including evaluation characteristics for product

designs in an objective function f, and constraint functions $g_j(j=1,2,...,m)$ and $h_k(k=1,2,...,p)$,as follows:

$f \rightarrow$ minimize or maximize

$g_j \le 0, \quad j=1,2,...,m$,

$h_k = 0, \quad k=1,2,...,p$,

f , $g_j(j=1,2,...,m)$ and $h_k(k=1,2,...,p)$ are functions of design variables $d_i(i=1,2,...,n)$. The design variables are determined by solving the foregoing optimization problem.

For the objective function f , an evaluation factor is selected from among those pertaining to the generation profits or conditions having business value, or an evaluation factor that is particularly important in terms of competition with other companies. The evaluation factors that have to be satisfied without fail are set as the constraints. Objective function f can be expressed as either a maximization or minimization problem, as desired, by expressing f as $-f$ or $1/f$.

Problems aiming to obtain values of characteristics, performances, costs, *etc*., after setting design variable values are called forward problems, while those seeking to obtain design variable values that satisfy the requirements of set characteristics, performances, costs, and the like, are called inverse problems. Design optimization problems are of the inverse type.

In any case, product designs always require that the product manufacturing cost be minimized, and methods for reducing this cost in most practical scenarios inevitably result in degradation of the product performances. There are cases where a specific product performance must be as high as possible, and to realize this requirement, the product manufacturing cost is forced upward. Furthermore, when the upper or lower bounds of the constraints are set, their values determine the result of the optimum solution, but in practical scenarios, setting specific upper or lower bounds is often problematic when certain factors are unclear. In these cases, formulating optimization problems with a number of objective functions that include such characteristics is effective, and design optimization problems of this type are generally called multiobjective optimization problems [1].

When there are two objective functions and smaller values of each objective function is more preferable, the objective of the multiobjective function is expressed as follows:

$$f=[f_1, f_2] \rightarrow \text{minimize.} \qquad (4.2)$$

As an example, consider a scenario where product designers are seeking a design solution that has a higher product performance while process designers engaged in practical manufacturing desire solutions that have lower product manufacturing costs. These two requirements naturally have conflicting interrelationships. Figure 4.4 shows the relationships between a product performance that must be maximized and the product manufacturing cost that always needs to be minimized. When the product performance and the product manufacturing cost are respectively expressed by f_1 and f_2 , the foregoing multiobjective formulation is changed as follows:

$$f=[-f_1, f_2] \rightarrow \text{minimize.} \qquad (4.3)$$

The shaded area in Figure 4.4 corresponds to the region that is feasible using presently available knowledge and technology. The line PQ corresponds to a Pareto optimum solution set for the two objective functions of the product performance and the product manufacturing cost.

The Pareto optimum solution set is defined as a set consisting of feasible solutions in each of which there exist no other feasible solutions that will yield an improvement in one objective without causing degradation in at least one other objective. The Pareto optimum solution set such as shown in Figure 4.4 is a set of candidate solutions from which the optimum solution is selected. The line (or, when there are three objective functions, the curved surface) is useful because it clearly shows the features of the solutions from a broad point of view [2–5]. Designers usually seek solutions in the direction of the large arrow located in the feasible region.

Looking at the design solutions at points A, B, and C on the Pareto optimum solution line PQ, we see that the design solution at point A provides excellent product performance, but at a very high manufacturing cost. The design solution at point C has a low manufacturing cost, but inferior product

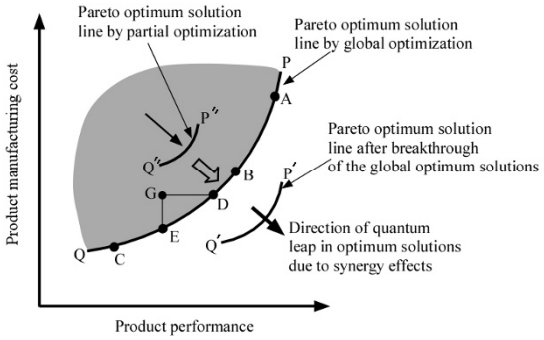


Figure 4.4. Conflicting relationships between a product performance characteristic and manufacturing cost

performance, and the design solution at point B offers rather good product performance and also a reasonable manufacturing cost. The solution actually used will be selected according to the customer's preference and priorities.

Designers generally look for practical design solutions on the Pareto optimum solution line. A global solution on the PQ line is difficult to obtain by the accumulation of partial optimizations that, for example, would yield solutions on the P"Q" line located within the feasible region, but rather far from the Pareto optimum solution line where the best solutions are located. For example, solution point G inside the feasible design region is inferior to any solution on solution line DE, and thus should not be selected as a design solution.

The foregoing discussion illustrates that searching for design solutions that lie on the global Pareto optimum solution line is an important part of practical product design and manufacturing. Given the competitive nature of the marketplace, it is obvious that companies making more preferable products that offer better value will usually gain market share. Obtaining Pareto optimum solutions that are superior in the global sense is therefore often of crucial importance in the development of successful product designs.

The display of a Pareto optimum solution set such as shown in Figure 4.4 is useful not only because it displays specific solutions, but also because a range of candidate optimum solutions on the PQ line can be visually and quantitatively understood. By looking at the whole Pareto optimum line, the relationships between the conflicting objective functions can be clearly recognized and compared. While accurately judging the worth of a single solution in isolation is impossible, the quality of specific available solutions can be judged and verified by the relative comparison of a set of candidate solutions.

In optimizations for product manufacturing, the initial focus is on obtaining solutions such those lying on the PQ line shown in Figure 4.4, which are termed the global optimum solutions. After such solutions are obtained, it is usually necessary to search for even better solutions, such as those lying on the P'Q' line, which represent important breakthroughs, beyond the PQ line. Given marketplace competition, there is significant pressure driving the evolution of product design solutions and product manufacturing techniques, and a currently successful product may rapidly lose its appeal due to the introduction of more sophisticated products that offer better customer value. The satisfaction levels of increasingly knowledgeable and sophisticated customers can only be met by continual improvements in product design and manufacturing.

4.5 Strategies of Advanced Product Design Optimization

Optimization methods and related technologies have been applied to many stages of product manufacturing. The levels at which such techniques can be applied have become increasingly broad, as shown in Figure 4.5. The accumulation of incremental improvements of parts, which can yield progressively better products over time, can now be augmented by optimizations of wider scope that extend beyond individual fields, or set of multidisciplinary fields, all the way to global optimizations.

Prior to the development of optimization techniques, incremental improvements were discovered through trial and error, and implemented at various stages of the design and manufacturing process. The accumulation of partial improvements over time ultimately led to quite profound advancements in the efficiency and quality of product designs and manufacturing.

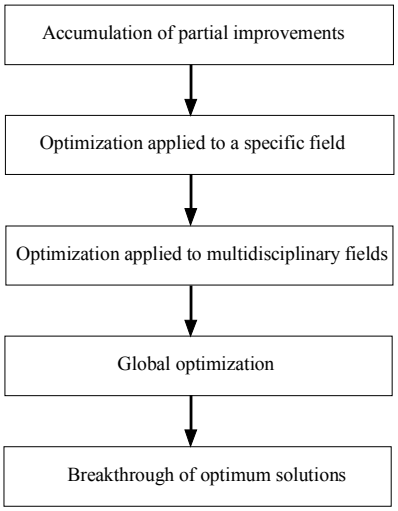


Figure 4.5. Developmental progress in optimization techniques applied to industrial activities

However, it became obvious that accumulations of partial improvements, and the results of trial and error processes, were inefficient and unlikely to bring about the best design solutions. The need to find more preferable schemes for the design and production of consumer products, and the industrial machines that manufacture them, made the utility of optimization techniques increasingly attractive. Thus, optimization techniques were partially applied in manufacturing areas under the direction and control of individual engineers.

As optimization techniques evolved, it became clear that decision-making factors in a specific field often affect, and are affected by, other fields, which gradually lead to the adoption of optimization techniques capable of handling broader scenarios, such as those that include a number of related fields. This type of optimization is generally called multidisciplinary optimization. Recently, it has been recognized that even optimum solutions for a set of multidisciplinary fields are not broad enough, so the importance of global optimization techniques is frequently discussed.

Multidisciplinary optimization (MDO) research has been carried out since the beginning of the 1980s, most notably with numerous applications for complex aeronautical design problems having a large number of design variables and criteria. In 1982, Sobieski [6], one of the pioneer MDO researchers, presented a method in which a complex design problem was decomposed into simpler sub-problems, each having a smaller number of design variables. This is assumed to mark the start of MDO research, and subsequent research efforts have focused on methods for decomposing large-scale systems and hierarchically expressing the resulting sub-problems.

Bloebaum *et al.* [7] decomposed large-scale systems by using a design structure matrix (DSM) that Steward [8] had proposed in 1981. In 1987, Kusiak *et al*. [9] proposed an optimization method whereby a system is decomposed by applying group technology to MDO, and the relationship between the design variables and criteria is expressed via a matrix [10].

Papalambros *et al.* [11] decomposed a large-scale system using Kusiak's research concepts, expressing the relations between the design variables and criteria via an overall matrix, and then extracting design variables common to the global problem. Papalambros' optimization method was later improved so that the system could be decomposed using graphical representations [12].

Recently, a variety of advanced decomposition methods for efficiently obtaining design solutions have been presented. The target cascading method for product development proposed by Papalambros [13] is a systematic means for consistently and efficiently propagating the desired top-level system design targets to appropriate subsystem and component specifications. The bi-level integrated system synthesis (BLISS) method proposed by Sobieski applies decomposition to the optimization of engineering systems, where system level optimization, which has relatively few design variables, is separated from potentially numerous subsystem optimizations that may each have a large number of local design variables [14].

Collaborative optimization is also a two-level optimization method specifically created for large-scale distributed-analysis applications [15]. Braun presented a collaborative architecture in a multi-disciplinary design environment, using a launch vehicle as an example [16].

Another useful method incorporating decomposition for optimization of machine product designs having hierarchical design variables is the hierarchical genetic algorithm proposed by Yoshimura and Izui [17, 18]. The decomposition-based assembly synthesis method proposed by Saitou also uses a systematic decomposition process as a tool [19]. A hierarchical multi-objective optimization method based on decomposition of characteristics and extraction of simpler characteristics has been proposed to address the importance of clarifying the conflicting relationships occurring between related characteristics in complex product design optimization problems [20].

4.5.1 Significance of Concurrent Optimization

Products are conventionally put on the market using the following manufacturing sequence: (1) research and development, (2) product design, (3) manufacturing, and then (4) marketing. Within a company, each of these operations usually corresponds to a single division, and within each division, particular decisions are made according to information received from upstream divisions. The decisions taken in upper divisions to implement various requirements and details therefore become constraints with respect to decision-making in downstream divisions. For example, attempting to reduce manufacturing costs after the details of a product design have already been decided will likely prove ineffective since it is the product design itself that largely determines the manufacturing cost. In a rigidly sequential manufacturing flow, cost reductions can seldom be implemented after the product design phase, such as at the process design stage when manufacturing methods and details are determined. Conflicting requirements may exist among divisions but these cannot be resolved due to the sequential manufacturing flow. Furthermore, a strictly chronological approach to product design and production is especially ill-suited to current merchandising trends where rapid product turnover and time to market are cardinal concerns.

When concurrent engineering principles are applied, the decision-making pertaining to product design and manufacturing factors is cooperatively performed, simultaneously and concurrently [21]. Concurrent engineering therefore means that all divisions work together cooperatively and at the same time, to make decisions concerning a range of factors before determining product details, a task that is facilitated by the use of computer networks. Competitive requirements, conflicting factors pertaining to different divisions, and trade-off relationships among product characteristics can all be appropriately resolved, and an enterprise atmosphere of mutual understanding and improved cooperation can be realized. Concurrent engineering has philosophical similarities with CIM (computer-integrated manufacturing) [22] from the standpoint of "integration" but the former emphasizes simultaneous and concurrent decision making in the early production stage.

To realize the potential benefits of concurrent engineering, the use of various optimization technologies is indispensable. Figure 4.6 shows the fundamental flow used when applying the concept of concurrent engineering to product designs. First, a wide range of evaluative factors and decision/design variables are gathered, according to experience. Next, the relationships between the evaluative factors are systematically analyzed and then suitable optimization procedures for obtaining the global optimum solution are constructed. Optimization based on the concept of concurrent engineering is here called concurrent optimization.

The products manufactured by various makers are bought by consumers who then use and maintain them when necessary, until they cease to

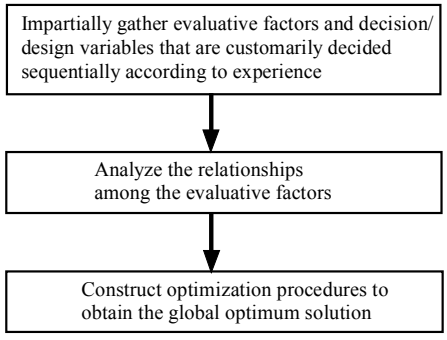


Figure 4.6. Fundamental flow in preparation for executing concurrent optimization

be useful. At that time, certain product parts and materials can, in certain cases, be reused or recycled, while the remainder is disposed of. This flow of products from creation, through use, repair, reuse, recycling and disposal, forms what is called a product's lifecycle. To achieve optimal product designs, all factors and items pertaining to a product's lifecycle should be fully considered at the earliest possible product design stage. That is, as the concept is shown in Figure 4.7, the full range of factors concerning a product's lifecycle, such as the manufacturing and purchase of machine components, the assembly, use, maintenance, disassembly, disposal, material recycling, and reuse of parts and materials, should all be concurrently considered and optimized from the initial design proposal stage.

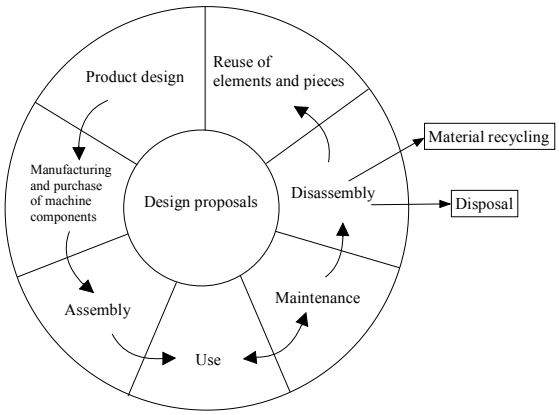


Figure 4.7. Conceptual diagram of lifecycle design

During the course of a product's lifecycle, many kinds of inconvenience may occur. Some of these undesirable outcomes affect the consumer's ability to use the product or derive the expected degree of satisfaction from it, while others may affect the environment in which the product is used, or the environment at large. If the steps required to mitigate these unwelcome circumstances are considered only when they occur, the potential for implementing the best possible solution or improvement will be clearly inferior to the outcome if such scenarios were considered at the early design stage of the product.

4.5.2 Fundamental Strategies of Design Optimization

Optimization methods based on mathematical programming methods and genetic algorithms have been widely developed and employed [23]. However, even though obtaining solutions for problems formulated as an optimization problem is often easy, judging the quality of the results in practical contexts is often difficult. In studies of practical methods for obtaining solutions to complex optimization problems, the response surface method based on the design of experiments has received much recent attention.

One of the troublesome aspects of current complex optimizations for product designs is that many local optimum solutions exist in the feasible design space. In many cases, obtaining the global optimum solution remains quite difficult, and optimization methods that simply and mechanically apply common optimization procedures seldom yield useful results for practical problems. However, by concentrating on the formulation of the optimization problem and by developing specific strategies to solve complex problems, practical optimization techniques and truly optimal results can be achieved, as will be explained below.

One of the most important points in the practical application of useful optimization methods is to formulate the problem being regarded while comprehensively including all available engineering knowledge and experiences, and to then carefully evaluate the obtained results.

The essential features that advanced and effective product design optimization methods should incorporate are as follows:

(1) Support design decision-making from the conceptual design stage.
(2) Facilitate detailed understanding and evaluation of exactly how the global optimum solution was obtained.
(3) Enable precise judgment concerning the validity of the obtained optimum solution.
(4) Support generation of novel and especially relevant ideas that lead to more preferable solutions.

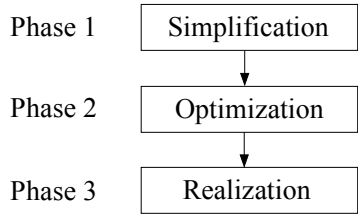


Figure 4.8. Multiphase design optimization procedures based on simplification of design models

Optimum design methods are often applied to the improvement of detailed designs, but this implies that the optimization starts from states where the most of the important design decisions have been already been made. In order to obtain more preferable design solutions, optimization methods should begin from a state where the range of design possibilities is as broad as possible, namely from the conceptual design stage. A method focusing on the fulfillment of requirement (1) above uses multiphase design optimization procedures based on the simplification of structural models, as shown in Figure 4.8 [24, 25].

In the first phase, the simplification process, a simplified mathematical or simulation model is constructed that has structural characteristics equivalent to the practical machine structure being considered. A complete, but simplified structural model that includes simplified structural models of parts and joints is constructed. In the second phase, an optimization procedure is conducted for the entire structural model. In the third and last phase, realization, practical detailed designs for each structural member and joint are determined from a wide range of possible alternatives, to most closely meet the specifications obtained in the second phase.

Solutions to goals (2), (3), and (4) above can be obtained by using a hierarchical multiobjective optimization method. In general, when requirements for a given performance characteristic can be realized without the presence of trade-off relationships with the other characteristics, the optimization problem is a simple one where the optimum solution can be easily obtained. The obtained solution is, in such cases, often quite similar to what can be achieved when relying on the experience and intuition of a decision maker. However, when conflicting relationships exist among the performance characteristics, and those characteristics have complex interrelationships, optimization problems become complicated and finding the optimum solution is far from easy. Optimizations for product designs are almost always of this type, where there are conflicting relationships among characteristics, but multiobjective optimization methods can be successfully applied to such problems.

4.6 Methodologies and Procedures for Product Design Optimization

Machine products have functions that are designed to accomplish specific tasks, jobs that are performed by the movement and operation of certain parts of the machine. During design, the operational accuracies and the time taken to complete specific jobs are evaluated so that the overall product efficiency can be considered. Here, the accuracy and efficiency are concurrently evaluated and higher values of both are generally more preferable, while it is desirable to minimize the operational energy used to accomplish the desired jobs that the product is designed to carry out. The product manufacturing cost is always to be minimized in actual manufacturing.

Each original performance characteristic is usually very complicated, since it is expressed as compounds or additions of various other component characteristics. The optimum design solutions for each of the original performance characteristics are generally different from each other, meaning that such performance characteristics have conflicting interrelationships, which is a proximate cause of the difficulty of obtaining globally optimal solutions.

To clarify the interrelationships among characteristics, they are examined so that their expression and composition, as well as their dynamic behavior and mathematical expression, can all be succinctly expressed in the context of the optimization problem at hand. For example, machine accuracies are often expressed by static and/or dynamic displacements at specific points that are determined according to the objective of

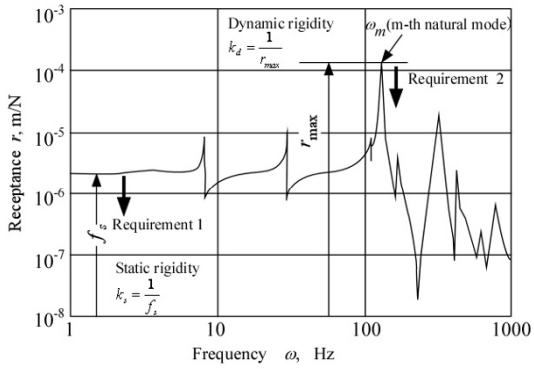


Figure 4.9. An example of frequency response at the cutting point of a machine-tool structure

specific jobs. Similarly, static rigidities can be used to evaluate the static displacements, and dynamic rigidities are used when evaluating the dynamic displacements. In general, machine products can be classified into those for which static rigidities alone are evaluated, and those for which dynamic rigidities are also evaluated. Since machine products carry out their jobs by the movement and operation of various parts, it is usually necessary to evaluate and optimize dynamic rigidities as well as static rigidities.

Figure 4.9 shows an example of the frequency response at a specific point of the machine (the cutting point in the case of machine tools, the end-effector point in the case of industrial robots, *etc*.). The receptance frequency response is expressed as follows:

$$r(\omega) = \frac{X}{F}(\omega) = \sum_{m=1}^{\infty} \left[\frac{f_m}{1 - (\frac{\omega}{\omega_m})^2 + 2j(\frac{\omega}{\omega_m})\varsigma_m} \right] \quad (4.4)$$

The static rigidity k_s is obtained using the reciprocal of the static compliance f_s, while the dynamic rigidity k_d is obtained using the reciprocal of the maximum receptance value $r_{\max}$ over the whole frequency range.

When the frequency ω is set to 0 in (4.4), the following simple relationship between f_s and modal flexibility f_m is established [26, 27].

$$f_S = \sum_{m=1}^{\infty} f_m \quad . \quad (4.5)$$

Both f_s and f_m have positive values. The modal flexibility f_m $(m = 1,2,...,\infty)$ expresses the distributed magnitude of the static compliance f_s for each natural mode. Equation (4.5) indicates that minimizing the static compliance f_s, which is equivalent to maximizing the static rigidity, reduces the modal flexibility at the natural mode where the modal flexibility value is highest.

In machine structures, vibration damping is most pronounced at joint interfaces, be they bolted or sliding. The consequences of damping effects can generally be controlled by carrying out detailed adjustments of joint parameters during the detailed design stage. When structural member rigidities are maximized, increasing the damping effects at the joints becomes easier [27]. The damping ratio ζ_m has a different value at each natural mode. The material damping ratios and the damping ratios for machine elements or parts vary according to the material properties, shapes and other parameters, however the damping ratio for the machine structure as a whole, despite the inclusion of many joints, often has a specific value or lies within a rather narrow range of values. Such values are often defined by experimental studies, and here the damping ratio is given as a specific constant value of ς for the initial stages of the design optimization.

The dynamic rigidity k_d is approximately expressed by the static rigidity k_s and the damping ratio ς as follows:

$$k_d = \frac{1}{r_{\max}} \cong \frac{2\zeta}{af_s} = \frac{2k_s\zeta}{a} \quad , \quad (4.6)$$

where a is assumed to be a constant value, such as 0.7. Examination of the related characteristics yields the result that increasing the static rigidity k_s increases the dynamic rigidity k_d.

In light of the above, it is clear that optimization of the static rigidity should have priority over optimization of the dynamic rigidity.

Practical procedures are explained with applied examples. Figure 4.10 shows a framework model of a machine tool composed of structural members and joints. The performance characteristics to be considered are the static and dynamic rigidities at the cutting point and the manufacturing cost of the

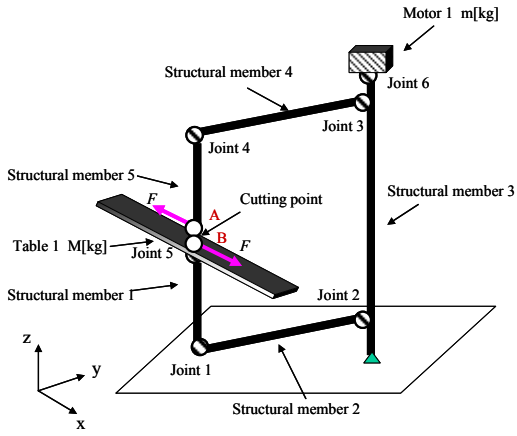


Figure 4.10. Framework model of a milling machine

machine tool. The static rigidity k_s is the reciprocal of the static compliance f_s between points A and B at the cutting point, which is obtained as X/F where X is the relative displacement between A and B, and F is the cutting force at points A and B. The dynamic rigidity k_d, *i.e.*, the reciprocal of the maximum receptance value $r_{\max}$ of the frequency response curve, is obtained from the frequency response curve.

The objective functions are the maximum receptance value and the machine's manufacturing cost C_T, each of which should be minimized. The formulation of $r_{\max}$ is simplified as shown in (4.6). Then, the characteristic of the maximum receptance value $r_{\max}$ is decomposed into two characteristics, namely the static compliance f_s and the damping ratio ς. The manufacturing cost C_T is decomposed into the material cost C_M of the structural members and the machining cost C_J of the joints

The optimization procedures carried out during the hierarchical multiobjective optimization [20] are as follows:

Step 1: The multiobjective optimization problem for the static rigidity k_M and the total structural weight W_s of the structural members on the static force loop is solved and a Pareto optimum solution set of cross-sectional dimensions is obtained. The structural model used for the structural analysis is shown in Figure 4.11, where only structural members on the static force loop are indicated, and each joint is treated as a rigid joint for the purposes of simplicity. The design variables are the cross-sectional dimensions of each structural member.

Step 2: The Pareto optimum solution line between the static rigidity k_M of the structural members and the material cost C_M of the structural members is obtained. The material cost C_M is calculated by multiplying the material cost per unit weight by W_s.

Step 3: The multiobjective optimization problem is solved for the total joint rigidities k_J on the static force loop and the machining cost C_J of the joints. The structural model used for the structural analysis is shown in Figure 4.11, where each joint is now treated as a flexible joint modeled as a spring, and the maximum surface roughness of the contact surface is included in the design variables. The results of the cross-sectional dimensions obtained in Step 1 are used as initial design variables. In this optimization, the relationships between the surface roughness $R_{\max}$ and the machining cost C_u per unit contact surface, shown in Figure 4.12, are used, where three kinds of machining methods, namely, milling, grinding, and super finishing, are considered. The joint rigidities are calculated according to their surface roughness values and contact surface areas [25].

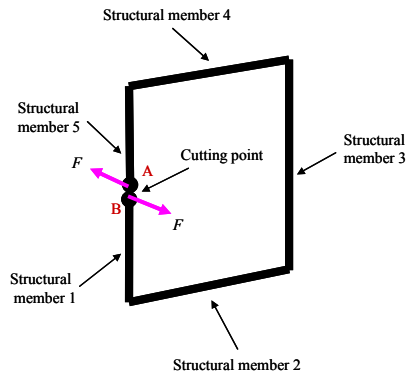


Figure 4.11. Structural model of the static force loop

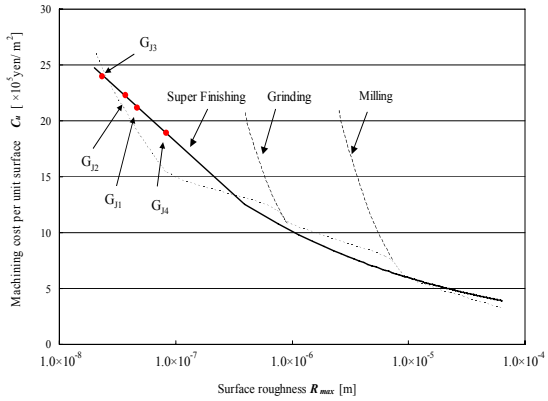


Figure 4.12. Relations between surface roughness and machining cost per unit contact area

Step 4: The multiobjective optimization problem is solved for the static compliance f_s (the reciprocal of the static rigidity k_s) and the total manufacturing cost C_T of the structural members on the static force loop, which is the sum of the material cost C_M and the machining cost C_J of the joints, and a Pareto optimum solution set is obtained.

Step 5: The multiobjective optimization problem for the maximum receptance value $r_{\max}$ and the total manufacturing cost C_T is solved and a Pareto optimum solution set is obtained. The structural model now used is shown in Figure 4.10, where each joint is modeled as a flexible joint and the maximum surface roughness of the contact surface is included in the design variables. The results of the cross-sectional dimensions and spring stiffnesses obtained in Step 2 are used as initial design variables.

Figure 4.13, the Step 1 result, shows the Pareto optimum solution set line between the static rigidity k_M and the total structural weight W_s of the structural members on the static force loop. Figure 4.14, the Step 4 result, shows the Pareto optimum solution set line between the static compliance f_s and the total manufacturing cost C_T .

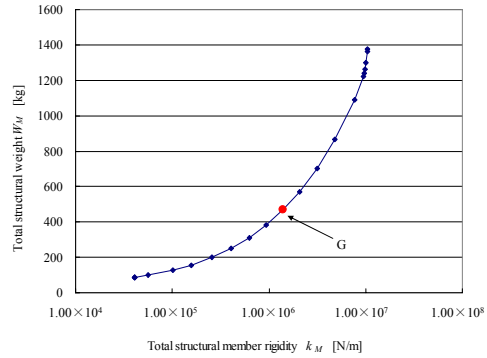


Figure 4.13. Pareto optimum solution line for Step1

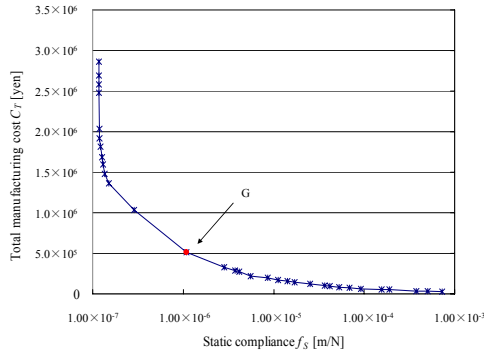


Figure 4.14. Pareto optimum solution line for Step 4

Figure 4.15, the Step 5 result, shows the Pareto optimum solution set line between the maximum receptance $r_{\max}$ and the total manufacturing cost C_T . To demonstrate the effectiveness of the proposed method, the obtained results are compared with those achieved by a conventional method, where the performance characteristics (objective functions at Step 5) are directly optimized using the feasible direction method but without using the proposed hierarchical optimization procedures. These are shown with ◆ symbols in Figure 4.15, while the results obtained by the proposed method are shown with ∗ symbols. The Pareto optimum solution line is shown by the thin line, which indicates the optimum solution frontier. The results show that proposed method obtains more preferable solutions, and does so more reliably.

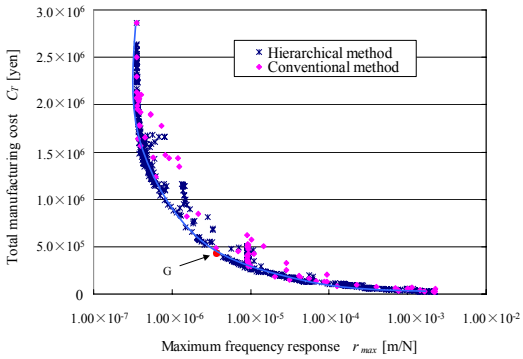


Figure 4.15. Pareto optimum solutions for Step 5

In the method explained above, the final global optimum solution can be analyzed and understood in terms of the interrelationships between correlated solution points existing in the final and first hierarchical levels, or in intermediate levels. The validity of the obtained design solutions, and their fitness for particular purposes, can therefore be more effectively evaluated. With point G selected on the Pareto optimum solution line in Figure 4.15, corresponding solution points on the Pareto optimum solution lines in Figures 4.13 and 4.14 are also indicated by points labeled G. At each corresponding point, the detailed values of the design variables and the characteristics can be examined, enabling a deeper understanding of the solution contents. For example, points G_{Jx}, with x corresponding to the joint number, are shown in Figure 4.12 and they indicate the solution's recommended machining method. The design solution corresponding to points G_{J1}, G_{J2}, G_{J3} and G_{J4} for joints 1, 2, 3 and 4, respectively, are illustrated, and it can be seen that super finishing machining is indicated for these particular joints. Furthermore, useful comparisons of several design solutions on the Pareto optimum solution line at the final stage can be conducted by going back to earlier optimization stages, enabling more detailed examinations of the optimum solutions.

Because the relationships between the optimum solution at the final hierarchical level and solutions at the topmost level are exposed and can be easily understood, examination of the features of characteristics at the lowest level, which are usually very simple, can often lead to further effective ways of improving these characteristics and, ultimately, the overall fitness of the final product design. That is, the techniques listed in Section 4.5.2 above more effectively support the generation of further ideas for improving tentative design solutions, and facilitate more rapid examination of the resulting improvement levels. For example, it may be advantageous to use a new material for a structural member, and the validity and utility of doing so can be readily evaluated using the Pareto optimum solutions obtained during earlier optimization stages.

4.7 Design Optimization for Creativity and Balance in Product Manufacturing

An important goal of product manufacturing is to design and manufacture products that, as far as possible, are in harmony with the environment, climate, nature, and culture where the products are used, in addition to satisfying personal preferences and tastes. This, and other goals, can be achieved by systematically considering a range of evaluative factors. Many industries are starting to realize that their long-term success depends on addressing factors beyond the design of products that merely satisfy minimum requirements in isolation. As shown in Figure 4.16, for industries to truly flourish, product manufacturers must be aware of the cultural impact of their products, and strive to achieve balanced approaches that address broader issues pertaining to natural environments, climate, and the personality of those who purchase and use

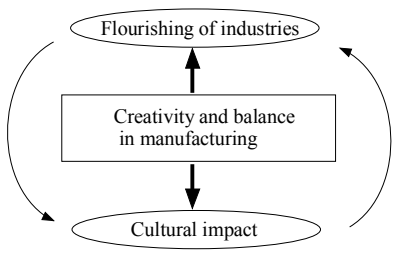


Figure 4.16. Conceptual diagram of the relationship between creativity and balance in manufacturing, and cultural impact and flourishing of industries

their products, so that customer satisfaction can be truly maximized.

Diversification in product manufacturing can increase the personal satisfaction of customers, and drive the creation of new products that better cope with a variety of local environments. The application of optimization techniques to product designs is important not simply from the standpoint of obtaining a single superior design solution, but because such techniques can provide a useful variety of design solutions. Using this variety, the most appropriate global solution can be selected from a number of alternative solutions, according to detailed requirements pertaining to specific products in specific locations and times. Thus, optimization techniques can potentially play important roles in both creating products that deliver greater satisfaction levels, and in manufacturing products that achieve greater harmony with their surroundings, by skillfully considering a broader range of factors.

4.8 Conclusions

Since a great deal of human activity is related in some way to product manufacturing, it directly affects the growth and survival of economic entities at all scales, while offering potential improvements in the satisfaction levels of people around the world. To achieve truly sustainable product manufacturing, its impact on gobal environments and ecologies, as well as the depletion of natural resources, must be given the attention that these pressing concerns deserve. Also of primary concern is the psychology of the people whose lives are affected by the manufacturing and use of mainstream as well as novel and improved products that aim to make our lives easier, more comfortable or more worthwhile. The use of advanced optimization technologies during product design processes is practically indispensable if these goals are to be met.

In the beginning of this chapter, progressive product design circumstances were explained, and the importance of clarifying product design criteria when seeking to develop more preferable product designs was emphasized. Next, the principal criteria for product designs were described, along with the problem of related criteria that often have complicated conflicting interrelationships. Then, to cope with the multitude of features that needs to be addressed, product optimization details and the use of multiobjective Pareto optimum solutions were explained. Concurrent engineering concepts for obtaining superior product designs were discussed next, and then fundamental strategies of product design optimizations were described. Product design optimization methodologies were explained using a practical machine-tool example. Product manufacturing is directly related to the flourishing of a wide range of industries. Since these industries also exercise considerable cultural impact, finally, their flourishing, as they recognize and respond to the global and interrelated nature of their environmental and cultural impact, was mentioned in terms of the need for increasingly sophisticated and practical product design optimization methods and strategies.

References

[1] Eschenauer H, Koski, J, Osyczka A. (editors). Multicriteria design optimization. Springer, Berlin, 1990.

[2] Yoshimura M. Integrated optimization of product design and manufacturing, control and dynamic systems – manufacturing and automation systems: techniques and technologies (Leondes CT). Academic Press, New York, 1991; 48 (Part. 4 of 5), 167–219.

[3] Yoshimura M. Concurrent optimization of product design and manufacture, concurrent engineering – contemporary issues and modern design tools. Parsaei HR, Sullivan WG (editors). Chapman and Hall, London, 1993; (Chapter 9), 159–183.

[4] Yoshimura M. Concurrent product design and manufacturing, control and dynamic systems – concurrent engineering techniques and applications. Leondes CT (editor). Academic Press, New York, 1994; 62, 89–127.

[5] Yoshimura M. System design optimization for product manufacturing. International Journal of Concurrent Engineering: Research and Applications 2007; Dec., 15(4):329–343.

[6] Sobieski J. A linear decomposition method for optimization problems–blueprint for development, NASA Technical Memo 1982; 832.

[7] McCulley C, Bloebaum CL. Ordering design tasks based on coupling strengths. American Institute of Aeronautics and Astronautics (AIAA-94-4326), 1984; 708-717.
[8] Steward DV. The design structure system: a method for managing the design of complex systems, IEEE Trans. on Engineering Management 1981; 28(3):71–74.
[9] Kusiak A, Chow WS. Efficient solving of the group technology problem. Journal of Manufacturing Systems 1987; 6(2):117–124.
[10] Kusiak A, Wang J. Decomposition of the design process. Trans. of the ASME Journal of Mechanical Design 1993; 115:687–694.
[11] Wagner TC, Papalambros PY. A general framework for decomposition analysis in optimal design. In: Gilmore BJ (editor). Advances in design automation. ASME, New York, 1993; 2:315–325.
[12] Michelena NF, Papalambros PY. A hypergraph framework for optimal model-based decomposition of design problems. Computational Optimization and Applications 1997; 8(2):173–196.
[13] Kim HM, Rideout DG, Papalambros PY, Stein JL. Analytical target cascading in automotive vehicle design. Trans. of ASME, Journal of Mechanical Design 2003; 125(3):481–489.
[14] Sobieszczanski-Sobieski J, Altus TD, Phillips M, Sandusky R. Bilevel. Integrated system synthesis for concurrent and distributed processing. AIAA Journal 2003; 41(10):1996–2003.
[15] Tappeta RV, Renaud JE. Multiobjective collaborative optimization. Transaction of ASME, Journal of Mechanical Design 1997; 119(3):403–411.
[16] Braun RD, Kroo IM. Development and application of the collaborative optimization architecture in a multidisciplinary design environment. Multidisciplinary design optimization: state-of-the-art, Alexandrov N, Hussaini MY (editors), Proceedings in Applied Mathematics, SIAM, Philadelphia 1995; 80.
[17] Yoshimura M, Izui K. Smart optimization of machine systems using hierarchical genotype representations. Trans. of ASME, Journal of Mechanical Design 2002; 124(3):375–384.
[18] Yoshimura M, Izui, K. Hierarchical parallel processes of genetic algorithms for design optimization of large-scale products, Trans. of ASME, Journal of Mechanical Design 2004;126(2):217–224.
[19] Cetin OL, Saitou K. Decomposition-based assembly synthesis for maximum structural strength and modularity. Trans. of ASME, Journal of Mechanical Design 2004; 126(1):244–253.
[20] Yoshimura M, Taniguchi M, Izui K, Nishiwaki S. Hierarchical arrangement of characteristics in product design optimization. ASME Journal of Mechanical Design 2006; 128:701–709.
[21] Yoshimura M, Itani K, Hitomi K. Integrated optimization of machine product design and process design. International Journal of Production Research 1989; 27(8):1241–1256.
[22] Harrington J. Computer integrated manufacturing. Industrial Press, New York, 1973.
[23] Arora S. Introduction to optimum design (Second Edition). Elsevier, Amsterdam, 2004.
[24] Yoshimura M,.Hamada T, Yura K, Hitomi K. Design optimization of machine-tool structures with respect to dynamic characteristics. Trans. of the ASME, Journal of Mechanisms, Transmissions, and Automation in Design 1983; March, 105(1):88–96.
[25] Yoshimura M, Takeuchi Y, Hitomi K. Design optimization of machine-tool structures considering manufacturing cost, accuracy and productivity. Transactions of the ASME, Journal of Mechanisms, Transmissions, and Automation in Design 1984; Dec., 106(4):531–537.
[26] Yoshimura M. Evaluation of forced and self-excited vibrations at the design stage of machine-tool structures. Trans. of the ASME, Journal of Mechanisms, Transmissions, and Automation in Design 1986; Sept., 108(3):323–329.
[27] Yoshimura M. Design optimization of machine-tool dynamics based on clarification of competitive-cooperative relationships between characteristics. Transactions of the ASME, Journal of Mechanisms, Transmissions, and Automation in Design 1987; March, 109(1):143–150.

5

Constructing a Product Design for the Environment Process

Daniel P. Fitzgerald[1], Jeffrey W. Herrmann[1], Peter A. Sandborn[1], Linda C. Schmidt[1] and Thornton H. Gogoll[2]

[1]University of Maryland in College Park, Maryland, USA
[2]Black & Decker in Towson, Maryland, USA

Abstract: The greatest opportunity to reduce the environmental impact of a new product occurs during the design phase of its life cycle. Design for environment (DfE) tools, when implemented, become part of the product development process. Often, however, the DfE tools are isolated from the other activities that comprise the product development process. To avoid this problem, tools must be situated in a DfE process that describes how the DfE tools will be used and links DfE activities with the rest of the product development process. This paper presents an innovative DfE process that is being incorporated into an existing product development process at a leading power tool manufacturing company, The Black & Decker Corporation. The DfE process includes DfE tools and activities that are specifically designed to help Black & Decker achieve their environmental objectives.

5.1 Introduction

Environmentally responsible product development (ERPD), also known as environmentally benign manufacturing, considers both environmental impacts and economic objectives during the numerous and diverse activities of product development and manufacturing. ERPD seeks to develop energy-efficient and environmentally benign products. Products generate environmental impacts throughout all stages (*i.e.* raw material extraction, manufacturing, assembly, distribution, and end of life) of their life cycle. There are many ways to minimize these environmental impacts. Studies demonstrate the greatest opportunity for ERPD occurs during the product design phases [1]. The decisions that are made during these phases determine most of the product's environmental impact. Although ERPD requires extra effort, it not only protects the environment but also provides a channel for the application of environmental policies determined at the corporate level.

Consequently, manufacturing companies have spent a great deal of effort developing tools to help designers create environmentally benign products. The two major classes of tools are life cycle assessment (LCA) [2] and design for environment (DfE) tools [3]. LCA provides a fundamental methodology that evaluates the environmental impact associated with a product during its complete life cycle. DfE tools are design decision support tools that help a designer reduce these impacts by improving the product design. DfE incorporates the consideration of national

regulations, human health and safety, hazardous material minimization, disassembly, recovery, recycling, and disposal into the design process.

Many obstacles to the effective use of LCA and DfE tools have been noted [1]. Two of the most significant obstacles are the difficulties acquiring the needed data and the challenges developing realistic, appropriate metrics of environmental impact. Consequently, LCA and DfE tools are, generally, not integrated with the other activities and tools used in the product development process. That is, the information flow and decision-making required for existing LCA and DfE tools to be effective is inconsistent with the information flow and decision-making present in product development organizations. The result is often a post-design, standalone, environmental review of a product.

However, manufacturing firms need a tool to consider environmental objectives during the design of new products. Especially urgent is the need to comply with an ever-increasing number of environmental regulations and customer demands. To overcome the limitations of standalone DfE tools, manufacturing firms need to consider important environmental objectives in a systematic way during the design process. This chapter describes such a DfE process for a leading worldwide power tool manufacturer, The Black & Decker Corporation. In close collaboration with Black & Decker, the authors have developed this DfE process. Black & Decker is now working to implement this process.

The development of this DfE process was advanced by considering the product development process as a decision-making system. The next section of this chapter elaborates on this perspective and desscribes a methodology for improving product development, which can be used to enhance any type of performability engineering. Section 5.3 presents an overview of Black & Decker's environmental objectives. Section 5.4 presents the specific product-level metrics that product development teams can evaluate and describes how they are relevant to Black & Decker's environmental objectives. Section 5.5 makes recommendations about the product development milestones when these metrics should be complete. Section 5.6 describes compares this innovative DfE process to traditional DfE and LCA tools. Section 5.7 concludes the chapter.

5.2 A Decision-making View of Product Development Processes

Product development is a complex and lengthy process of identifying a need, designing, manufacturing and delivering a solution, often in the form of a physical object, to the end-user. Product development is a difficult task made more difficult by the challenges inherent in complex, open-ended, and ill-defined tasks. A successful product development process incorporates information inputs from seemingly unrelated and remote areas of an organization into the decision-making process [4].

Due to their complexity, it is not surprising that a variety of perspectives is needed to understand product development processes. The task-based perspective view product development as a project of related tasks and emphasizes project management guidelines. Smith and Reinertsen [5] present an economic view of product development and stress the relationships between development time, development cost, unit cost, and product performance and the product's overall profitability.

5.2.1 Decision Production Systems

Building on both the decision-based perspective of engineering design and the decision-making paradigm of organizational design, Herrmann and Schmidt [6] argued that product development organizations are decision production systems and describe product development as an information flow governed by decision-makers who operate under time and budget constraints to produce new information. The term is relevant because a product development organization creates new product designs and other information that are the accumulated results of complex sequences of decisions. Herrmann and Schmidt [7] present a methodology for improving a product development organization. Herrmann [8] further explores the

concepts on which this view depends and considers their implications for designing product development processes.

The decision production system (DPS) perspective looks at the organization in which the product development process exists and considers the decision-makers and their information processing tools (like databases) as units of a manufacturing system that can be viewed separately from the organization structure. By viewing organizations in this manner, one can understand how information flows and who is making the key decisions. As a result the hierarchical view and decision production system view of a product development organization are quite different. Similarly, Simon [4] noted that an organization's "anatomy" for information processing and decision-making is naturally different than the departmentalization displayed in an organization chart. The greater the interdependence between decision-makers, the less the DPS will resemble an organization chart.

The DPS perspective is an overarching framework to map product development activities (with an emphasis on decisions) within an organization in such a way as to illustrate current decision-making practices. The DPS representation of a product development organization provides a meta-level view of the actual decision-making processes taking place in an organization, which are not necessarily the processes that management may have prescribed. The DPS perspective enables problem identification in decision-making practices that will lead to a more effective deployment of resources including decision support tools.

The DPS perspective enables a deeper understanding of the organization than typical hierarchical organization charts of a firm or Gantt charts of product development projects. Understanding the real process (as opposed to the corporate guide for the design process) is a key step in improving product development. Furthermore, recognizing design as a "knowledge agent" and the designing activity as a crucial organizational knowledge process can improve an organization's ability to innovate within their competitive environment [9]. The need for research on new work practices [10] and the need for developing new representation schemes for product development [11] are additional motivations for considering the DPS perspective.

5.2.2 Improving Product Development Processes

Simon [4] argues that systematic analysis of the decision-making in a product development process would be useful for implementing changes to the product development organization in a timely and profitable manner, and he proposes the following technique for designing an organization:

- Examine the decisions that are actually made, including the goals, knowledge, skills, and information needed to make those decisions.
- Create an organization pattern for the tasks that provide information for these decisions.
- Establish (or change) the pattern of who talks to whom, how often, and about what.

Of course, this must be repeated for the more specific decisions that form the more general decisions.

Viewing a product development organization as a decision-making system leads to a systems-level approach to improving product development. In particular, this perspective is not concerned primarily with formulating and solving a design optimization problem. Moreover, the problem is not viewed only as helping a single design engineer make better decisions (though this remains important). Instead, the problem is one of organizing the entire system of decision-making and information flow to improve the performability of the new products that are being developed.

As with other efforts to improve manufacturing operations or business processes, improving product development benefits from a systematic improvement methodology. The methodology presented here includes the following steps in a cycle of continuous improvement, which is based in part on ideas from Checkland [12].

1. Study the product development decision-making system.
2. Build, validate, and analyze one or more models of this decision-making system.
3. Identify feasible, desirable changes.
4. Implement the changes, evaluate them, and return to Step 1.

The important features of the decision-making system are the persons who participate in it, the decisions that are actually made, including the goals, knowledge, skills, and information needed to make those decisions. Also relevant are the processes used to gather and disseminate information. It will also be useful to study other processes that interact with product development, including marketing, regulatory compliance, manufacturing planning, and customer service.

An especially important part of studying product development is determining the sources that provide information to those making decisions. If they are not documented, changes to the system may eliminate access to these sources, which leads to worse decision-making. In addition, like any group of tools accumulated over time, it is critical to review how and when each decision support tool is applied to the product development process. This requires a meta-level understanding of decision-making during all phases of product development.

Modeling is a key feature of this methodology. Creating a model of the as-is product development organization has many benefits. Though it may be based on pre-existing descriptions of the formal product development process, it is not limited to describing the "should be" activities. The process of creating the model begins a conversation among those responsible for improving the organization. Each person involved has an incomplete view of the system, uses a different terminology, and brings different assumptions to the table. Through the modeling process, these persons develop a common language and a complete picture. Validation activities give other stakeholders an opportunity to give input and also to begin learning more about the system. Even those that are directly involved in product development benefit from the "you are here" information that a model provides. For more details about possible models, see Herrmann and Schmidt [7].

5.3 Environmental Objectives

Based on discussions with Black & Decker staff, such as the Director of Engineering Standards and the Senior Manager of Environmental Affairs, and documents provided by Black & Decker, we identified six primary environmental objectives based on the corporation's environmental policy:

1. Practice environmental stewardship.
2. Comply with environmental regulations.
3. Address customer concerns.
4. Mitigate environmental risks.
5. Limit financial liability.
6. Report environmental performance.

This section describes these in more detail.

5.3.1 Practice Environmental Stewardship

Black & Decker seeks to demonstrate environmental awareness through creating an environmental policy and publishing it on their website, including information about recycled content on packaging, and its Design for Environment program. In addition, Black & Decker belongs to environmental organizations such as the World Environmental Center, which contributes to sustainable development worldwide by strengthening industrial and urban environment, health, and safety policy and practices. It is also member of the Rechargeable Battery Recycling Corporation (RBRC) and RECHARGE which promote the recycling of rechargeable batteries.

5.3.2 Comply with Environmental Regulations

As a global corporation that manufactures, purchases, and sells goods, Black & Decker must comply with all applicable regulations of countries where its products are manufactured or sold. Currently, the European Union exerts significant influence on addressing environmental issues through regulations and directives. Listed below are examples of important US and European environmental regulations.

There are many regulations that apply to US and European workers and these are set by both

federal and state agencies. The Occupational Safety & Health Administration (OSHA) limits the concentration of certain chemicals to which workers may be exposed. The Environmental Protection Agency (EPA) regulates management of waste and emissions to the environment. Black & Decker provides employees with training on handling hazardous wastes, which is required by the Resource Conservation and Recovery Act and the Hazardous Materials Transportation Act [13]. California's Proposition 65 requires a warning before potentially exposing a consumer to chemicals known to the State of California to cause cancer or reproductive toxicity. The legislation explicitly lists chemicals known to cause cancer and reproductive toxicity.

The EU Battery Directive (91/157/EEC) places restrictions on the use of certain batteries. The EU Packaging Directive [14] seeks to prevent packaging waste by requiring packaging re-use and recycling. In the future, countries in the European Union will require Black & Decker to adhere to certain laws so that the state achieves the goals of the EU Packaging Directive. Thus, Black & Decker will be interested in increasing the recyclability of its packaging.

Black & Decker has also implemented procedures to comply with the Waste Electrical and Electronic Equipment Directive (WEEE). The following excerpt describing this directive is from the UK's Environmental Agency [15]: "The Directive is one of a series of 'producer responsibility' directives that makes producers of new equipment responsible for paying for the treatment and recycling of products at the end of their life. It affects any business that manufactures, brands or imports [electrical and electronic equipment (EEE)] as well as businesses that sell EEE or store, treat or dismantle WEEE within the EU. It will affect businesses that have WEEE to dispose of and the public who will have more opportunities to reuse, recycle and recover these products."

This regulation requires appropriate marking on EEE, sets targets for household WEEE collection, requires EU member states to register EEE producers, requires procedures to enable take-back and treatment, and sets targets for recycling and recovery.

5.3.3 Address Customer Concerns

Black & Decker's retail customers are concerned about the environmental impacts of the products they sell. Examples of customer concerns are: ensuring timber comes from appropriate forests, increasing the recyclability and recycled content in packaging, using cadmium in batteries, and using lead in printed wiring boards and electrical cords. More specifically, some retailers require that Black & Decker's products be free of lead-based surface coatings.

5.3.4 Mitigate Environmental Risks

An activity's environmental risk is the potential that the activity will adversely affect living organisms through its effluents, emissions, wastes, accidental chemical releases, energy use, and resource consumption [16]. Black & Decker seeks to mitigate environmental risks through monitoring chemical emissions from manufacturing plants, reducing waste produced by its operations, ensuring safe use of chemicals in the workplace, and ensuring proper off-site waste management.

5.3.5 Reduce Financial Liability

There are different types of environmental liabilities [17]:

- Compliance obligations are the costs of coming into compliance with laws and regulations.
- Remediation obligations are the costs of cleaning up pollution posing a risk to human health and the environment.
- Fines and penalties are the costs of being non-compliant.
- Compensation obligations are the costs of compensating "damages" suffered by individuals, their property, and businesses due to use or release of toxic substances or other pollutants.

- Punitive damages are the costs of environmental negligence.
- Natural resource damages are the costs of compensating damages to federal, state, local, foreign, or tribal land.

Some of these may be a concern to Black & Decker.

5.3.6 Reporting Environmental Performance

Black & Decker reports environmental performance to many different organizations with local, national or global influence and authority. An example of an organization is the Investor Responsibility Research Center (IRRC).

Consistent with its policy, Black & Decker's environmental objectives will evolve. New regulations will be promulgated in the years to come. Stakeholders will ask for additional environmental information. Black & Decker must be flexible enough to comply. The need for a DfE process that is robust and can adapt to the constantly changing nature of environmental regulations and requirements is great.

5.4 Product-level Environmental Metrics

Incorporating a DfE process that fits into the existing product development process has significant potential to help manufacturing firms achieve their environmental objectives. This section briefly describes eight product-level environmental metrics developed by the authors and Black & Decker staff that product development teams can evaluate during the product development process. These metrics were chosen because they relate directly to a particular product (they are not plant or corporate metrics). In addition, the measures concern attributes that are relevant to Black & Decker's primary environmental objectives, as described below.

5.4.1 Description of the Metrics

There are eight product-level environmental metrics, which the following paragraphs describe:

1. Flagged material use in product
2. Total product mass
3. Flagged material generated in the manufacturing process
4. Recyclability/disassembly rating
5. Disassembly time
6. Energy use
7. Innovation statement
8. Application of the DfE approach

Flagged Material Use in Product

This measures the mass of each flagged material contained in the product. A material is considered flagged if it is banned, restricted or being watched with respect to regulations or customers. A consulting firm has provided Black & Decker with a list of materials that are banned, restricted and being watched. This metric addresses the following corporate environmental objectives:

- Comply with environmental regulations.
- Address customer concerns.
- Limit financial liability.
- Report environmental performance.

Total Product/Packaging Mass

This measures the mass of the product and packaging separately. This metric addresses the following corporate environmental objectives:

- Comply with environmental regulations.
- Address customer concerns.
- Report environmental performance.

Flagged Material Generated in the Manufacturing Process

This is a list of each flagged material generated during the manufacturing process. A material is considered flagged if it is banned, restricted or being watched with respect to regulations or customers. This metric addresses the following corporate environmental objectives:

- Comply with environmental regulations.
- Address customer concerns.
- Mitigate environmental risks.
- Limit financial liability.
- Report environmental performance.

Recyclability/Disassembly Rating

This metric is the degree to which each component and subassembly in the product is recyclable. Recyclability and separability ratings can be calculated for each component based on qualitative rankings. Design engineers are provided with a list of statements that describe the degree to which a component is recyclable or separable and a value from 1 to 6 is associated with each statement. Low ratings for both recyclability and separability facilitate disassembly and recycling. The design engineer rates the recyclability and separability of each component, subassembly, and final assembly. If both ratings for an item are less than "3", than the item is recyclable [18].

This metric addresses the following corporate environmental objectives:

- Practice environmental stewardship.
- Comply with environmental regulations.
- Address customer concerns.
- Mitigate environmental risks.
- Report environmental performance.

Disassembly Time

A measure of the time it will take to disassemble the product. Research has been conducted on how long it typically takes to perform certain actions. Charts with estimates for typical disassembly actions are provided to the design engineers who can then estimate how long it would take to disassemble a product [18].

This metric addresses the following corporate environmental objectives:

- Practice environmental stewardship,
- Mitigate environmental risks.

Energy Consumption

The total expected energy usage of a product during its lifetime. This metric can be calculated by multiplying the total expected lifetime hours by the energy use per hour the product consumes. This metric need to be calculated only for large energy consumers such as compressors, generators, and battery chargers.

This metric addresses the following corporate environmental objectives:

- Practice environmental stewardship.
- Comply with environmental regulations.
- Address customer concerns.
- Mitigate environmental risks.
- Limit financial liability.

Innovation Statement

A brief paragraph describing the ways a product development team reduced the negative environmental impact of their product. The product development team should write this after the product is launched. All environmental aspects considered should be included as well.

This metric addresses the following corporate environmental objectives:

- Practice environmental stewardship.
- Report environmental performance.

Application of DfE approach

This binary measure (yes or no) is the answer to the following question: Did the product development team follow the DfE approach during the product development process? Following the DfE approach requires the team to review the DfE guidelines and evaluate the product-level environmental metrics.

This metric addresses the following corporate environmental objectives:

- Practice environmental stewardship.
- Report environmental performance.

While this list of metrics cannot completely measure every environmental impact, the metrics provide designers with a simple way to compare different designs on an environmental level. Black & Decker plans to track the trends of these metrics as the products advance through future redesigns. Furthermore, each product will have environmental targets set at the beginning of the project, and the metrics provide a way to track how well the product development team performed with respect

to attaining the targets. The Corporate Environmental Affairs group will also use the metrics to respond to retailers requests for environmental information.

5.4.2 Scorecard Model

A scorecard was created in Microsoft Excel in order to ensure that the metrics above could be used more effectively during the product development process. There is a single worksheet with inputs and outputs specifically related to most of the aforementioned metrics. Calculations for each metric are carried out on a hidden calculations worksheet. Separate worksheets contain the most important outputs from each metric and appropriate graphs. The following paragraphs list the specific inputs and outputs for each metric.

Flagged Material Use in Product:

Inputs: The components containing flagged material, mass of each component, flagged material contained within each component, percent of each component that is hazardous.
Outputs: The mass of each flagged material in each component, and the total mass of each flagged material within each product.

Total Product and Packaging Mass:

Inputs: Product weight and packaging weight.
Outputs: Product mass and packaging mass.

Flagged Material Generated in Manufacturing Process:

Inputs: Flagged material generated, manufacturing process, component being made.
Outputs: List of flagged materials generated for product.

Recyclability/Disassembly Rating:

Inputs: Assembly name, component name, quantity, material the component is made of, total mass, recyclability rating, separability rating.
Outputs: Total mass of product for each recyclability rating, total mass of product for each disassembly rating, pie charts for both sets of outputs, percent of the product that is recyclable, whether a particular component is recyclable.

Disassembly Time:

Inputs: Disassembly step, fastener used, removal method, time per fastener, number of jobs.
Outputs: Total time for each step, total time for disassembly.

Energy Consumption:

Inputs: Expected lifetime of the product, total power rating.
Outputs: Total energy used by product over lifetime.
The innovation statement and application of DfE approach metrics are not included in the spreadsheet because they do not involve numbers or calculations. The final output page highlights key environmental metrics and is calculated with the spreadsheet based on the designer inputs listed above. The key environmental metrics are: Amount of flagged material in product (g), total product mass and (g), number of manufacturing processes that generate flagged materials, percent product recyclable, total disassembly time (s), and total energy consumed (kJ).

5.4.3 Guidelines and Checklist Document

To ensure that design teams at Black & Decker address appropriate environmental concerns during the product development process, a guidelines and checklist document has been created. The checklist portion of the document lists items that must be addressed before the product is released to the market. The document contains references which are links to additional information about the requirements and guidelines. The guidelines section of the document lists issues that engineers should try to address to make the product more environmentally friendly. Not addressing an item in the guideline section would not prevent a product from going to the market however.

The Checklist of Regulatory and Policy Requirements contains the following requirements:

- No material restricted by Black & Decker is used in the product or manufacturing process.
- All materials restricted in the RoHS directive are under the respective threshold limit within the product.

- All special lead applications are under the respective threshold limit within the product.
- Product manual contains appropriate Proposition 65 warning if necessary.
- Packaging of product adheres to the European Packaging Directive.
- Batteries contain no materials banned in the European Union's battery directive.
- Product and manual contain appropriate markings for products with batteries.
- Product and manual contain appropriate markings for products with respect to the WEEE directive.
- Prohibited manufactured processes are not used.

The following are the Design for Environment Guidelines:

- Reduce the amount of flagged materials in the product by using materials not included on Black & Decker's should not use list.
- Reduce raw material used in product by eliminating or reducing components.
- Reduce the amount of flagged material released in manufacturing by choosing materials and processes that are less harmful.
- Increase the recyclability and separability of the product's components.
- Reduce the product's disassembly time.
- Reduce the amount of energy the product uses.

Samples of these documents can be found in Fitzgerald *et al*. [19].

5.5 The New DfE Process

Ideally, every product and process design decision should consider environmental concerns. However, this is not feasible because some designers are unfamiliar with DfE principles. Therefore, we defined a DfE process that naturally integrates environmental issues into the existing product development process with little extra effort or time. Black & Decker uses a stage-gate product development process that has eight stages. Every stage requires certain tasks to be completed before management signs off giving permission to proceed to the next stage. This signoff procedure is known as the gate.

Currently, Black & Decker has safety reviews during stages 2, 3, 4, and 6. Safety reviews are meetings intended for reviewers to evaluate the assessment, actions, and process of the design team in addressing product safety. The DfE process adds an environmental review to the agenda of the safety reviews held during Stages 2, 4, and 6. A separate environmental review will be held during Stage 3, an important design stage, in order to focus specifically on the environmental issues for the particular product. The environmental reviews will require design teams to review the checklist of key requirements and to consider guidelines for reducing environmental impact. When the DfE process is first implemented, design teams will have to fill out the Environmental Scorecard only during Stage 6 after the product design is complete. Doing this begins the process of recording environmental data and allows design teams to adapt gradually to the new process. When design teams become more familiar with the process, the scorecard will be completed two or more times during the stage-gate process in order to track design changes that effect environmental metrics during the development process.

In addition to the environmental reviews, environmental targets will be set during Stage 1 as goals for the new product. The design team will write a lessons learned summary during Stage 8 to highlight innovative environmental design changes. The lessons learned summary will provide the innovation statement metric. Figure 5.1 shows the Safety Review Process and Environmental Review Process running in parallel. The sections below discuss the aforementioned environmental activities in more detail. Note that, throughout this process, many other product development activities occur, causing changes to the product design.

5.5.1 Product Initiation Document

The Product Initiation document is a document that Black & Decker uses to benchmark competitors, define performance targets, and predict

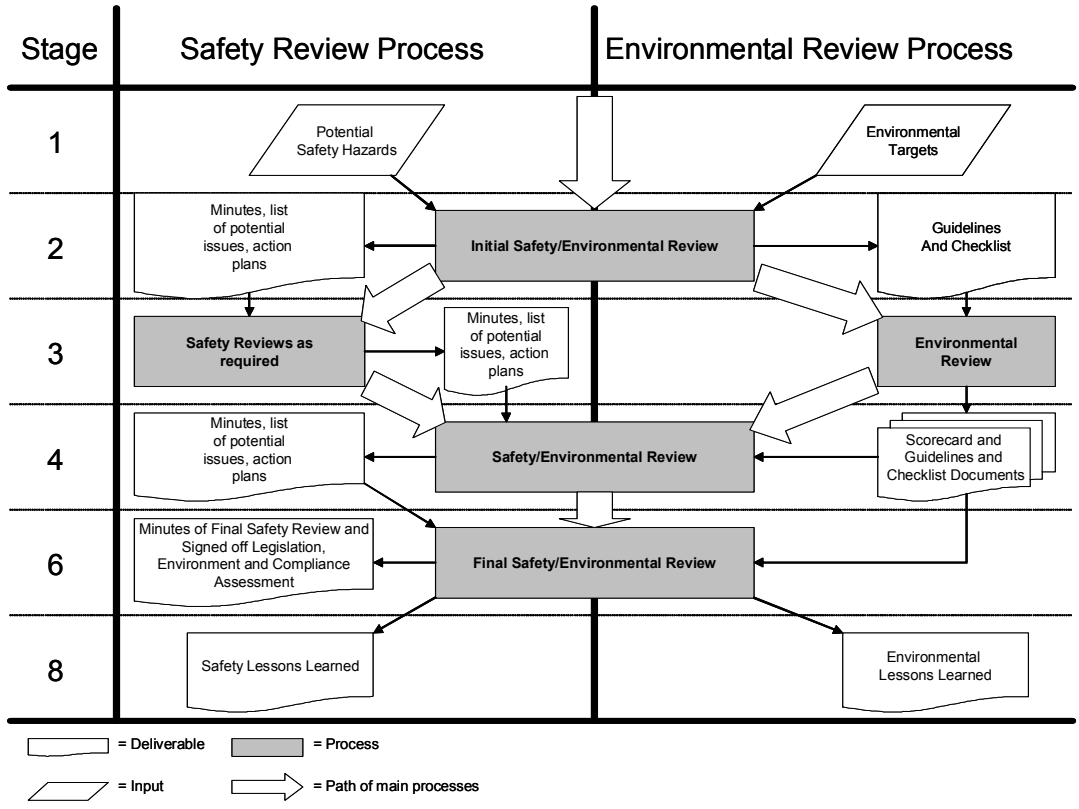


Figure 5.1. Combined safety and environmental review process [19]

profitability and market share. In addition to these issues, the product initiation document will also address environmental regulations and trends and opportunities to create environmental advantage. Targets for environmental improvement will also be included.

5.5.2 Conceptual Design Environmental Review

The second environmental review is held separately from the safety hazard review. During this meeting, the project team will check compliance regulations, fill in the guidelines and checklist document, discuss the metrics in the guidelines and checklist document and write the minutes.

The lead engineer will update the scorecard and review opportunities and additional environmental issues for the next meeting.

The result of this meeting is an updated guidelines and checklist document and meeting minutes. The reliability representative will update.

5.5.3 Detailed Design Environmental Review

The third environmental review is coupled with a safety review. During this meeting, the project team should ensure that all environmental compliance issues are resolved. There should be no further changes to the design due to environmental reasons after this meeting. The result of the meeting is an updated guidelines and checklist document and meeting minutes. The reliability representative will update the guidelines and

checklist document and write the minutes. The lead engineer will update the scorecard for the next meeting.

5.5.4 Final Environmental Review

The fourth and final environmental review is coupled with a safety review. During this meeting, all environmental compliance issues must be resolved. Optimally, no design changes due to environmental reasons would have been made between the last meeting and this meeting. The result of the meeting is a final guidelines and checklist document and meeting minutes. The reliability representative will finalize the guidelines and checklist document and write the minutes. The lead engineer will finalize the scorecard and create a material declaration statement (MDS) packet for the product.

5.5.5 Post-launch Review

Black & Decker includes a lessons learned summary in their product development process. This document discusses what went well with the project, what did not go well with the project, and reasons why the product did not meet targets set in the trigger document. The lessons learned summary will include environmental design innovations realized during the product development process for publicity and customer questionnaires. An example of an item to be included in the lessons learned summary is a materials selection decision. Details should include what materials were considered and the rationale of the decision. The lessons learned summary is a very important part of the DfE process because it provides future design teams with the environmental knowledge gained by the previous designers.

5.5.6 Feedback Loop

The completed checklist and guidelines documents and lessons learned summaries create a feedback loop for the DfE process. Design engineers working on similar products can use this information to make better decisions immediately and the information is also valuable when the next generation of the product is designed years down the road. Design engineers will record what environmental decisions were made and why they were made. The decision information, scorecards and comments on the guideline document will be archived permanently. The goal is to save the right things so the information is there in the future when more feedback activities, such as a product tear-down to verify scorecard metrics, can be introduced.

5.6 Analysis of the DfE Process

Black & Decker's new DfE process described above is innovative and has many advantages compared to traditional DfE tools. There are many standalone DfE tools available to designers. Otto and Wood [18] provide an overview of some of the DfE tools currently used. Two examples cited are general guideline/checklist documents and life cycle assessments (LCAs).

A general guideline/checklist document is a simple DfE tool that forces designers to consider environmental issues when designing products. Integrating a guideline/checklist within a new DfE process is simple and effective way to highlight environmental concerns. However, it should be noted that the guideline/checklist document needs to be company specific and integrated systematically into the product development process. Using an existing generic, standalone guideline/checklist document will most likely be ineffective. First, the point of a guideline/checklist document is to ensure that designers are taking the proper steps towards achieving environmental objectives. Another organization's guidelines /checklist document was designed to obtain their own objectives which may not coincide with another company's objectives. Second, obtaining a guideline/checklist document and simply handing it to designers will lead to confusion as to when and how to use the list. Specific procedures need to be implemented to ensure the designers are exposed to the guideline/checklist document early in the product development process to promote environmental design decisions.

LCAs are time-consuming projects that research a product's environmental impacts and conducts tests to produce environmental impact quantities. The problem with LCAs is that they take a long time, are very expensive, and provide information only after the design is complete. LCAs do not help designers improve a current product's environmental impact. Our DfE process, however, provides guidelines that help achieve Black & Decker's environmental objectives, and it contains a lessons learned summaries that provide a design engineer with helpful information about previously used decisions and techniques.

Klein and Sorra [20] argue that successfully implementing an innovation depends upon "the extent to which targeted users perceive that use of the innovation will foster the fulfilment of their values." The DfE process contains values that coincide with the organization's values. Within the Corporation's Code of Ethics and Standards of Conduct [21], there is a section titled Environmental Matters which "places responsibility on every business unit for compliance with applicable laws of the country in which it is located, and…expects all of its employees to abide by established environmental policies and procedures." Black & Decker's environmental objectives were taken into account and consequently the DfE process requires designers to track related metrics. The process leverages existing processes hence minimizing time-to-market and requiring little extra effort from the designers. Black & Decker's product development process was studied to ensure information availability. A DfE process that is customized for Black & Decker is much more likely to be implemented than standalone tools. By researching any organization's product development process and understanding the decision-making processes, information flow, and organizational and group values, it is possible to construct a DfE process that is customized and easy to implement.

5.7 Conclusions

This chapter describes an innovative DfE process in which a design team repeatedly considers key product-level environmental metrics. These metrics are directly related to the corporation's environmental objectives. These metrics do not require excessive time or effort. The iterative nature of the DfE process means that design teams consider different aspects of DfE at the most appropriate time, when information is available and key decisions must be made.

The DfE process was created specifically for Black & Decker through studying their product development process and incorporating DfE activities with similar existing activities. Environmental regulations are treated in a systematic and formal way so that the design teams can document the new product's compliance. Finally, this report includes guidelines and an environmental scorecard that the product development teams can use to improve the product's environmental performance.

The research team is now assisting with the implementation and planning assessment activities such as material declaration forms and upgrading service bill of material lists to include material identification for recycling. The assessment of this approach remains for future work. Such an assessment would need to involve performance metrics such as: the time required for DfE reviews, the number of additional tasks required, the improvement in product environmental metrics, and the percentage of questions that can be accurately answered in customer questionnaires. Further research using this methodology will establish its usefulness for improving product development.

Acknowledgements

The authors greatly appreciate the help provided by Black & Decker employees, especially Mike Justice. This material is based upon work supported by the National Science Foundation under grant DMI-0225863. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] Handfield Robert B, Melnyk Steven A, Calantone Roger J, Curkovic Sime. Integrating environmental concerns into the design process: the gap between theory and practice. IEEE Transactions on Engineering Management 2001; 48, (2): 189–208.

[2] Menke Dean M, Davis Gary A, Vigon Bruce W. Evaluation of life-cycle assessment tools. Environment Canada. 30 August 1996. http://eerc.ra.utk.edu/ccpct/pdfs/LCAToolsEval.pdf

[3] Poyner JR, Simon M. Integration of DfE tools with product development. Clean Electronics Products and Technology, (CONCEPT), International Conference on 1995; 9-11 Oct: 54–59.

[4] Simon Herbert A. Administrative behavior (4th edition). The Free Press, New York, 1997.

[5] Smith Preston G, Reinersten Donald G. Developing products in half the time. Van Nostrand Reinhold, New York, 1991.

[6] Herrmann Jeffrey W, Schmidt Linda C. Viewing product development as a decision production system. DETC2002/DTM-34030, Proceedings of the 14th International Conference on Design Theory and Methodology Conference, ASME, Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Montreal, Canada 2002; September 29–October 2.

[7] Herrmann Jeffrey W, Schmidt Linda C. Product development and decision production systems. In: Chen W, Lewis K, Schmidt LC, editors. Decision making in engineering design. ASME Press, New York, 2006.

[8] Herrmann Jeffrey W. Decision-based design of product development processes. Working paper 2007.

[9] Bertola P, Teixeira JC, Design as a knowledge agent: how design as a knowledge process is embedded into organizations to foster innovation. Design Studies 2003; 24:181–194.

[10] Brown John Seely. Research that reinvents the corporation. In: *Harvard Business Review on Knowledge Management*, Harvard Business School Press, Boston, 1998.

[11] Krishnan V, Ulrich Karl T. Product development decisions: a review of the literature. Management Science 2001; 47(1):1–21.

[12] Checkland Peter. Systems thinking, systems practice. Wiley, West Sussex, 1999.

[13] Knudsen Sanne, Keoleian Gregory A. Environmental law: exploring the influence on engineering design. Center for Sustainable Systems, University of Michigan, April 5, 2001; Report No. CSS01-09, Available online at http://css.snre.umich.edu/css_doc/CSS01-09.pdf, accessed July 1, 2003.

[14] Directive 2004/12/EC of the European Parliament and of the Council of 11 February 2004 amending Directive 94/62/EC on packaging and packaging waste. Official Journal of the European Union. Accessible online at http://www.europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_047/l_04720040218en00260031.pdf

[15] Waste Electrical and Electronic Equipment (WEEE) Directive. UK's Environmental Agency. Accessible electronically through the Environmental Agency's Website http://www.environment-agency.gov.uk/business/444217/444663/1106248/?version=1&lang=_e

[16] Terms of environment. Environmental Protection Agency. Document number EPA175B97001. Accessibly electronically through The Environmental Protection Agency's Website. http://www.epa.gov/OCEPAterms/eterms.html

[17] EPA. Valuing potential environmental liabilities for managerial decision-making. EPA742-R-96-003. Dec. 1996. http://www.epa.gov/opptintr/acctg/pubs/liabilities.pdf3

[18] Otto Kevin N, Wood Kristin L. Product design: techniques in reverse engineering and new product development. Prentice Hal, Upper Saddle River, NJ. 2001.

[19] Fitzgerald DP, Herrmann JW, Sandborn Peter A, Schmidt Linda C, Gogoll Ted. Beyond tools: a design for environment process. International Journal of Performability Engineering 2005; 1(2):105–120.

[20] Klein Katherine J, Sorra Joann Speer, The challenge of innovation implementation. Academy of Management Review 1996; 21(4):1055–1080.

[21] The Black & Decker Corporation Code of Ethics and Standards of Conduct. 13 February 2003. http://www.bdk.com/governance/bdk_governance_appendix_1.pdf

6

Dependability Considerations in the Design of a System

Krishna B. Misra

RAMS Consultants, Jaipur, India

Abstract: For better system performance, attributes such as quality, reliability, maintainability, safety, and risk that are closely related and govern the dependability of the system, must be considered. It is also necessary to understand the inter-relationship between these factors so that one not only minimizes the chances of occurrence of any untoward incident at the design and fabrication stage but also minimizes the chances of occurrences and the consequences of such an event during the system operation and use phase.

6.1 Introduction

As systems become more and more complex, their chance of failure-free operation also decreases and we cannot possibly altogether eliminate a failure within a system but we can certainly attempt to contain its impact. High-risk systems particularly require a thorough investigation or analysis to ensure high level of performance and safety as an accident can cause havoc in the surrounding environment and may be economically disastrous if it occurs.

We have seen in Chapter 1 that to ensure that a system or product is dependable, we must ensure that its survivability is high and that it is safe during its operation and use. Obviously, ensuring high performance levels in design and operation of the system in question can avert accidents. Prevention of an accident requires excellence in performance, which leads to high plant dependability and reduces the chances of failure and the associated risk. Consequently, the safety of the plant should be high. In other words, high system dependability helps prevent accidents. However, there is a balance to be struck between the safety and the cost of achieving it. On the other hand, although a plant may be safe, the standards from ecological and stringent environmental protection may require serious consideration of the consequences that would follow from a probable accident.

6.2 Survivability

The ultimate worth of any product or system is judged by its performance, either expected or specified. In order to define the desired performance of a product or system, it is important to consider the following aspects:

- Definition or objective of a product or a system
- Criteria of acceptable performance
- Definition of failure or malfunctioning
- Expected time of operation
- Operating conditions
- Maintenance conditions
- Tests and sampling procedures

How well a product or a system meets its performance requirements depends on its various characteristics, such as quality, reliability, availability and efficiency. A product or a system having these attributes is usually expected to perform well over its lifetime incurring minimum life-cycle costs, which include design and development, manufacturing, and maintenance costs.

No one can ever dispute the necessity for a product or a system to survive its expected life; however, this survivability depends on attributes like quality, reliability and maintainability or availability. Therefore, to ensure higher survivability of a product or a system, it is essential that all the above attributes be ensured, not just one of them.

Often the only concern of a manufacturer appears to be the *product quality* and the customer is happy to accept the product as long as it is supported with a warranty. At best the customer may also have some protection in law, so that he may claim redress for failures occurring within a reasonable time, usually the warranty period. However, this approach provides no guarantee of performance over a period of time, particularly outside the warranty period. Even within a warranty period, the customer usually has no grounds for further action if the product fails once, twice or several times, provided that the manufacturer repairs the product as promised each time. If it fails often, the manufacturer will suffer high warranty costs, and the customers will suffer inconvenience. However, outside the warranty period, it is only the customer who is left to suffer the consequences of failures. Of course, the manufacturer may also probably incur a loss of reputation and possibly future business.

Therefore, we have the requirement of a time-based concept of quality. The inspectors' concept is not time-dependent nor does it ensure that the product will be able to function satisfactorily under the actual conditions of environment of use. The quality tests either pass a product or fail it. In other words we must not only have high quality but also higher reliability, since reliability is usually concerned with failures in the time domain of the use of a product or a system. This distinction also highlights the difference between traditional quality control efforts and pursuing reliability engineering programs. Moreover, whether or not failures occur and the times of their occurrence, can never be forecast accurately. Therefore, reliability implies an aspect of engineering uncertainty, which is often reflected in its probabilistic definition, *viz.*, *it is the probability that a product or a system will perform the intended function without failure under stated conditions of use over a stated period of time*. However, to produce reliable products or systems, we may have to incur increased costs of design and manufacturing.

Besides *one-shot equipment/devices* like ICs, electric components, bulbs, rockets, missiles, *etc*., there are products or systems whose survivability can be improved considerably and these can be maintained in a functional state over a long period of time by carrying out necessary maintenance, whether it is *preventive* or *corrective*. Preventive maintenance consists of routine maintenance at predetermined points of time during the operation phase to reduce the chances of failure of a unit, whereas corrective maintenance or repair is carried out only after a failure has occurred. Sometimes maintenance may be carried out based on the condition of a unit based on the signature analysis of certain parameters like vibration, noise, *etc*. Such maintenance is known as *predictive* maintenance.

Maintenance also has a significant influence on the life of a product or system and consequently on the reliability. In addition to maintenance, the supply function also has a considerable effect on reliability. The supply function is concerned with providing of the necessary personnel, material, parts and equipment to support operation in the field. Collectively, maintenance and supply efforts, materials, facilities and manpower form the logistics support. The logistics costs over the lifetime of a product or system may exceed considerably the initial cost of the product or system. In fact, maintenance includes all actions necessary to keep the unit in a usable condition through preventive measures, which include check-out, testing, overhaul, repair, instructions, operational schedules, spares and last but not least personnel.

Maintainability and reliability are the two most important design parameters in establishing the availability of a product. Availability is defined as the probability of a product working satisfactorily at any given point of time when used under given conditions. Obviously, availability depends on the time during which the product is available. Time is of basic importance in this concept. The available time or uptime and is the time during which the product is working. The unavailable time or downtime is the time during which the maintenance is being done. Obviously, availability becomes a more important parameter of performance of the maintained product or system than reliability. However, reliability and maintainability are both related to availability.

Maintainability is determined by the design of the product or system and can be greatly enhanced if fault detection, isolation and repair procedures are worked out during the design stage itself. Maintenance procedure charts and diagrams can also help considerably during repair and should include all pertinent tests points and a description of what should be measured and observed at each test point. In documenting these repair procedures, due consideration must be given to personnel skill levels, tools, facilities and the time that will be available under field conditions for the repairs.

Poor or deficient performance attributes not only affect the life-cycle costs but also have effects in terms of environmental consequences. Degraded performance attributes reflect more on the material and energy requirement and wastes and cause more environmental pollution when reckoned over a given period of time. Obviously, a product with poor quality, reliability, maintainability, availability, or efficiency will incur more life-cycle costs and would be uneconomical to use. Generally, these costs are also inter-dependent on the attributes of performance. For example, a highly reliable product will have lower maintenance costs.

6.3 System Effectiveness

The *system effectiveness* relates to that property of system output, which was the reason for having that system. Obviously, if the system is effective, it should carry out this function very well otherwise efforts can be made to improve the chosen system attributes in which the system is deficient. Effectiveness is influenced not only by the way the system/equipment is designed and built, but also the way in which the system/equipment is used and maintained. In other words, the design engineer, the production engineer, the operator and the maintenance man can materially influence system effectiveness. It can also be influenced by the logistic system that supports the operation, and by the administration through personnel policy, rules governing equipment use, fiscal control, and many other administrative policy decisions.

The term *system effectiveness* is defined in several ways. A formal definition is:

1. *System effectiveness is the probability that the system would successfully meet an operational demand within a given time when operated under specified conditions*.

An alternative definition of system effectiveness is given as:

2. *System effectiveness is the probability that the system will operate successfully when called upon to do so under specified conditions.*

The major difference between these two definitions lies in the fact that, in definition 2 (which is basically for one-shot devices or non-maintained systems such as missiles, *etc*.), time is relatively unimportant. The first definition is more general and the operating time is a critical element, and effectiveness is expressed as a function of time. Another difference is that the first definition provides for the repair of failures, both at the beginning of the time interval (if the system is inoperable then) and also during the operating interval (if a failure occurs after a successful start); the second definition assumes no repairs.

However, both the definitions imply that the system fails if:

(1) It is an inoperable condition when needed, or,
(2) It is operable when needed but fails to complete the assigned mission successfully.

The expression "*specified conditions*" implies that system effectiveness must be stated in terms of the requirements placed upon the system, indicating that failure and use conditions are related. As the operational stress increases, the failure frequency may also be expected to increase.

6.4 Attributes of System Effectiveness

There are several attributes of system effectiveness and it would be worthwhile to discuss these here. Various definitions of terms used shall also be provided. The following is an outline, not necessarily a complete and perfect enumeration, of the factors, which must be considered while designing a system:

(i) Design Adequacy

The system should satisfy the following attributes:

1. Technical capabilities
   - Operational simplicity
   - Accuracy
   - Range
   - Invulnerability to countermeasures
2. Specifications
   - Space and weight requirements
   - Input power requirements
   - Input information requirements
   - Requirements for special protection against shock, vibration, low pressure, and other environmental influences

(ii) Operational Readiness

In order that the system fulfills operational requirements adequately over the intended period of time, the system must be designed for:

- Reliability, which means, the system has
  - failure-free operation
  - redundancy or provision for alternative modes of operation
- Maintainability
  - Time to restore the failed system to operating state
  - Technical manpower requirements for maintenance
  - Effects of use cycle on maintenance
  - Logistic support

(iii) System Cost

The system must be developed with minimum cost.

- Development cost, and particularly development time, from inception to operational capability
- Production cost
- Operating and operational support costs

The optimization of *system effectiveness* by judiciously balancing the conflicting requirements or specifications in the above list is an extremely difficult task, as there is a high degree of interaction among the factors involved in the problem. It is not always practicable to maximize all the desirable properties of a system simultaneously. Naturally, there would be some *trade-offs* between system cost and the achievable levels of reliability and maintainability and many other parameters of design. In the following sections, we will define these parameters one by one and also discuss the implications of choosing one or more parameters of system design.

6.4.1 Reliability and Mission Reliability

The definition of reliability is generally given as:

> *Reliability is the probability that a system will perform satisfactorily for at least a given period of time under stated conditions of use.*

However, *mission reliability* is defined as:

> *The probability that a system will operate in the mode for which it was designed for the duration of a mission, given that it was operating in this mode at the beginning of the mission*.

Mission reliability thus defines the probability that no system failure takes place during the *mission time, i.e.*, the period of time required to complete a mission. All possible redundant modes of operation must be considered while describing reliability, mission reliability, and system effectiveness.

6.4.2 Operational Readiness and Availability

The capability of a system to perform its intended function when called upon to do so is often referred to by either of the two terms, namely, *operational readiness* and *availability*. System effectiveness includes the built-in capability of the system, its accuracy, power, *etc*. Operational readiness excludes the ability of the system to do the intended job but includes only its readiness to do it at a particular time.

It would be worthwhile to mention the distinction between the terms-operational readiness and availability. Availability is defined in terms of operating time and downtime, where the downtime includes active repair time, administrative time, and logistic time. On the other hand, operational readiness is defined in terms of all of these times, and, in addition, includes both free time and storage time, *i.e.*, all calendar time. Therefore, availability and operational readiness are defined as follows:

Availability of a system or equipment is the probability that it is operating satisfactorily at any given point in time when used under stated conditions, where the total time considered includes operating time, active repair time, administrative time, and logistic time.

Operational readiness of a system or equipment is the probability that at any point in time it is either operating satisfactorily or is ready to be placed in operation on demand when used under stated conditions, including stated allowable warning time. Thus, total calendar time is the basis for computation of operational readiness.

6.4.3 Design Adequacy

System design adequacy is the probability that a system will successfully accomplish its mission, given that the system is operating within design specifications.

The design may include alternative modes of operation, which are equivalent to built-in automatic repair, usually with allowable degradation in performance. These alternative modes of operation are included in the definition of system design adequacy.

6.4.4 Repairability

Repairability is defined as the probability that a failed system will be restored to operable condition in a specified active repair time.

6.4.5 Maintainability

Obviously, this attribute refers to only those systems that can be repaired or maintained. *Maintainability* is defined as the probability that a failed system is restored to operable condition in a specified downtime. Actually downtime consists of *administrative*, *logistic*, and *actual repair times*. In reality, preparation time, fault location time, part procurement time, actual repair time and testing time after repair all add up to increase the total downtime. Maintainability [4] is primarily determined by the design of the product or system and can be greatly enhanced if the fault detection, isolation, and repair procedures are worked out during the design stage itself. In documenting the repair procedure, due consideration should be given to personal skill levels, tools, facilities, and the time that will be available under the field operating conditions.

This attribute is quite analogous to repairability. The difference is merely that while maintainability is based on the *total downtime* (which includes active repair time, logistic time, and administrative time), repairability is restricted to include active repair time only.

6.4.6 Serviceability

Intuitively, it would seem that some term should be used to present the degree of difficulty with which equipment can be repaired. The term serviceability has been selected for this concept. Serviceability has a strong influence on reparability, but the two are essentially different concepts. *Serviceability* is an equipment design characteristic while reparability is a probability involving certain categories of time.

Although the definition of serviceability is stated in a manner that suggests a quantitative concept, it is often necessary to accept a qualitative evaluation of the serviceability of a system or

equipment. When we say that equipment A is more serviceable than equipment B, we mean that the better the serviceability, the shorter the active repair time. Hence, reparability is a reflection of serviceability even though the two concepts are quite distinct.

Serviceability is dependent on many hardware characteristics, such as engineering design, complexity, and the number and accessibility of test points. These characteristics are under engineering control, and poor serviceability traceable to such items is the responsibility of design engineers. However, many other characteristics, which can cause poor serviceability, are not directly under the control of a design engineer. These include lack of proper tools and testing facilities, shortage of workspace in the maintenance shop, poorly trained maintenance personnel, shortage of repair parts, and other factors that can increase the difficulties of maintenance.

6.4.7 Availability

Availability is defined as: the probability of a product or system working satisfactorily at any given point of time when used under the given conditions of use.

Thus availability signifies the probability that the system is available and is working satisfactorily at a given point of time. Availability is a more meaningful parameter of performance of a maintained system than reliability. However, reliability and maintainability are related to availability and are two important design parameters in establishing the availability of equipment.

6.4.8 Intrinsic Availability

The intrinsic availability of a system or equipment is the probability that it is operating satisfactorily at any given point in time when used under stated conditions, where the time considered is operating time and active repair time. Thus, intrinsic availability excludes from consideration all *free time*, *storage time*, *administrative time*, and *logistic time*. As the name indicates, intrinsic availability refers to the built-in capability of the system or equipment to operate satisfactorily under stated conditions.

6.4.9 Elements of Time

Time is of basic importance in the concept of corrective maintenance. The unavailable time or downtime is the time in which the maintenance is being done. This includes waiting time, which is the time lost for administrative or logistic reasons. There are other classifications of time such as free time and storage time. This time may or may not be the downtime depending on whether the product is in operable condition or not. Uptime is the time during which the product is available for use by an intended user. In order to use the probability definitions discussed in the previous sections, the following definitions are given for the time elements, which must be considered in the evaluation of system effectiveness.

6.4.9.1 Operating Time

Operating time is the time during which the system is operating in a manner acceptable to the operator.

6.4.9.2 Downtime

Downtime is the total time during which the system is not in an acceptable operating condition.

Since downtime is subdivided into *active repair time*, *administrative time* and *logistic time*, it is appropriate here to discuss these elements in a little more detail.

6.4.9.3 Active Repair Time

Active repair time is that portion of downtime where the repair crew is working on the system to affect a repair. This time includes preparation time, fault-location time, fault-correction time, and final checkout time for the system.

Both the active repair time and operating time are determined by the inherent characteristics of the equipment, and hence are primarily the responsibility of the manufacturer. Improvement in this area requires action to reduce the frequency of failure or to facilitate the ease of repair, or both. In fact, operating time and active repair time are representative of reliability and reparability and are related through the concept of intrinsic availability.

6.4.9.4 Logistic Time

Logistic time is that portion of downtime during which a repair is held up because of procurement or replacement of a failed part or parts.

Logistic time is the time consumed by delays in repair due to the unavailability of replacement parts. This is a matter largely under the control of administration, although the requirements for replacements are determined by operating conditions and the built-in ability of the equipment to withstand operating stress levels. Policies determined by management and procurement personnel can, if properly developed, minimize logistic time. Therefore, the responsible administrative officials in this area are likely to be different from those who most directly influence the other time categories.

6.4.9.5 Administrative Time

Administrative time is that portion of the total downtime that is not included under active repair time and logistic time. This is the time lost on account of necessary administrative activities and unnecessarily wasted time in organizing a system repair.

The administrative time category is almost entirely determined by administrative decisions concerning the processing of records and the personnel policies governing maintenance engineers, technicians, and those engaged in associated clerical activities. Establishing efficient methods of monitoring processing, and analyzing repair activities is the responsibility of administration. In addition, administration time has been defined to include time wasted due to bottlenecks in executing the responsibility of administration. It is independent of engineering activities as such, and is also does not concern the manufacturer of equipment.

6.4.9.6 Free Time

Free time is the time during which the system is idle and is not operational. This time may or may not be downtime, depending on whether or not the system is in an operable condition.

6.4.9.7 Storage Time

Storage time is the time during which the system is presumed to be in good condition (and can be put to use), but is being held as a spare for emergency.

It may be noted here that while the system effectiveness is dependent upon all of the time elements, the design adequacy does not involve any of them.

6.5 Life-cycle Costs (LCC)

All expected costs incurred during the entire life of a product discounted to obtain the present value at a given level of reliability forms the part of life-cycle cost (LCC) analysis. It is well known that we can engineer survivability into a product at the design stage, if adequate resources are available. Generally, survivability costs, which include quality and reliability costs, can be split into two parts, *viz.*, c*ontrollable costs* and r*esultant costs*.

The controllable costs are the costs that are incurred on planned activities that are necessary to ensure quality and reliability, inspection and testing costs being included in these costs. The remaining costs are unplanned costs on account of not achieving the desired levels of quality and reliability. These include *internal failures* costs and *external failures* costs. External failures costs result from failures after the product is delivered to the customer, whereas the internal costs are the costs incurred on account of failures before the shipment of a product. If the manufacturer intends to stay in business, not only he is required to optimize LCC and profits but also customer satisfaction.

Usually, manufacturer costs consist of reliability design costs (including, planning, inspection and life testing training and management cost, and research and development costs), internal failure costs (including yield loss scrap and wastage, diagnostic costs, repair and rework operations, and loss of time and wages), and the external costs (including after-scale service and repair costs, replacement, warrantee costs and costs of loss of reputation). It may be observed that any effort to increase the reliability of a product will increase

quality and reliability costs, however the internal-failure costs would increase. The external costs would also decrease with an increase in the reliability of a product.

On the other hand, customer satisfaction depends on initial cost, operating cost, maintenance cost, failure and associated costs, and depreciation cost. The sum total of the above costs is called the *life-cycle cost* of a product and is often several times greater than the basic purchase cost of a product. One way of expressing customer product satisfaction can be in terms of the benefit/cost ratio, also known as the product value, is given by

$$Product Value = \frac{performance\ and\ /\ or\ service}{total\ life - cycle\ costs},$$

where the performance of the product can be assessed in terms of the reliability or one or more of its allied characteristics, such as quality, availability, MTTF, *etc*.

6.6 System Worth

In designing a system, the economics of building that system must always be considered. Every system has certain intended functions to perform at minimum cost. The total cost of ownership (including initial and operating costs for the service life of the equipment) can be substantially reduced if proper attention is given to factors like reliability and maintainability right at the early design stage of the system. These considerations, therefore, lead to the concept of *system worth*, and relate system effectiveness to total cost, scheduling, and personnel requirements. To optimize system worth, program managers face a difficult task of striking balances in maximizing system effectiveness while minimizing the total cost, development time, and personnel requirements.

6.7 Safety

The general definition of *safety* is the condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or any other types of consequences arising from failure, damage, error, accidents, harm or any other event that could be considered *undesirable*. This can take the form of being protected from an event or from exposure to something that can cause health or economical losses. It can include protection of people or of possessions. There are also two slightly different notions of *safety*, namely, a *safety home* may indicate its ability to protect against any external harmful events, and the second that its internal installations are safe (not dangerous/harmful) for its habitants or users. Safety is generally interpreted as implying a real and significant impact on the risk of death, injury or damage to property. In response to perceived risks many interventions may be proposed, with engineering responses and regulation being two of the most common.

It is important to distinguish between products that meet standards that are safe and those that merely feel safe.

Normative safety is a term used to describe products or designs that meet applicable design standards.

Substantive safety means that the real-world safety history is favorable, whether or not standards are met.

Perceived safety refers to the level of comfort of users. For example, traffic signals are perceived as safe, yet under some circumstances they can increase traffic crashes at an intersection. Probably the most common individual response to perceived safety issues is insurance, which compensates for or provides restitution in the case of damage or loss of property.

6.7.1 Plant Accidents

A complex system or a plant constitutes several kinds of subsystems. It is usually a failure of some small part somewhere in a system or a plant that leads to an accident of enormous consequences. In reality a wide variety of failures, errors and events can occur in complex and potentially hazardous plants and these usually occur on account of logical interactions between human operators and

the system or plant. Some of these interactions can be listed by arguing "why", "how", "when", and "where" of failures. In fact, these interactions can occur at any instant or time during the plant life; *viz.*, during sitting, design, manufacturing, construction, commissioning, and operation. It is generally believed that accidents occur as a result of failures during plant operations but this is too narrow a view. Failures can occur at any stage of system acquisition and operation or use. Broadly speaking, an accident may occur due to any of the following reasons:

New Technology: New technologies improve system functioning but may sometimes introduce some snags during the initial burn-in period or during the technology maturing period.

Location: The physical location of the system or plant including natural factors, such as geological and seismological conditions and potential for hydrological and meteorological disturbances, may affect plant safety. The release of toxic and flammable gases from chemical plants, and aircraft impact (if located in the air corridor) can also influence plant safety. In the case of such a release, air, food chains, ground water and water supplies provide pathways for the possible transport of hazardous materials to humans.

External Events: External events such as fire, floods, lightening, and earthquakes may also be responsible for major accidents. In such cases, the design of a system should be such that consequences of such an external event are minimized and cause minimal fatalities or loss of property.

Design: Accidents can also be caused by errors committed during research, development and demonstration phases, and while commercializing a design for an actual use. Design errors may be caused by short research, development and monitoring periods. A system deficiency can prove to be very costly once the design has been released for production and is manufactured and deployed, since the costs may not only include replacement and redesign costs, due to modifications but also include liability costs, and loss of user faith.

Manufacturing, Construction and Commissioning: Defects can be introduced when a system or a plant is being fabricated and constructed with deviations from the original design specifications and from fabrication/construction procedures or due to inadequate quality checks. Defects in design, manufacturing and construction stages may show up after commissioning and during the demonstration before it is made operational. A bug in the software package can also be an example of commissioning failures.

Operation: A system or plant operation can be categorized as *normal*, *operation during anticipated abnormal occurrences*, operation *during complex events below design basis*, and *operation during complex events beyond design basis*. Generally, physical barriers, normal control systems, emergency safety systems, and in-site and off-site emergency counter-measures protect all plants. For example, an emergency safety system in a nuclear reactor [1] operates when the plant state reaches a trip set point below the safety limit but above the operating range. The safety system can fail in two modes, *viz.*, *fail-safe* and *fail-dangerous*. Accident causation mechanisms can also be split into an *event layer* and *a likelihood layer*. Usually, event and fault trees analyses deal with the event layer. Recently, emphasis has been placed on the likelihood layer where management plays crucial role in managing occurrence probabilities, dependence of event and uncertainties associated with the events.

System safety [2] is constrained by physical containments and stabilization of an unstable phenomenon. In fact, accidents can be caused either by hardware failure, human error or external events. Generally, accidents are caused by any of the following reasons:

Failure of Physical Containment: All systems have built-in physical barriers or containment to prevent the release of hazardous materials or to prevent hazardous effects. As long as these containments do not fail, an accident of high consequence cannot take place. It is only when the containment fails that an accident occurs.

Failure of Safety Systems: All systems have adequate control systems during their normal

operations and safety systems and in-site and off-site emergency measures during an emergency. If anything goes wrong with the normal control system, incidents occur and if emergency safety systems fail to cope up with these incidents, a plant accident may occur. Finally, if in-site emergency measures fail to contain an accident, it invades into the environment and when off-site emergency measures fail to cope up with the invasion, this may cause serious consequences for the public and the environment.

Human Errors: Human errors constitute the vast majority of causes of major accidents. Sometimes hardware failure induces human errors, which may eventually lead to an accident. For example, a faulty indicator may cause wrong human intervention to cause an accident. Sometimes, system induced failures occur due to improper management caused by human and hardware failures.

Dependent Failures: A chain of failure events can be caused by dependency of failures due to sharing of a common environment or location.

6.7.2 Design for Safety

Safety engineers work on the early design of a system, analyze it to find what faults can occur, and then propose safety requirements in design specifications up front and changes to existing systems to make the system safer. In the early design stage, a fail-safe system can often be made acceptably safe with a few sensors and some software to read them. Probabilistic fault-tolerant systems can often be made by using more, but smaller and less expensive pieces of equipment. Far too often, rather than actually influencing the design, safety engineers are assigned to prove that an existing, completed design is safe. If a safety engineer then discovers significant safety problems late in the design process, correcting them can be very expensive.

Through safe design and better performance of systems, one can minimize the ecological impacts and associated losses. This also does not mean that we do not build these systems at all to avoid such accidents or hazards. We have work out the advantages accruing from these systems *vis-à-vis* the risk involved. Of course this opens up the question of an acceptable risk *vis-à-vis* employing the technologies that build the systems [3].

Safety has been considered important in the following cases:

- Design of the end product for safety
- Design of the manufacturing process for safety
- Design of the safety system

A safety system is defined as the total set of men, equipment and procedures specifically designed for the purpose of ensuring safety.

Safety and reliability are related engineering disciplines [4, 5] with many common statistical techniques. In fact safety has lot of mathematical techniques common with reliability, like fault trees, events trees, *etc*. Here we are concerned with statistical safety, which is one of the attributes of dependability related to other attributes like quality, reliability, availability, maintainability or in short survivability. These issues tend to determine the performance of any product, system or service, and a deficiency in any of these attributes is considered to result in lower dependability and higher cost. Besides the cost of addressing the problem, good management is also expected to minimize total cost.

References

[1] Fullwood, R.R., and Hall, R.E. Probabilistic Risk Assessment in the Nuclear Industry: Fundamentals and Applications, Pergamon Press, Oxford, 1988.

[2] International Nuclear Safety Advisory Group: Basic Safety Principles for Nuclear Power Pants, Safety Series, No. 75-INSAG-3, IAEA, 1988.

[3] Greenberg, H.R. and Cramer J.J. (eds.), Risk Assessment and Risk Management for the Chemical Process Industry, Van Nostrand Reinhold, New York, 1991.

[4] Misra, K.B., Reliability Analysis and Prediction: A Methodology Oriented Treatment, Elsevier Science, Amsterdam, 1992.

[5] Misra K.B. (ed.), New Trends in System Reliability Evaluation, Elsevier Science, Amsterdam, 1993.

7

Designing Engineering Systems for Sustainability

Peter Sandborn and Jessica Myers

CALCE, Department of Mechanical Engineering, University of Maryland, USA

Abstract: Sustainability means keeping an existing system operational and maintaining the ability to manufacture and field versions of the system that satisfy the original requirements. Sustainability also includes manufacturing and fielding revised versions of the system that satisfy evolving requirements, which often requires the replacement of technologies used in the original system with newer technologies. Technology sustainment analysis encompasses the ramifications of reliability on system management and costs via sparing, availability and warranty. Sustainability also requires the management of technology obsolescence (forecasting, mitigation and strategic planning) and addresses roadmapping, surveillance, and value metrics associated with technology insertion planning.

7.1 Introduction

The word "sustain"" comes from the Latin *sustenare* meaning "to hold up" or to support, which has evolved to mean keeping something going or extending its duration [1]. The most common non-specialized synonym for sustain is "maintain". Although maintain and sustain are sometimes used interchangeably, maintenance usually refers to activities targeted at correcting problems, and sustainment is a more general term referring to the management of system evolution.

Sustainability can mean static equilibrium (the absence of change) or dynamic equilibrium (constant, predictable or manageable change) [2]. The most widely circulated definition of sustainability (or more accurately sustainable development) is attributed to the Brundtland Report [3], which is often stated as "development that meets the needs of present generations without compromising the ability of future generations to meet their own needs." This definition was created in the context of environmental sustainability, however, it is useful for defining all types of sustainability. Although the concept of sustainability appears throughout nearly all disciplines, we will only mention the most prevalent usages here.

Environmental Sustainability is the ability of an ecosystem to maintain ecological processes and functions, biological diversity, and productivity over time [4]. The objective of environmental sustainability is to increase energy and material efficiencies, preserve ecosystem integrity, and promote human health and happiness by merging design, economics, manufacturing and policy.

Business or Corporate Sustainability refers to the increase in productivity and/or reduction of consumed resources without compromising

product or service quality, competitiveness, or profitability. Business sustainability is often described as the triple bottom line (3BL) [5]: financial (profit), social (people) and environmental (planet). A closely related endeavor is "sustainable operations management", which integrates profit and efficiency with the company's stakeholders and the resulting environmental impacts [6].

Technology Sustainment refers to all activities necessary to a) keep an existing system operational (able to successfully complete its intended purpose), b) continue to manufacture and field versions of the system that satisfy the original requirements, and c) manufacture and field revised versions of the system that satisfy evolving requirements. The term "sustainment engineering" is sometimes applied to technology sustainment activities and is the process of assessing and improving a system's ability to be sustained by determining, selecting and implementing feasible and economically viable alternatives [7]. For technology sustainment, "present and future generations" in the Brundtland definition can be interpreted as the users and maintainers of a system.

This chapter focuses on the specific and unique activities associated with technology sustainability.

7.1.1 Sustainment-dominated Systems

In the normal course of product development, it often becomes necessary to change the design of products and systems consistent with shifts in demand and with changes in the availability of the materials and components from which they are manufactured. When the content of the system is technological in nature, the short product life cycle associated with fast moving technology changes becomes both a problem and an opportunity for manufacturers and systems integrators.

For most high-volume, consumer oriented products and systems, the rapid rate of technology change translates into a critical need to stay on the leading edge of technology. These product sectors must adapt the newest materials, components, and processes in order to prevent loss of their market share to competitors. For leading-edge products, updating the design of a product or system is a question of balancing the risks of investing resources in new, potentially immature technologies against potential functional or performance gains that could differentiate them from their competitors in the market. Examples of leading-edge products that race to adapt to the newest technology are high-volume consumer electronics, *e.g.*, mobile phones and PDAs.

There are, however, significant product sectors that find it difficult to adopt leading-edge technology. Examples include airplanes, ships, computer networks for air traffic control and power grid management, industrial equipment, and medical equipment. These product sectors often "lag" the technology wave because of the high costs and/or long times associated with technology insertion and design refresh. Many of these product sectors involve "safety critical" systems where lengthy and expensive qualification/ certification cycles may be required even for minor design changes and where systems are fielded (and must be maintained) for long periods of time (often 20 years or more). Because of these attributes, many of these product sectors also share the common attribute of being "sustainment-dominated", *i.e.*, their long-term sustainment (life cycle) costs exceed the original procurement costs for the system.

Some types of sustainment-dominated systems are obvious, *e.g.*, Figure 7.1 shows the life cycle cost breakdown for an F-16 military aircraft where only 22% of the life cycle cost of the system is associated with design, development and manufacturing (this 22% also includes deployment,

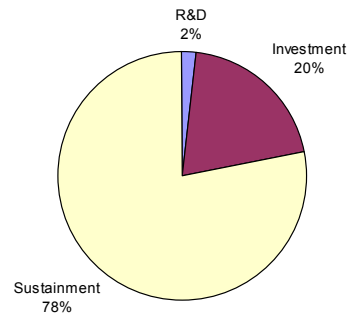


Figure 7.1. Cost breakdown for an F-16, [8]

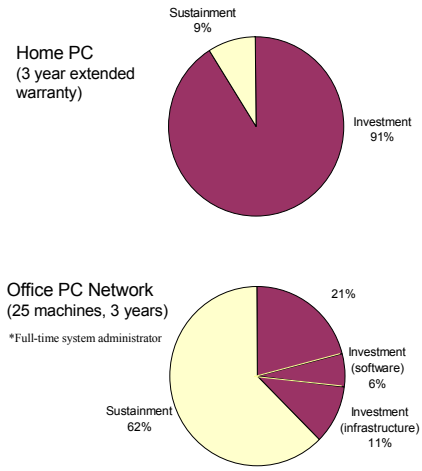


Figure 7.2. Life cycle cost breakdown of PCs, [9, 10]

training, and initial spares). The other 78% is operation and support and includes all costs of operating, maintaining, and supporting, *i.e.*, costs for personnel, consumable and repairable materials, organizational, intermediate and depot maintenance, facilities, and sustaining investment.

Sustainment-dominated systems are not necessarily confined to just the military or other exotic technology systems. Consider the systems shown in Figure 7.2. Obviously, a home PC is not sustainment-dominated, however, an office network of PCs (once you account for system administration) can quickly become a sustainment-dominated system. In fact, when one considers the cyclical "upgrade trap" that is often forced upon PC users (Figure 7.3), the effective sustainment cost of an individual PC and an office PC network may be even larger.

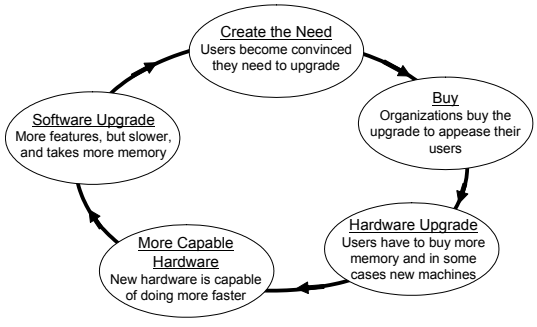


Figure 7.3. Cyclical upgrade trap commonly experienced by PCs and PC networks

The upgrade trap is indiscriminant, even users who derive no actually benefit from higher performance hardware or greater functionality software, are forced to "keep up" whether they want to or not. Even systems that are seemingly disconnected from commercial interests such as weapons systems are impacted, *e.g.*, if these systems contain COTS (commercial off-the-shelf) application software, the application may require the operating system to be upgraded, *etc*.

The one thing that is worse than being caught in the upgrade trap, is not being caught in the upgrade trap, *i.e.*, many sustainment-dominated systems get caught in the "sustainment vicious circle" (also called the DoD death spiral) – Figure 7.4. In this case, more money is going into sustainment at the determent of new investment, which causes the systems to age, which in turn causes more money to be required for sustainment, which leaves less money for new investment, *etc.* The sustainment vicious circle is a reality for militaries of many of the world's countries. On a smaller scale, individuals might face this dilemma with their automobile – fixing your existing car is expensive, but it is less expensive than buying a new car; after several such repairs one is left to wonder if purchasing a new car would have been less expensive, but there is no turning back, too much has been invested in repairing the old car.

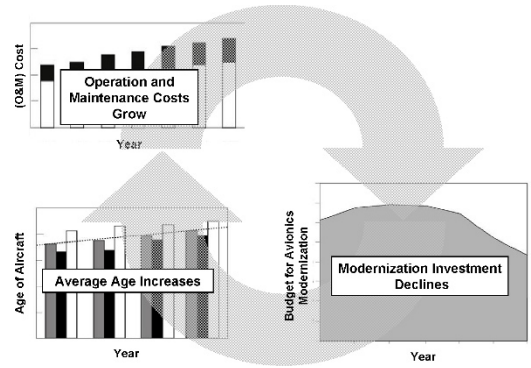


Figure 7.4. Sustainment vicious circle, a.k.a., the DoD death spiral for aircraft avionics [11]

7.1.2 Technology Sustainment Activities

Technology sustainment activities range from automobile oil changes every 3,000 miles and timing belt replacement in a car after 60,000 miles, to warranty repair of a television and scheduled maintenance of a commercial aircraft engine. There are also less obvious sustainment activities that include time spent with technical support provided by a PC manufacturer via telephone or email, installation of an operating system upgrade, or addition of memory to an existing PC to support a new version of application software. The various elements involved in sustainment include:

- Reliability
- Testability
- Diagnosability
- Repairability
- Maintainability
- Spares
- Availability
- Cross-Platform Applicability
- Obsolescence
- Warranty/guarantee
- Qualification/ certification
- Configuration control
- Regression testing
- Upgradability
- Total cost of ownership
- Technology infusion/insertion

Obviously, the relevancy of sustainment activities varies depending on the type of system. For "throw-away" products such as a computer mouse or keyboard, sustainment primarily translates into warranty replacement. For consumer electronics, such as televisions, sustainment is dominated by repair or warranty replacement upon failure. Demand-critical electronics (availability sensitive systems), such as ATM machines and servers, include some preventative maintenance, upgrades, repair upon failure, and sparing. Long field life electronics, such as avionics and military systems, are aggressively maintained, have extensive built in test and diagnosis, are repaired at several different levels, and are continuously upgraded.

This chapter cannot practically cover all the topics that make up technology sustainment. We will not focus on reliability (reliability is the topic of many books and addressed in several other chapters within this book). Neither will we focus on testability or diagnosability since these are also the topics of other books and journals. Rather, we will concentrate on the ramifications of reliability on system management and costs via sparing, availability and warranty (Section 7.2). Section 7.3 treats technology obsolescence and discusses forecasting, mitigation and strategic planning. Section 7.4 addresses technology insertion.

7.2 Sparing and Availability

Reliability is possibly the most important attribute of a system. Without reliability, the value derived from performance, functionality, or low cost cannot be realized. The ramifications of reliability on the system life cycle management are linked to life cycle cost through sparing requirements and warranty return rates, and measured by system availability.

Reliability is the probability that an item will not fail. Maintainability is the probability that the item can be successfully restored to operation after failure; and availability provides information about how efficiently the system is managed and is a function of reliability and maintainability.

7.2.1 Item-level Sparing Analysis

When a system encounters a failure, one of the following things happens:

- Nothing – a workaround for the failure is implemented and operation continues or the system is disposed of and the functionality or role that the system performed is accomplished another way or deleted.
- The system is repaired – if your car has a flat tire, you do not dispose of the car, and you may not dispose of the tire either, you fix the tire.
- The system is replaced – at some level, repair is impractical and the failing portion of the system is replaced; if an IC in your laptop computer fails, you cannot repair a problem inside the IC, you have to replace the IC.

If a tire on your car blows out on the highway and is damaged to such an extent that it cannot be repaired, you have to replace it. What do you replace the flat tire with? If you have a replacement (spare) in your trunk, you can change the tire and be on your way quickly. If you do not have a replacement you have to either have a replacement brought to the car or you have to have the car towed to some place that has a replacement. If no one has a replacement, someone has to manufacture one for you.

Spare tires exist and are carried in cars because the "availability" of a car is important to the car's driver, *i.e.*, having your car unavailable to you because no spare tire exists is a problem, you cannot get to work, you cannot take the children to school, *etc*. If you are an airline, having an airplane unavailable to carry passengers (thus not earning revenue) because a spare part does not exist or is in the wrong location can be a very costly problem. Therefore, *spares* are manufactured and available for use for many types of systems.

There are several issues with spares that make sparing analysis challenging:

- How many spares do you need to have? I do not want to manufacture 1000 spares if I will only need 200 to keep the system operational (available) at the required rate.
- When are you going to need the spares? The number of spares I need is a function of time (or miles, or other accumulated environmental stresses), *i.e.*, as systems *age,* the number of spares needed may increase. When should I manufacture the spares (with the original production or later)? What if I run out and have to manufacture more spares?
- Where the spares should be kept? Spares need to be available where systems fail, not 3000 miles away. When I have a flat tire, is a spare tire more useful in my garage or in the trunk of my car?
- What level (in a system) do you want to spare at? It makes sense to carry a spare tire in my trunk, but it does not make sense to carry a spare transmission in the trunk, why? Because transmissions do not fail as frequently as tires, transmissions are large and heavy to carry, and one may not have the tools, or expertise to install a new transmission on the side of the road.

Spare part quantities are a function of demand rates and are expected to [12]:

- cover actual item replacements occurring as a result of corrective and preventative maintenance actions,
- compensate for repairable items in the process of undergoing maintenance,
- compensate for the procurement lead times required for replacement item acquisition, and
- compensate for the condemnation or scrappage of repairable items.

In order to explore how spare quantities are determined, we first need to review simple reliability calculations. Reliability is given in terms of time (t) by,

$$R(t) = 1 - \int_0^t f(t)dt . \qquad (7.1)$$

The reliability, R(t), is the probability of no failures in time t. If the time to failure, f(t), follows an exponential distribution,

$$f(t) = \lambda e^{-\lambda t}, \qquad (7.2)$$

where λ is the failure rate (λ = 1/MTBF, MTBF = mean time between failure), then the reliability becomes,

$$R(t) = 1 - \int_0^t \lambda e^{-\lambda t} dt = 1 + e^{-\lambda t}\Big|_0^t = e^{-\lambda t} . \qquad (7.3)$$

Equation (7.3) is the probability of exactly 0 failures in time t. This result can be generalized to give the probability of exactly x failures in time t,

$$P(x) = \frac{(\lambda t)^x e^{-\lambda t}}{x!} . \qquad (7.4)$$

So, for x = 0, $P(0) = e^{-\lambda t}$ (the result in Equation (7.3)), for x = 1, $P(1) = \lambda t e^{-\lambda t}$, *etc*. For a unique system with no spares, the probability of surviving to time t is P (0). For a unique system with exactly

one spare available, the probability of surviving to time t is given by,

$$P(0) + P(1) = e^{-\lambda t} + \lambda t e^{-\lambda t}, \qquad (7.5)$$

or in general,

$$P(x \le k) = \sum_{x=0}^{k} \frac{(\lambda t)^x e^{-\lambda t}}{x!}. \qquad (7.6)$$

Equation (7.6) is the cumulative Poisson probability, *i.e.*, the probability of k or fewer failures in time t. This is the probability of surviving to time t with k spares, or, k is the minimum number of spares needed in order to have a confidence level of $P(x \le k)$ that the system will survive to time t.

The derivation of (7.6) assumes that there is only one instance of the spared item in service, if there are n instances in service, then (7.6) becomes [13],

$$P(x \le k) = \sum_{x=0}^{k} \frac{(n\lambda t)^x e^{-n\lambda t}}{x!}, \qquad (7.7)$$

where,

k = number of spares
n = number of unduplicated (in series, not redundant) units in service
λ = constant failure rate (exponential distribution of time to failure) of the unit *or* the average number of maintenance events expected to occur in time t
t = given time interval
$P(x \le k)$ = probability that k is enough spares *or* the probability that a spare will be available when needed
nλt = system unavailability.

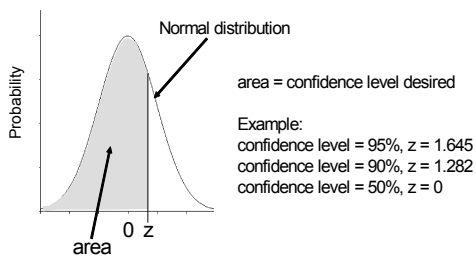


Figure 7.5. Relationship between z and confidence level

When k is large, the Poisson distribution can be approximated by the normal distribution and k can be approximately calculated in closed form,

$$k \cong \left\lceil n\lambda t + z\sqrt{n\lambda t} \right\rceil, \qquad (7.8)$$

where z is the number of standard deviations from the mean of a standard normal distribution, Figure 7.5. Equation (7.8) is only applicable when times between failures are exponentially distributed, and the recovery/repair times are independent and exponentially distributed.

Figure 7.6 shows a simple example sparing calculation performed using (7.7) and (7.8). For the example data shown in Figure 7.6 a simple approximation for the number of required spares is: the MTBF = $1/\lambda = 2\text{x}10^6$ hours and the unit has to be supported for t = 1500 hours; $1500/2\text{x}10^6$ = 0.0008 spares per unit; therefore, for n = 25,000 units, the total number of spares needed is (25000)(0.0008) = 18.75. Rounding up to19 spares, Figure 7.6 indicates that for the simple approximation, there is a 58% confidence that 19 are enough spares to last 1500 hours.

There are several costs associated with carrying spares:

- Cost of manufacturing spares.
- Cost of money tied up in manufactured spares for future use – spares for the future may have to be made now before the required components become obsolete (see Section 7.3).

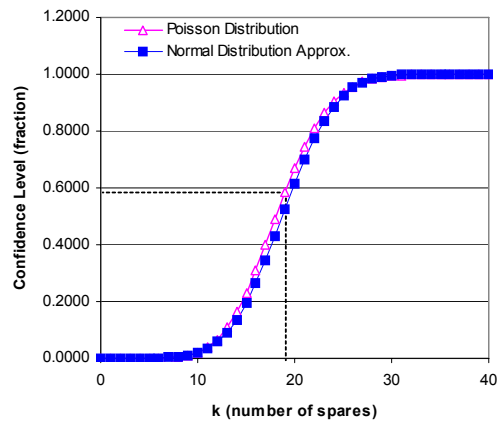


Figure 7.6. Sparing calculation for n = 25000, t = 1500 hours, and λ = 0.5 failures/million hours

- Cost of transporting spares to where they are needed (or conversely the cost of transporting the system to the location where the spares are kept).Cost of storing spares until needed.
- Cost of replenishing spares if they run out.
- Cost of system availability impacts due to spares not being in the right place at the right time.

The simple "item-level availability method" performed in this section ((7.7) and (7.8)) determines recommended quantities of spares based on only demand rates and the confidence in having a spare item available. The difficulty with the item-level availability approach is the following: if I have a 95% confidence that each item within a system has a spare available when needed, what is the availability of a system containing 100 different items? In other words, the calculation so far only determines the number of required spares one item at a time, and ignores interactions between multiple items that make up a system, *i.e.*, it assumes that all the items that make up a system can be spared independently. In order to address system-level sparing, we must first consider availability.

7.2.2 Availability

Availability is the probability that system will be able to function (*i.e.*, not failed or undergoing repair) when called upon to do so. Availability is a function of a system's reliability (how quickly it fails) and its maintainability (how quickly it can be replaced or repaired when it does fail). Availability is closely tied to many of the issues associated with sparing.

Many types of systems care about availability. For example, bank ATM machines, communications systems such as 911 systems, airlines, and military systems. Recently, a large customer claimed the cost of downtime on their point-of-sale verification systems was on the order of $5M/minute [14] – obviously in this case, the availability of the point-of-sale verification system is probably a more important characteristic than the system's price. The United States Department of Defense is adopting a new approach for the management and acquisition of systems. "Performance based logistics" (PBL) is the purchase of support as an integrated, affordable, performance package designed to optimize system readiness and meet performance goals for a system through long-term support arrangements with clear lines of authority and responsibility. Simply put, performance-based strategies would be "buy outcomes, not products or services" [15]. Although PBL implies many things, at its core it is essentially a shift from purchasing systems and then separately purchasing their support, to purchasing the availability of systems.

There are several different types of availability that can be evaluated. Generally, availability is classified either according to the time interval considered, or the type of down time [16]. Time-interval availabilities are characterized as the probability that the system will be available at a time t (instantaneous or point availability), proportion of time available within a specified interval of time (average up-time availability), or the limit as $t\to\infty$ of the average up-time availability (steady-state availability). Alternatively, down-time classified availability includes: only corrective maintenance (inherent availability), corrective and preventative maintenance (achieved availability), and operational availability. In operational availability, down time includes contributions from a broader set of sources than other types of availability,

$$\begin{aligned}\text{Availability}_{\text{operational}} &= \frac{\text{Up time}}{\text{Total time}} = \frac{\text{Up time}}{\text{Up time} + \text{Down time}} \\ &= \frac{\text{Average up time}}{\text{Average up time} + \text{Average down time}}, \\ &= \frac{\text{MTBM}}{\text{MTBM} + \text{MDT}}\end{aligned} \tag{7.9}$$

where

MTBM = mean time between maintenance actions (corrective and preventative)

MDT = mean down time.

Figure 7.7 shows a summary of the elements that could be included within an operational availability calculation.

There are potentially significant life cycle costs associated directly with availability including: loss sales (point-of-sale systems), loss of capacity (in a

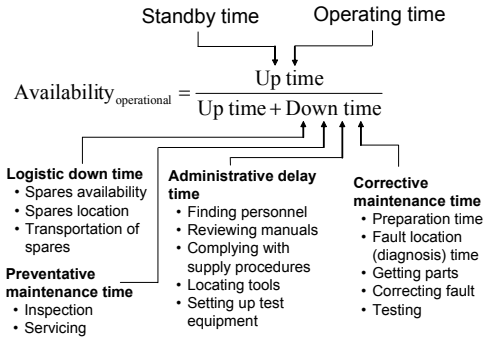


Figure 7.7. Elements included within an operational availability calculation (after [17])

manufacturing operation), loss of customer confidence (*e.g.*, airlines), and loss of mission/assets (military). In addition, many military contracts are now written with availability clauses in them, *e.g.*, the fraction of the contract price paid to the supplier is a function of the availability of the product that the customer actually experiences.

7.2.3 System-level Sparing Analysis

In order to perform a system-level sparing analysis, the number of spares is minimized subject to a required minimum operational availability (alternatively, the availability can be maximized for a fixed set of spares). This type of minimization has been performed numerous ways (*e.g.*, [18–20]). One approach is to compute the number of backorders (expected number of demands that cannot be filled because of lack of spares) [20]. The number of backorders is inversely related to the system availability. It has been shown that if the number of backorders is minimized, the system availability will be maximized [20]. The number of backorders, BO, for exactly x failures with k spares available is given by,

$$BO(x|k) = (x - k). \qquad (7.10)$$

The expected (mean) number of backorders (EBO) for k spares is then given by,

$$EBO(k) = \sum_{x=k+1}^{\infty} (x - k) P(x). \qquad (7.11)$$

Operational availability is the expected fraction of systems that are operational, *i.e.*, not waiting for a spare; and a particular version of operational availability is supply availability, which is computed by approximating MDT as MSD (mean supply delay time) in Equation 7.9. The supply availability can be computed as a function of the expected number of backorders [20],

$$\text{Availability}_{\text{supply}} = \prod_{i=1}^{I} \left(1 - \frac{EBO_i(k_i)}{NZ_i}\right)^{Z_i}, \qquad (7.12)$$

where

$EBO_i(k_i)$ = expected number of backorders for item i with k_i spares
N = number of systems
Z_i = number of instances of item i in the system
I = number of different items in the system.

In Equation 7.12, there are NZ_i instances of item i installed, the probability that one of those fails is $EBO_i(k_i)/NZ_i$, a system is available only if there are no failures (1-…) in all of the Z_i instances of item i in the system (the Z_i exponent), or for any other items (the product of I items).

Consider the example provided in Figure 7.6: λ = 0.5 failures/million hours, if there are k = 0 spares and t = 6 million hours, (7.11) predicts EBO(0) = 3 (3 = (0.5)(6)). If k = 1, then EBO(1) = 2.05 (note, as the number of spares increases, EBO decreases but never gets to zero because the time to failure follows an exponential distribution, (7.2), *i.e.*, it is not exactly 2 million hours ($1/\lambda$) for every instance of every item in every system). If N = 1000, I = 100, and Z_i = 2 (assuming that all the different items in the system have the same reliability and number of instances), then equation (7.12) predicts a supply availability of 81.4%. Conversely, for a minimum required availability, the number of spares, k_i, of ith items in the system can be varied until availability greater than the minimum is obtained.

7.2.4 Warranty Analysis

A warranty is a manufacturer's assurance to a buyer that a product or service is or shall be as represented. A warranty is considered a contractual

agreement between the buyer and the manufacturer entered into upon sale of the product or service. In broad terms, the purpose of a warranty is to establish liability among two parties (manufacturer and buyer) in the event that an item fails. This contract specifies both the performance that is to be expected and the redress available to the buyer if a failure occurs [21].

Warranty cost analysis is performed to estimate the cost of servicing a warranty (so that it can be properly accounted for in the sales price or maintenance contract for the system). Similar to sparing analysis, warranty analysis is focused on determining the number of expected system failures during some period of operation (the warranty period) that will result in a warranty action. Unlike, sparing analysis, warranty analysis does not base its sparing needs on maintaining a specific value for system availability, but only servicing all the warranty claims.

Warranties do not assume that failed items need to be replaced (they may be repairable). Those items that are not repairable need replacement and therefore need spares. Spares may also be needed as "loaners" during system repair.

Warranty analysis differs from sparing in two basic ways. First, warranty analysis usually aims to determine a warranty reserve cost (the total amount of money that has to be reserved to cover the warranty on a product). The cost of servicing an individual warranty claim may vary depending on the type of warranty provided. The simplest case is an unlimited free replacement warranty in which every failure prior to the end of the warranty period is replaced or repaired to its original condition at no charge to the customer. In this case, the warranty reserve fund (ignoring the cost of money) is given by,

$$C_{wr} = C_{fr} + nkC_c, \tag{7.13}$$

where,

- n = quantity of product sold
- C_{fr} = fixed cost of providing warranty coverage
- C_c = recurring replacement/repair cost per produce instance
- k = number of warranty actions, *i.e.*, $\cong \lambda T_w$ or determined from Equations (7.7) or (7.8)
- T_w = length of the warranty.

Other types of warranties also exist. For example some warranties are *pro-rata* – whenever a product fails prior to the end of the warranty period, it is replaced at a cost that is a function of the item's age at the time of failure. If θ is the product price including the warranty then (following a linear depreciation with time), $\theta\left(1-\frac{t}{T_w}\right)$ is the amount of money rebated to a customer for a failure at time t. In this case, the total cost of servicing the warranty assuming a constant failure rate is given by,

$$C_{wr} = \int_0^{T_w} \theta\left(1-\frac{t}{T_w}\right) n\lambda e^{-\lambda t} dt = n\theta\left(1-\frac{1}{\lambda T_w}\left(1-e^{-\lambda T_w}\right)\right). \tag{7.14}$$

Consider a manufacturer of television sets who is going to provide a 12 month *pro-rata* warranty. The failure rate of the televisions is $\lambda = 0.004$ failures per month, n = 500,000, the desired profit margin is 8%, and the recurring cost per television is $112; what warranty reserve fund should be put in place? From Equation (7.14), $C_{wr}/\theta = 11{,}800$. Assuming that the profit margin is on the recurring cost of the television and its effective warranty cost, θ is given by,

$$\theta = (\text{profit margin} + 1)\left(\text{recurring cost} + \frac{C_{wr}}{n}\right), \tag{7.15}$$

and solving for C_{wr} gives $1,464,659, or $2.93/television to cover warranty costs.

The warranty reserve funds computed in Equations (7.13) and (7.14) assume that every warranty action is solved by replacement of the defective product with a new item. If the defective product can be repaired, than other variations on simple warranties can be derived, see [22].

A second way that warranties differ from sparing analysis is that the period of performance (the period in which expected failures need to be counted) can be defined in a more complex way. For example, two-dimensional warranties are common in the automotive industry – 3 years or 36,000 miles, whichever comes first. A common way to represent a two-dimensional warranty is shown in Figure 7.8. Note, many other more

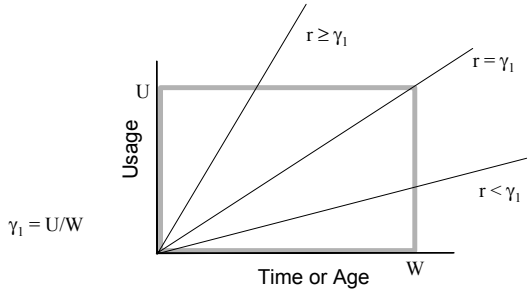


Figure 7.8. A representation of a two-dimensional free-replacement warranty policy

complexly shaped two-dimensional warranty schemes are possible, see [23]. In Figure 7.8, W is the warranty period and U is the usage limit, *i.e.*, unlimited free replacement up to time W or usage U, whichever occurs first from the time of initial purchase. r is called the usage rate (usage per unit time). The warranty ends at U (if r ≥ γ1) or W (if r < γ1). Every failure that falls within the rectangle defined by U and W requires a warranty action. As a result, modeling the number of failures that require warranty actions involves either a bivariate failure model (*e.g.*, [23]), or a univariate model that incorporates the usage rate appropriately (*e.g.*, [24]).

7.3 Technology Obsolescence

A significant problem facing many "high-tech" sustainment-dominated systems is technology obsolescence, and no technology typifies the problem more than electronic part obsolescence, where electronic parts refers to integrated circuits and discrete passive components. In the past several decades, electronic technology has advanced rapidly causing electronic components to have a shortened procurement life span, *e.g.*, Figure 7.9. QTEC estimates that approximately 3% of the global pool of electronic components goes obsolete every month, [26]. Driven by the consumer electronics product sector, newer and better electronic components are being introduced frequently, rendering older components obsolete. Yet, sustainment-dominated systems such as aircraft avionics are often produced for many years

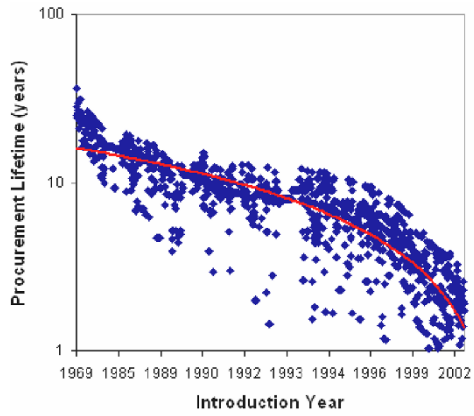


Figure 7.9. Decreasing procurement lifetime for operational amplifiers, [25]. The procurement life is the number of years the part can be procured from its original manufacturer

and sustained for decades. In particular, sustainment-dominated products suffer the consequences of electronic part obsolescence because they have no control over their electronic part supply chain due to their low production volumes. The obsolescence problem for sustainment-dominated systems is particularly troublesome since they are often subject to significant qualification/certification requirements that can make even simple changes to a system prohibitively expensive. This problem is especially prevalent in avionics and military systems, where systems often encounter obsolescence problems before they are fielded and always during their support life, *e.g.*, Figure 7.10.

Obsolescence, also called DMSMS (diminishing manufacturing sources and material shortages), is defined as the loss or impending loss of original manufacturers of items or suppliers of items or raw materials. The key defining characteristic of obsolescence problems is that the products are forced to change (even though they may not need to or want to change) by circumstances that are beyond their control. The type of obsolescence addressed here is caused by the unavailability of technologies (parts) that are needed to manufacture or sustain a product. A different type of obsolescence called "sudden obsolescence" or "inventory obsolescence" refers

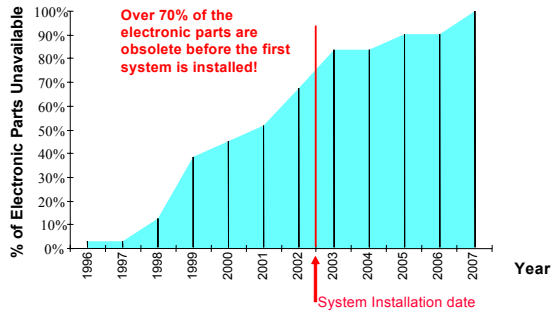


Figure 7.10. Percent of commercial off-the-shelf (COTS) parts that are un-procurable versus the first ten years of a surface ship sonar system's life cycle (courtesy of NAVSURFWARCENDIV Crane)

to the opposite problem in which inventories of parts become obsolete because the system they were being saved for changes so that the inventories are no longer required, see, *e.g.*, [27].

7.3.1 Electronic Part Obsolescence

Electronic part obsolescence began to emerge as a problem in the 1980s when the end of the Cold War accelerated pressure to reduce military outlays and lead to an effort in the United States military called *acquisition reform*. Acquisition reform included a reversal of the traditional reliance on military specifications ("mil-specs") in favor of commercial standards and performance specifications [28]. One of the consequences of the shift away from mil-specs was that mil-spec parts that were qualified to more stringent environmental specifications than commercial parts and manufactured over longer periods of time were no longer available, creating the necessity to use commercial off-the-shelf (COTS) parts that are manufactured for non-military applications and, by virtue of their supply chains being controlled by commercial and consumer products, are usually procurable for much shorter periods of time. Although this history is associated with the military, the problem it has created reaches much further, since many non-military applications depended on mil-spec parts, *e.g.*, commercial avionics, oil well drilling, and industrial equipment.

Most of the emphasis associated with methodology, tool and database development targeted at the management of electronic part obsolescence has been focused on tracking and managing the availability of parts, forecasting the risk of parts becoming obsolete, and enabling the application of mitigation approaches when parts do become obsolete. Most electronic part obsolescence forecasting is based on the development of models for the part's life cycle. Traditional methods of life cycle forecasting utilized in commercially available tools and services are ordinal scale based approaches, in which the life cycle stage of the part is determined from an array of technological attributes, *e.g.*, [29, 30], and are available in commercial tools such as TACTRAC™, Total Parts Plus™, and Q-Star™. More general models based on technology trends have also appeared including a methodology based on forecasting part sales curves [31], leading-indicator approaches [32], and data mining based solutions [33]. The OMIS tool, [34], consolidates demand and inventory, and combines it with obsolescence risk forecasting. A few efforts have also appeared that address non-electronic part obsolescence forecasting, *e.g.*, [35, 36].

7.3.2 Managing Electronic Part Obsolescence

Many mitigation strategies exist for managing obsolescence once it occurs [37]. Replacement of parts with non-obsolete substitute or alternative parts can be done as long as the burden of system re-qualification is not unreasonable. There are also a plethora of aftermarket electronic part sources ranging from original manufacturer authorized aftermarket sources that fill part needs with a mixture of stored devices (manufactured by the original manufacturer) and new fabrication in original manufacturer qualified facilities (*e.g.*, Rochester Electronics and Lansdale Semiconductor) to brokers and even eBay. Obviously buying obsolete parts on the secondary market from non-authorized sources carries its own set of risks [38]. David Sarnoff Laboratories operate GEM and AME, [39], which are electronic part emulation foundries that fabricate obsolete parts that meet original part qualification standards using newer technologies (BiCMOS gate arrays).

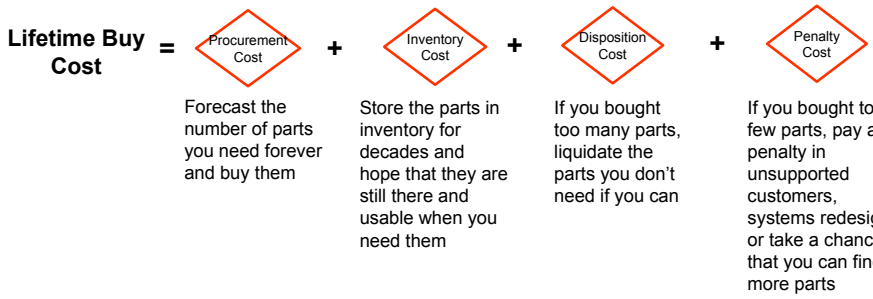


Figure 7.11. Lifetime buys made when parts are discontinued are a popular electronic part obsolescence mitigation approach, but are also plagued by uncertainties in demand forecasting and fraught with hidden costs

Thermal uprating of commercial parts to meet the extended temperature range requirements of an obsolete mil-spec part is also a possible obsolescence mitigation approach [40].

Most semiconductor manufactures notify customers and distributors when a part is about to be discontinued providing customers 6–12 months of warning and giving them the opportunity to place a final order for parts, *i.e.*, a "lifetime buy". Ideally, users of the part determine how many parts will be needed to satisfy manufacturing and sustainment of the system until the end of the system's life and place a last order for parts. The tricky problem with lifetime buys of electronic parts is determining the right number of parts to purchase. For inexpensive parts, lifetime buys are likely to be well in excess of forecasted demand requirements because the cost of buying too many is small and minimum purchase requirements associated with the part delivery format. However, for more expensive parts, buying excess inventory can become prohibitively expensive. Unfortunately, forecasting demand and sparing requirements for potentially 10–20 years or longer into the future is not an exact science, and predicting the end of the product life is difficult. Stockpiling parts for the future may also incur significant inventory and financial expenses. In addition, the risk of parts being lost, un-usable when needed, or used by another product group (pilfered), are all very real occurrences for electronic part lifetime buys that may need to reside in inventory for decades. Figure 7.11 shows lifetime buy cost drivers. A method of optimizing lifetime buys is presented in [41].

The obsolescence mitigation approaches discussed in the preceding paragraph are *reactive* in nature, focused on minimizing the costs of obsolescence mitigation, *i.e.*, minimizing the cost of resolving the problem after it has occurred. While reactive solutions will always play a major role in obsolescence management, ultimately, higher payoff (larger sustainment cost avoidance) will be possible through *strategic* oriented methodology/tool development efforts [42].

If information regarding the expected production lifetimes of parts (with appropriate uncertainties considered) is available during a system's design phase, then more strategic approaches that enable the estimation of lifetime sustainment costs should be possible, and even with data that is incomplete and/or uncertain, the opportunity for sustainment cost savings is still potentially significant with the application of the appropriate decision making methods.

Two types of strategic planning approaches exist: material risk indices and design refresh planning. Material risk index (MRI) approaches analyze a product's bill of materials and scores a supplier-specific part within the context of the enterprise using the part, *e.g.*, [43]. MRIs are used to combine the risk prediction from obsolescence forecasting with organization-specific usage and supply chain knowledge in order to estimate the magnitude of sustainment dollars put at risk within a customer's organization by the part's obsolescence. The other type of strategic planning approach is design refresh planning, which is discussed in the next section.

7.3.3 Strategic Planning – Design Refresh Planning

Because of the long manufacturing and field lives associated with sustainment-dominated systems, they are usually refreshed or redesigned one or more times during their lives to update functionality and manage obsolescence. Unlike high-volume commercial products in which redesign is driven by improvements in manufacturing, equipment or technology, for sustainment-dominated systems, design refresh is often driven by technology obsolescence that would otherwise render the product un-producible and/or un-sustainable.

Ideally, a methodology that determines the best dates for design refreshes, and the optimum mixture of actions to take at those design refreshes is needed. The goal of refresh planning is to determine:

- When to design refresh
- What obsolete system components should be replaced at a specific design refresh (*versus* continuing with some other obsolescence mitigation strategy)
- What non-obsolete system components should be replaced at a design refresh

Numerous research efforts have worked on the generation of suggestions for redesign in order to improve manufacturability. Redesign planning has also been addressed outside the manufacturing area, *e.g.*, general strategic replacement modeling, re-engineering of software, capacity expansion, and equipment replacement strategies. All of this work represents redesign driven by improvements in manufacturing, equipment or technology (*i.e.*, strategies followed by leading-edge products), not design refresh driven by technology obsolescence that would otherwise render the product un-producible and/or un-sustainable. It should also be noted that manufacturers and customers of sustainment-dominated systems have as much interested in "design refresh" as "redesign".[1]

The simplest model for performing life cycle planning associated with technology obsolescence (explicitly electronic part obsolescence) was developed by Porter [45]. Porter's approach focuses on calculating the net present value (NPV) of last time buys[2] and design refreshes as a function of future date. As a design refresh is delayed, its NPV decreases and the quantity (and thereby cost) of parts that must be purchased in the last time buy required to sustain the system until the design refresh takes place increases. Alternatively, if design refresh is scheduled relatively early, then last time buy cost is lower, but the NPV of the design refresh is higher. In the simplest form of a Porter model, the cost of the last time buy (C_{LTB}) is given by,

$$C_{LTB} = P_0 \sum_{i=0}^{Y_R} N_i \,, \tag{7.16}$$

where

P_0 = price of the obsolete part in the year of the lifetime buy (year 0)
Y_R = year of the design refresh (0 = present year, 1 = 1 year from now, *etc*.)
N_i = number of parts needed in year i.

Equation (7.16) assumes that the part becomes obsolete in year 0 and that the last time buy is made in year 0.

The design refresh cost for a refresh in year Y_R (in year 0 dollars), C_{DR}, is given by,

$$C_{DR} = \frac{C_{DRI_{Y_R}}}{(1+d)^{Y_R}} \,, \tag{7.17}$$

where

$C_{DRI_{Y_R}}$ = inflation adjusted design refresh cost in year Y_R
d = discount rate.

The total cost for managing the obsolescence with a year Y_R refresh is given by,

$$C_{Total} = C_{LTB} + C_{DR} \,. \tag{7.18}$$

[1] Technology refresh refers to changes that "have To be done" in order for the system functionality to remain useable. Redesign or technology insertion means "want to be done" system changes, which include new technologies to accommodate system functional growth and new technologies to replace and improve the existing functionality of the system, see [44].

[2] A last time buy (also called a bridge buy) means procuring and storing enough parts to sustain manufacturing and fielded units until the next design refresh.

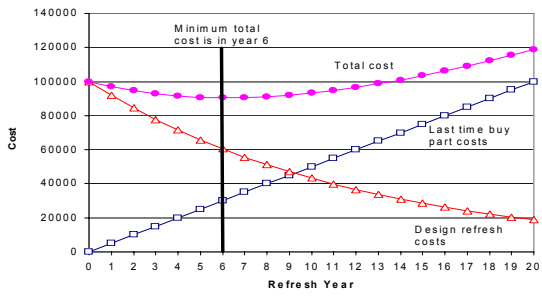


Figure 7.12. Example application of Porter's refresh costing model

Figure 7.12 shows a simple example using the Porter model. In this case C_{DRI_0} = \$100,000, d = 12%, N_i = 500 (for all i), P_0 = \$10 and an inflation rate of 3% was assumed. In this simple example, the model suggests that the optimum design refresh point is in year 6.

The Porter model performs its tradeoff of last time buy costs and design refresh costs on a part-by-part basis. While the simple Porter approach can be extended to treat multiple parts, and a version of Porter's model has been used to plan refreshes in conjunction with lifetime buy quantity optimization in [46], it only considers a single design refresh at a time. In order to treat multiple refreshes in a product's lifetime, Porter's analysis can be reapplied after a design refresh to predict the next design refresh, effectively optimizing each individual design refresh, but the coupled effects of multiple design refreshes (coupling of decisions about multiple parts *and* coupling of multiple refreshes) in the lifetime of a product are not accounted for, which is a significant limitation of the Porter approach.

A more complete optimization approach to refresh planning called MOCA has been developed that optimizes over multiple refreshes and multiple obsolescence mitigation approaches (the Porter model only considers last time buys) [47]. Using a detailed cost analysis model, the MOCA methodology determines the optimum design refresh plan during the field-support-life of the product. The design refresh plan consists of the number of design refresh activities, their content and respective calendar dates that minimize the life cycle sustainment cost of the product.

Figure 7.13 shows the MOCA design refresh planning timeline. Fundamentally, the model supports a design through periods of time when no parts are obsolete, followed by multiple part-specific obsolescence events. When a part becomes obsolete, some type of mitigation approach must take effect immediately: If sufficient inventory exists, a lifetime buy of the part is made or some other short-term mitigation strategy that only applies until the next design refresh. Next there are periods of time when one or more parts are

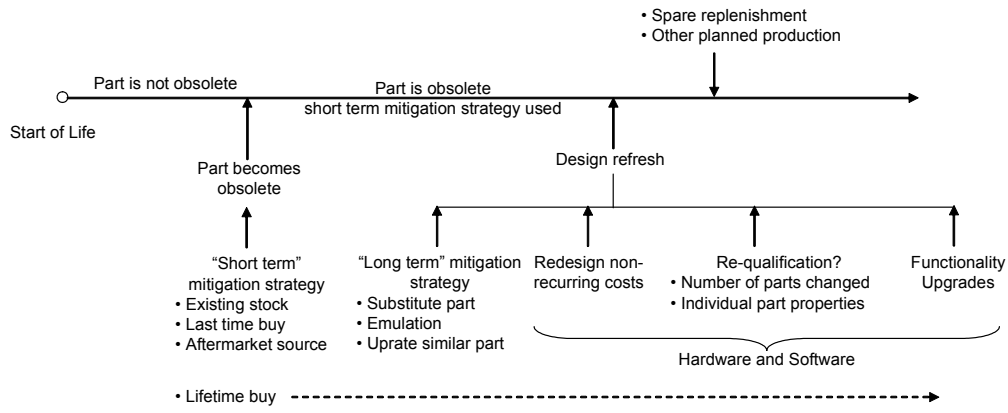


Figure 7.13. Design refresh planning analysis timeline (presented for one part only, for simplicity, however in reality, there are coupled parallel timelines for many parts, and design refreshes and production events can occur multiple times and in any order)

obsolete, and short-term mitigation approaches are in place on a part-specific basis. When design refreshes are encountered the change in the design at the refresh must be determined and the costs associated with performing the design refresh are computed. At a design refresh, a long-term obsolescence mitigation solution is applied (until the end of the product life or possibly until some future design refresh), and non-recurring, recurring, and re-qualification costs are computed. Re-qualification may be required depending on the impact of the design change on the application – the necessity for re-qualification depends on the role that the particular part(s) play and/or the quantity of non-critical changes made. The last activity appearing on the timeline is production. Systems often have to be produced after parts begin to go obsolete due to the length of the initial design/manufacturing process, additional orders for the system, and replenishment of spares.

The MOCA methodology can be used during either a) the original product design process, or b) to make decisions during system sustainment, *i.e.*, when a design refresh is underway, determine what the best set of changes to make given an existing history of the product and forecasted future obsolescence and future design refreshes. See [47], for refreshing planning analyses using MOCA.

7.3.4 Software Obsolescence [48]

In most complex systems, software life cycle costs contribute as much or more to the total life cycle cost as the hardware, and the hardware and software must be co-sustained. Software obsolescence is usually caused by one of the following:

1. Functional obsolescence: Hardware, requirements, or other software changes to the system, obsolete the functionality of the software (includes hardware obsolescence precipitated software obsolescence; *and* software that obsoletes software).
2. Technological obsolescence: The sales and/or support for COTS software terminates:
   - The original supplier no longer sells the software as new
   - The inability to expand or renew licensing agreements (legally unprocurable)
   - Software maintenance terminates – the original supplier and third parties no longer support the software
3. Logistical obsolescence: Digital media obsolescence, formatting, or degradation limits or terminates access to software.

Analogously, hardware obsolescence can be categorized similarly to software obsolescence: functional obsolescence in hardware is driven by software upgrades that will not execute correctly on the hardware (*e.g.*, Microsoft Office 2005 will not function on a 80486 processor based PC); technological obsolescence for hardware means that more technologically advanced hardware is available; and logistical obsolescence means that you can no longer procure a part.

Although some proactive measures can be taken to reduce the obsolescence mitigation footprint of software including: making codes more portable, using open-source software, and third-party escrow where possible; these measures fall short of solving the problem and it is not practical to think that software obsolescence can somehow be avoided. Just like hardware, military and avionics systems have little or no control over the supply chain for COTS software or much of the software development infrastructure they may depend upon for developing and supporting organic software. Need proof? Consider the following quote from Bill Gates [49]: "The only big companies that succeed will be those that obsolete their own products before someone else does." Obviously, Microsoft's business plan is driven by motivations that do not include minimizing the sustainment footprint of military and avionics systems.

In the COTS world, hardware and software have developed a symbiotic supply chain relationship where hardware improvements drive software manufactures to obsolete software, which in turn cause older hardware to become obsolete – from Dell and Microsoft's viewpoint, this is a win-win strategy. Besides COTS software (hardware specific and non-hardware specific), system sustainment depends on organic application software, software that provides infrastructure for

hardware and software development and testing, and software that exists at the interfaces between system components (enabling interoperability. While hardware obsolescence precipitated software obsolescence is becoming primarily an exercise in finding new COTS software (and more often COTS software and new hardware are bundled together), the more challenging software obsolescence management problem is often found at the interfaces between applications, applications and the operating system, and drivers. One particular class of functional obsolescence of software that is becoming increasingly troublesome for many systems is security holes.

In reality, obsolescence management is a hardware/software co-sustainment problem, not just a hardware sustainment problem. Software obsolescence (and its connection to hardware obsolescence) is not well defined and current obsolescence management strategic planning tools are not generally capable of capturing the connection between hardware and software. For additional information on various aspects of software obsolescence, readers are encouraged to refer to [50, 51].

7.4 Technology Insertion

Each technology used in the implementation of a system (*i.e.*, hardware, software, the technologies used to manufacture and support the system, information, and intellectual property) can be characterized by a life cycle that begins with introduction and maturing of the technology, and ends in some type of unavailability (obsolescence). The developers of sustainment-dominated systems must determine when to get off one technology's life cycle curve and onto another's in order to continue supporting existing systems and accommodate evolving system requirements, (Figure 7.14).

In order to manage the insertion of new technologies into a system, organizations need to maintain an understanding of technology evolution and maturity ("technology monitoring and forecasting"), measure the value of technology changes to their systems ("value metrics"), and build strategic plans for technology changes they wish to incorporate ("roadmapping").

7.4.1 Technology Monitoring and Forecasting

Attempts to predict the future of technology and to characterize its affects have been undertaken by many different organizations, which use many different terms to describe their forward-looking actions.

These terms include "technological intelligence", "technology foresight", "technology opportunities analysis (TOA)" [53], "competitive technological intelligence", and "technology assessment" [54]. These terms fall under two, more general umbrella terms: "technology monitoring" and "technology forecasting". To monitor is "to watch, observe, check and keep up with developments, usually in a well-defined area of interest for a very specific purpose" [55]. Technology monitoring is the process of observing new technology developments and following up on the

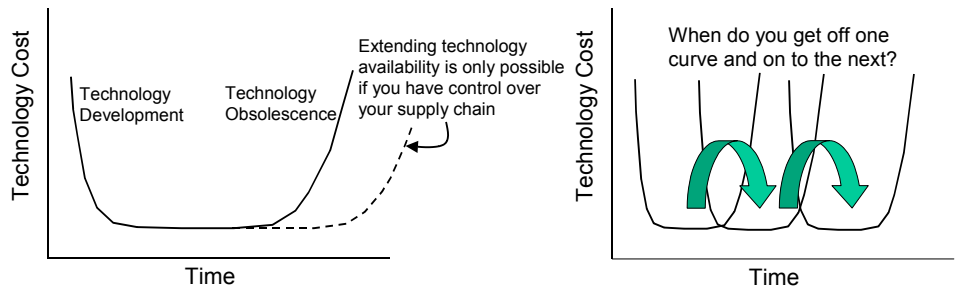


Figure 7.14. Supporting systems and evolving requirements [52]

developments that are relevant to an organization's goals and objectives. Technology forecasting, like technology monitoring, takes stock of current technological developments, but takes the observation of technology a step further by projecting the future of these technologies and by developing plans for utilizing and accommodating them.

For high-volume consumer oriented products, there are many reasons for organizations to monitor and forecast technological advances. First, when the organization's products are technologically-based, a good understanding of a nascent technology is needed as early as possible in order to take advantage of it. Additionally, monitoring and forecasting technology allows organizations to find applications for new technology [54], manage the technologies that are seen as threats, prioritize research and development, plan new product development, and make strategic decisions [56]. For manufacturers of sustainment-dominated products, monitoring and forecasting technology is of interest for the reasons listed above and also to enable prediction of obsolescence of the currently used technologies. The primary method for locating and evaluating materials relevant to technology monitoring is a combination of text mining and bibliometric analysis. These methods monitor the amount of activity in databases on certain specified topics and categorize the information found into graphical groupings. Because of the amount of literature available on a given technology, much of the text mining process has been automated and computerized. Software is used to monitor data bases of projects, research opportunities, publications, abstracts, citations, patents, and patent disclosures [56]. The general methodology for the automated text mining process is summarized in Figure 7.15.

The monitoring process involves identifying relevant literature by searching text that has been converted into numerical data [57]. Often there are previously defined search criteria and search bins where results can be placed. After literature has been found it must be clustered [58] with similar findings and categorized into trends. The data is categorized using decision trees, decision rules, k-nearest neighbors, Bayesian approaches, neural networks, regression models and vector-based models [57]. This categorization allows hidden relationships and links between data sets to be determined, and helps locate gaps in the data, [58]. Once the data has been grouped, it is organized graphically in a scatter-plot form. Each point on the scatter plot can represent either a publication or an author. These points can be linked or grouped together to show the relationships and similarities between points.

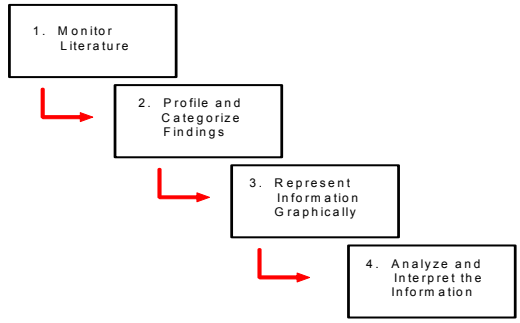


Figure 7.15. Steps in the technology monitoring process

The monitored data must then be interpreted and analyzed to determine which new technologies are viable and relevant. To do this, many organizations network with experts in related fields, and they employ surveys and other review techniques similar to the Delphi method [59] to force consensus among the experts. Expert opinion allows organizations to assess the implications of a new technology, and it is the first step in planning and taking action to cope with the benefits and risks associated with a new technology [53].

Technology monitoring and forecasting methods are still relatively new and untested, especially for larger databases of documents. Automated methods of forecasting and monitoring need to be refined and improved upon before they truly perform as they are intended to. Additionally, these tools will need to operate on a larger scale and in a more diverse environment. Also, many organizations will begin to seek customer and client input when monitoring and forecasting. Finally, forecasts will eventually be evaluated against global, political, environmental, and social trends [54], placing them in a broader context, and expanding their uses beyond single organizations.

7.4.2 Value Metrics and Viability

Value is used to refer to the relative usefulness of an object, technology, process, or service. In the case of a system, value is the relative benefit of some or all of the following: acquiring, operating, sustaining, and disposing of the system. One way to represent value is shown in Figure 7.16 [60]. The "attributes" axis includes measures of the application-specific direct product value. The "conditions" axis includes details of the product usage and support environment. In simplified models, the conditions axis provides the weights and constraints that govern how the attributes are combined together. The "time" axis is the "instantaneous time value", *i.e.*, value at a particular instant in time. Particular attributes may be weighted more than other attributes and their relative weightings are functions of time. For example, the value attributes during the final 20 seconds of a torpedo's life are weighted differently than the value attributes during its prior ten year storage life. All three axes in Figure 7.16 can be integrated. For example, if you integrate over the time (instantaneous time value) axis, you get "sustainability value". Integrating over the time axis tells you things about value attributes like "total cost of ownership" and availability. You could also integrate over the conditions axis, which would give you a measure how you are balancing multiple stockholder's conflicting requirements. Integration along the attributes axis builds composite value metrics.

A special case of Figure 7.16 is viability that addresses the application-specific impact of technology decisions on the life cycle of a system [52]. The objective of evaluating viability is to enable a holistic view of how the technology (and specific product) decisions made early in the design process impact the life cycle affordability of a system solution.

We define viability as a monetary and non-monetary quantification of application-specific risks and benefits in a design/support environment that is highly uncertain. The definition of viability used in this discussion is a combination of economics and technical "value", but assumes that technical feasibility has already been achieved. Traditional "value" metrics go part of the way

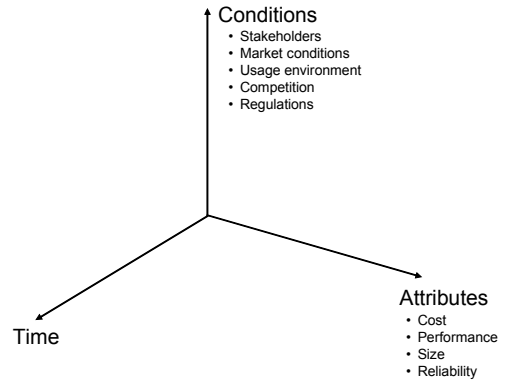


Figure 7.16. Three-dimensional value proposition [60]

toward defining viability by providing a coupled view of performance, reliability and acquisition cost, but is generally ignorant of how product sustainment may be impacted. We require a viability metric that measures both the value of the technology refreshment and insertion, *and* the degree to which the proposed change impacts the system's current and future affordability and capability needs. This viability assessment must include hardware, software, information and intellectual property aspects of the product design. Viability therefore goes beyond just an assessment of the immediate or near-term impacts of a technology insertion, in that it evaluates the candidate design (or candidate architecture) over its entire lifetime.

Although *viability* can be defined in many ways, its underlying premise is that economic well-being is inextricably linked to the sustainability of the system. According to studies conducted for the United States Air Force Engineering Directorate [11] viability assessment must include:

- *Producibility* – The ability to produce the system in the future based upon the "current" architecture and design implementation. (production and initial spares, not replenishment spares).
- *Supportability* – The ability to sustain the system and meet the required operational capability rates. This includes repair and re-supply as well as non-recurring redesign for supportability of the "as is" design implementation and performance.

- *Evolvability (Future Requirements Growth)* – The ability of the system to support projected capability requirements with the "current" design. This includes capability implemented by hardware *and* software updates.

The critical steps to making use of viability concepts in decision making are:

1) Identifying practical and measurable indicators of viability
2) Understanding how the indicators can be measured as a function of decisions made (*and* time passed)
3) Managing the necessary qualitative and quantitative information (with associated uncertainty) needed to evaluate the indicators
4) Performing the evaluation (possibly linked to other analyses/tools that are used early in the design process).

The viability of each technology decision made, whether during the initial design of a product or during a redesign activity, should be evaluated. Viability is formulated from a mix of many things including the following two critical elements:

- *Technology life cycle* – the life cycle of various technology components (for example electronic parts) has been modeled and can be represented, *e.g.*, technical life cycle maturity, life codes and obsolescence dates. The life cycle forecast may be dynamic and change (with time) in response to some form of technology surveillance program. In general, this metric is not application specific (and only hardware-part specific at this time). This concept, however, could be extended in two ways: 1) for a "technology group", *i.e.*, computers, memory, bus architectures, sensors, databases, middleware, operating systems, *etc*. A "scaled-up" version of life cycle forecasting could provide a maturity metric for a technology grouping versus a specific application that uses one (or a combination of) technology groups; and 2) for non-hardware components such as software, information and intellectual property.[3] No present methodologies or tools are capable of assessing a particular technology category and mapping evolutions against the 30, 40 or 50 year life cycles that military systems and platforms are expected to perform.
- *Associativity* – the second element is the impact of a particular technology's modification on the specific application. As an example, one technology may be late in its life cycle, but the impact of changing it on the application is low (making it a candidate for consideration), *i.e.*, it is not in the critical path for qualification or certification, it does not precipitate any other changes to the application, or it is modularized in such a way as to isolate its impact on the rest of the system, *i.e.*, a timing module that provides synchronization can be easily changed without impacting on any other part in the system and thus no associativity. On the other hand, other technologies (at the same point in their life cycle) may be central to everything (such as an operating system or bus architecture) and therefore have high associativity.[4]

When formulating the indicators of viability, the methodology must accommodate the fact that there

[3] For example, electronic part obsolescence forecasting benefits from the commonality of parts in many systems, non-electronic part obsolescence cannot take advantage of this situation, and therefore, common commercial approaches that depend on subjective supply chain information will likely be less useful for general non-electronic and non-hardware obsolescence forecasting.

[4] This is important as we begin to consider the affordability of a technology refresh or insertion. It is also important to identify the "critical system elements"; one way to do this is by using acquisition cost multiplied by the quantity needed in a system. But an operating system is relatively inexpensive and yet very critical. Thus the "value" of the operating system is *not* just its acquisition cost multiplied by its quantity, but should also sum all of the acquisition costs (multiplied by quantities) of all effected parts of the system refreshment. This would be done for each element in the system bill of materials, and thus a new sorting of the bill of materials would highlight the "system critical elements" by their impact to change. System critical really refers to "difficulty to change based on affordability". This is also important because technology management represents a cost, and thus must focus on the system elements that drive cost.

are many stakeholders who all possess different portions of the knowledge necessary to accurately evaluate the viability of a specific choice or decision. Another difficulty is that the information necessary to make the decision is generally incomplete, and consists of qualitative and quantitative content and their associated uncertainties. Thus viability evaluation represents an information fusion problem.[5]

7.4.3 Roadmapping

Technology roadmapping is a step in the strategic planning process that allows organizations to systematically compare the many paths toward a given goal or result while aiding in selecting the best path to that goal.

Many organizations have been forced to increase their focus on technology as the driver behind their product lines and business goals. This is different from the focus on customer wants and needs and the competitive demands that have previously determined the path of an industry. Technology roadmaps are seen as a way to combine customer needs, future technologies, and market demands in a way that is specific to the organization, and enables mapping a specific plan for technologies and the products and product lines they will affect.

Physically, the nodes and links depicted in roadmaps contain quantitative and qualitative information regarding how science, technology, and business will come together in a new or novel way to solve problems and reach the organization's end goal [61]. The time domain factors into the roadmap because it takes time for new technologies to be discovered, become mature, and be incorporated into a product, and for market share to grow to encompass new products, or for new possibilities to arise. In essence, technology roadmaps are graphical representations of the complex process of "identifying, selecting, and developing technology alternatives to satisfy a set of product needs" [62].

It is important to note that, like their real world counterparts, technology roadmaps are not just needs driven documents (as in, "I need to get somewhere, what direction do I go?") but can also be based on current position (as in, "where could we go from here?"). It should also be stressed that roadmapping is an iterative process and that roadmaps must be continually maintained and kept up to date [63]. This is because the information contained in the roadmaps will change as time passes and new paths emerge or old paths disappear, and because an iterative roadmapping process will lead to a mature roadmap with clear requirements and fewer unknowns [64]. An iterative roadmapping process also leads to better understanding and standardization of the process, allowing roadmaps to be created more quickly, and the information in them to be more valuable.

Regardless of the type of roadmap and the information it contains, all roadmaps seek to answer three basic questions [64]:

1) Where are we going?
2) Where are we now?
3) How can we get there?

The process of creating a roadmap should answer these questions by listing and evaluating the possible paths to an end goal, and result in the selection of a single path to focus funding and resources on. Despite selecting a 'final path', companies should remain open minded and keep alternative paths open in case a poor decision has been made. This is yet another reason to continually update the roadmap, since it serves as a mechanism to correct previous bad decisions.

Developing strategies and roadmaps that leverage technology evolution has been of interest for some time. The difficulty with historic roadmapping-based strategies is that they are 1) inherently not application-specific and 2) tend to focus more on accurately forecasting the start of the technology life (when the technology becomes available and mature) and ignore the end of the technology life (obsolescence). While this roadmapping approach may be acceptable for those

[5] Information fusion is the seamless integration of information from disparate sources that results in an entity that has more value (and less uncertainty) than the individual sources of information used to create it. Fused information is information that has been integrated across multiple data collection "platforms" (soft and hard) and physical boundaries, then blended thematically, so that the differences in resolution and coverage, treatment of a theme, character and artifacts of data collection methods are eliminated.

product sectors where there is no requirement for long-term sustainment (*e.g.*, consumer electronics), it is not acceptable to sustainment-dominated product sectors. Thus the process of roadmapping will need to grow and develop if it is to be used by the sustainment industry. Since product roadmapping is still a relatively new process it will gradually become more application specific and more defined as time passes.

The design refresh planning tool discussed in Section 7.4, MOCA, has been extended to include technology roadmapping constraints [65]. MOCA maps technology roadmap constraints into 1) timing constraints on its timeline, *i.e.*, periods of time when one or more refreshes (redesigns) must take place in order to satisfy technology insertion requirements; and 2) constraints on which parts or groups of parts must be addressed at certain refreshes (redesigns); and 3) additional costs for redesign activities.

7.5 Concluding Comments

Over the past 20 years, the use of the term sustainability has been expanded and applied to the management of environmental, business, and technology issues. In the case of environmental and business, sustainability often refers to balancing or integration of issues [1], while for technology its meaning is much closer to the root definition meaning to maintain or continue.

For many systems the largest single expenditure is for operation and support. Sustainment of military equipment was recognized as early as the 6th century BC as a significant cost driver by Sun-tzu in the Art of War [66]: "Government expenses for broken chariots, worn-out horses, breast-plates and helmets, bows and arrows, spears and shields, protective mantles, draught oxen and heavy wagons, will amount to four-tenths of its total revenue." Today it is not just military systems but many other systems ranging from avionics to traffic lights and the technology content in rides at amusement parks.

Failure to proactively sustain the technological content of systems is no longer an option for many types of systems. System evolution is not free and also cannot be avoided, proactive solutions are required in order to maintain market share and/or affordably provide continued system support and operation.

References

[1] Sutton P. What is sustainability? Eingana 2004; Apr, 27(1):4–9.

[2] Costanza R. Ecological economics: the science and management of sustainability. Columbia University Press, 1991.

[3] Brundtland Commission, Our common future. World Commission on Environment and Development, 1987.

[4] ForestERA, http://www.forestera.nau.edu/glossary.htm

[5] Elkington J. Cannibals with forks: The triple bottom line of 21st century business. Capstone Publishing, Oxford, 1997.

[6] Kleindorfer PR, Singhal K, Van Wassenhove LN. Sustainable operations management. Production and Operations Management 2005; winter, 14(4):482–492.

[7] Crum D. Legacy system sustainment engineering. Proceedings of the DoD Diminishing Manufacturing Sources and Material Shortages Conference, New Orleans, LA, March 2002. Available at: http://smaplab.ri.uah.edu/dmsms02/ presentations/crum.pdf

[8] Cost Analysis Improve Group (CAIG), Operating and support cost-estimating guide. Office of the Sec. of Defense, http://www.dtic.mil/pae/, May 1992.

[9] Gateway Inc., www.gateway.com, December 2001.

[10] Shields P. Total cost of ownership: Why the price of the computer means so little. http://www.thebusinessmac.com/ features/tco_hardware.shtml, December 2001.

[11] Ardis B. Viable/affordable combat avionics (vca) implementation update. Dayton Aerospace, Inc., June 2001.

[12] Reliability and support factors. http://home.wanadoo.nl/jdonders/AVAIL.html

[13] Myrick A. Sparing analysis – A multi-use planning tool, Proceedings of the IEEE Reliability and Maintainability Symposium, Philadelphia, PA, 1989; January 296–300.

[14] McDougall R. Availability – What I means, why it's important, and how to improve it. Sun Blue Prints OnLine, Oct. 1999, http://www.sun.com/ blueprints/1099/ availability.pdf

[15] Performance based logistics: A program manager's product support guide. Defense Acquisition University Press, Fort Belvoir, VA, March 2005, http://www.dau.mil/ pubs/misc/PBL_Guide.pdf

[16] Lie CH, Hwang CL, Tillman, FA. Availability of maintained systems: A state-of-the-art survey. AIIE Trans. 1977; 9(3):247–259.

[17] LM-720 Reliability, availability, & maintainability (RAM) (hardware and software). https://acc.dau.mil/getattachment.aspx?id=22523&pname=file&aid=2212

[18] Coughlin RJ, Optimization of spares in a maintenance scenario. Proceedings of the IEEE Reliability and Maintainability Symposium, San Francisco, CA, 1984; January, 371–376.

[19] Adams CM. Inventory optimization techniques, system *vs*. item level inventory analysis. Proceedings of the IEEE Reliability and Maintainability Symposium, Los Angeles, CA, 2004; January, 55–60.

[20] Sherbrooke CC. Optimal inventory modeling of systems: ulti-echelon techniques. Wiley, New York, 1992.

[21] Murthy DNP, Djamaludin I. New product warranty: A literature review. Int. Journal of Production Economics 2002; 79(3):231–260.

[22] Elsayed EA, Reliability engineering. Addison Wesley, Reading, MA, 1996.

[23] Blischke WR, Murthy DNP, Warranty cost analysis. Marcel Dekker, New York, 1994.

[24] Hunter JJ. Mathematical techniques for warranty analysis. Product warranty handbook. Blishke WR, Murthy DNP, editors. Marcel Dekker, New York, 1996; Chapter 7:157-190.

[25] Feldman K, Sandborn P. Integrating technology obsolescence considerations into product design planning. Proceedings of the ASME Design for Manufacturing and Life Cycle Conference, Las Vegas, NV 2007; September.

[26] QTEC, http://www.qtec.us/Products/QStar_Introduction.htm, 2006.

[27] Masters JM. A note on the effect of sudden obsolescence on the optimal lot size. Decision Sciences 1991; 22(5): 1180–1186.

[28] Perry W. (1994), U.S. Secretary of Defense.

[29] Henke AL, Lai S. Automated parts obsolescence prediction. Proceedings of the DoD DMSMS Conference, San Antonio, TX, 1997; August.

[30] Josias C, Terpenny JP, McLean KJ. Component obsolescence risk assessment. Proceedings of the IIE Industrial Engineering Research Conference (IERC), Houston, TX, 2004; May.

[31] Solomon R, Sandborn P, Pecht M. Electronic part life cycle concepts and obsolescence forecasting. IEEE Trans. on Components and Packaging Technologies 2007; Dec., 23:707–713.

[32] Meixell M, Wu SD. Scenario analysis of demand in a technology market using leading indicators. IEEE Trans. on Semi. Manuf. 2001; 14:65-78.

[33] Sandborn P, Mauro F, Knox R, A data mining based approach to electronic part obsolescence forecasting. IEEE Trans. on Components and Manufacturing Technology. 2007; 30:397-401.

[34] Tilton JR. Obsolescence management information system (OMIS). http://www.jdmag.wpafb.af.mil/elect%20obsol%20mgt.pdf, NSWC Keyport.

[35] Howard MA. Component obsolescence – It's not just for electronics anymore. Proceedings of the Aging Aircraft Conference, San Francisco, CA, 2002; September.

[36] ARINC, Inc., ARINC Logistics assessment and risk management (ALARM) tool, http://www.arinc.com/ news/2005/06-28-05.html

[37] Stogdill RC. Dealing with obsolete parts. IEEE Design & Test of Computers 1999; 16:17–25.

[38] Pecht M, Tiku S. Electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectrum 2006; May:43(5):37–46.

[39] Johnson W. Generalized emulation of microcircuits. Proceedings of the DoD DMSMS Conference, Jacksonville, FL, 2000; August.

[40] Pecht M, Humphrey D. Uprating of electronic parts to address obsolescence. Microelectronics International 2006; 23(2):32–36.

[41] Feng D, Singh P, Sandborn P. Lifetime buy optimization to minimize lifecycle cost. Proceedings of the Aging Aircraft Conference, Palm Springs, CA 2007; April.

[42] Sandborn P. Beyond reactive thinking – We should be developing pro-active approaches to obsolescence management tool. DMSMS COE Newsletter 2004; 2 (3): 4–9.

[43] Robbins RM. Proactive component obsolescence management. A-B Journal 2003; 10:49–54.

[44] Herald TE. Technology refreshment strategy and plan for application in military systems – A how-to systems development process and linkage with CAIV. Proc. National Aerospace and Electronics Conference (NAECON), Dayton, OH, 2000; October: 729–736.

[45] Sandborn P, Herald T, Houston J, Singh, P. Optimum technology insertion into systems based on the assessment of viability. IEEE Trans. on Comp. and Pack. Tech 2003; 26:734–738.

[46] Porter GZ. An economic method for evaluating electronic component obsolescence solutions. Boeing Company White Paper 1998.
[47] Cattani KD, Souza GC. Good buy? Delaying end-of-life purchases. European J. of Operational Research 2003; 146:216–228.
[48] Singh P, Sandborn P. Obsolescence driven design refresh planning for sustainment-dominated systems. The Engineering Economist 2006; April–June, 51(2):115–139.
[49] Sandborn P. Software obsolescence – complicating the part and technology obsolescence management problem. IEEE Trans. On Comp. and Pack. Tech 2007; 30:886-888.
[50] Gates B. Founder, Chairman, Microsoft Corp. The Bill Gates method. APT News July 21, 2003.
[51] Merola L. The COTS software obsolescence threat. Proceedings of the International Conference on Commercial-off-the-shelf (COTS) Based Software Systems, Orlando, FL, 2006; February.
[52] Rickman T, Singh G. Strategies for handling obsolescence, end-of-life and long-term support of COTS software. COTS Journal, Jan. 2002; 17–21.
[53] Porter AL, Jin X-Y, *et al.*, Technology opportunities analysis: Integrating technology monitoring, forecasting, and assessment with strategic planning. SRA J. 1994; Oct., 26(2):21–31.
[54] Coates V, Faroque M, Klavins R, Lapid K, Linstone HA, Pistorius C, *et al*., On the future of technological forecasting. Technology Forecasting and Social Change 2001; 67(1):1–17.
[55] Porter AL, Detampel MJ. Technology opportunities analysis. Tech. Forecasting and Social Change 1995; July, 49(3):237–255.
[56] Zhu D, Porter AL. Automated extraction and visualization of information for technological intelligence and forecasting. Technological Forecasting and Social Change 2002; June, 69(5):495–506.
[57] Teichert T, Mittermayer MA. Text mining for technology monitoring. Proceedings of the IEEE International Engineering Management Conference (IEMC), Cambridge, UK, 2002; August, 2:596– 601.
[58] Zhu D, Porter A, *et al*., A process for mining science and technology documents databases, illustrated for the case of "knowledge discovery and data mining". Cienc Inf. 1999; 28(1):1–8.
[59] Helmer O. Analysis of the future: the Delphi method; and the Delphi method: An illustration. Technological Forecasting for Industry and Government, Bright, J. Ed. Prentice Hall, Englewood Cliffs, NJ, 1968.
[60] Nassar A. Product value proposition: a step by step approach. Intercontinental Networks White Paper April 2003, http://www.anassar.net.
[61] Kostoff RN, Schaller RR. Science and technology roadmaps. IEEE Trans. on Engineering Management 2001; 48(2):132–143.
[62] Walsh ST. Roadmapping a disruptive technology: A case study: The emerging microsystems and top-down nanosystems industry. Technological Forecasting and Social Change 2004; January–February, 71(1–2):161–175.
[63] Rinne M. Technology roadmaps: Infrastructure for innovation. Tech. Forecasting & Social Change 2004; 71(1–2):67–80.
[64] Phaal R, Farrukh C, Probert D. Developing a technology roadmapping system. In: Anderson TR, Kocaoglu DF, Daim TU, editors. Technology management: A unifying discipline for malting the boundaries. Portland: PICMET, 2005.
[65] Myers J, Sandborn P. Integration of technology roadmapping information and business case development into DMSMS-driven design refresh planning of the V-22 advanced mission computer. Proceedings of the Aging Aircraft Conference, Palm Springs, CA 2007; April.
[66] Sun-tzu. The art of war. Translated by Sawyer R.D. MetroBooks, New York, March 2002.

8

The Management of Engineering

Patrick D.T. O'Connor

Consultant
62 Whitney Drive, Stevenage, Hertfordshire SG1 4BJ, UK

Abstract: Managing engineering is more difficult, more demanding and more important than managing any other human activity in modern society. The article explains how, by adhering to the principles taught by Peter F. Drucker in his landmark book *The Practice of Management*, managers can exploit the full potentials of their peoples' talents and of changing technologies, methods and markets. The chapter is extracted from parts of the book [1] by the author.

8.1 Introduction

Peter Drucker's landmark book *The Practice of Management* [2] was published in 1955. In this book are to be found all of the profound ideas that have shaped the way that the world's best-managed companies and other excellent organizations work. Drucker exposed the poverty of so-called "scientific" management, which held that managers were the people who knew how all levels of enterprises should be run, and who should therefore provide detailed instructions to the "workers", who were assumed not to have the knowledge and skills necessary for managing their own work. They then had to manage the workers to ensure that they performed as required. "Scientific" management was the term used by the American engineer F.W. Taylor [3] to define the doctrines he proposed during the early years of 20th century industrialisation. This management approach called for detailed controls and disciplines, and it inspired the production line, the division of labor, and emphasis on specialisation. Drucker showed that there is no level at which management stops: every worker is a manager, and every manager a worker. Modern workers have knowledge and skills that can be applied to the management of their work. Freeing these talents generates improvements in motivation and productivity that can greatly exceed "planned" levels. It follows that work involving high levels of knowledge and skill are particularly suited to the management philosophy presented by Drucker.

Drucker taught that work should be performed by teams of people who share the same motivations. Management's role, at all levels, is to set objectives, organize, motivate, measure performance and to develop the people in the teams. Drucker initiated management concepts which today seem new and revolutionary to many engineers, such as "simultaneous engineering", involving all the skills of design, production, marketing, *etc*., in an integrated development team from the start of a project. The "quality circles" movement, in which production workers are

encouraged to generate ideas for improvement, is entirely in keeping with Drucker's teaching.

Drucker's teaching on management is universal. Drucker wrote that the people are "the only resource that really differs between competing businesses". Each business can buy the best machines, and their performance will not vary significantly between users. However, the performance of people, particularly as managers, can be greatly enhanced by applying the new first principles of management. He forecast that countries whose managers understood and practised the approaches he described would become the world's economic leaders. Japanese managers quickly adopted them across nearly all industries.

In the West the ideas received patchy recognition and application: many leading companies owe their success to the application of Drucker's teaching, but other companies and organizations fall far short of their potential because their managers do not appreciate or apply the principles.

Ironically, engineers often have difficulty in applying Drucker's principles, yet the principles of "scientific" management, that managers manage and workers do what they are told, is fundamentally inappropriate to even the simplest engineering tasks. In fact, because of the pace of technological change, it is common for engineering managers to be less knowledgeable than many of their subordinates in important aspects of modern product and process development, so making a philosophy based on trust and teamwork even more necessary.

The main reason why engineers have tended to gravitate towards the "scientific" approach to management is that they are normally, and have been taught to be, rational, numerate and logical. Engineering is the application of science to the design, manufacture and support of useful products, and scientific education is rational, numerate, and logical. Therefore the ideas of "scientific" management were welcomed by engineers, and they have difficulty in giving them up in favor of methods that seem vague, subjective, and not amenable to quantification and control. This attitude is reinforced by the fact that few engineers receive training in the new management principles, and in fact much current management training and literature is tinged with Taylorism. However, all engineering work is based on knowledge, teamwork and the application of skills. Applying "scientific" plans and controls to such work takes Taylor's original concept far beyond its original intent of managing manual labor. "Scientific" management, and related forms of organization and project control so often observed in engineering are inappropriate, wasteful and destructive of morale, both within enterprises and in the societies in which such principles are applied.

8.1.1 Engineering is Different

Managing engineering is different to managing most other activities, due to the fact that engineering is based on science. It is a first principle of management that the managers must understand the processes they are managing. Most non-scientific endeavors, such as retailing, financial services and transport planning can be learned fairly quickly by people with basic knowledge and reasonable intelligence. However, engineering requires proficiency in relevant science and mathematics and their application, and this can be obtained only by years of specialist study and practice.

Every engineering job is different to every other, even within a design team or on (most) production lines. Every one requires skill and training and there is always scope for improvement in the way they are performed. Nearly all involve individual effort as well as teamwork. These aspects also apply in different degrees to many other jobs, but engineering is unique in the extent to which they are relevant and combined.

Engineering is also different due to the reality that engineering products must proceed through the phases of design, development testing, manufacture and support. This is also true in part for some other fields of endeavor: for example, a building or a civil engineering structure like a dam or a bridge must be designed and built. However, these projects do not share some of the greatest challenges of most engineering creations: the first

design is usually correct, so there is little or no need to test it. They are seldom made in quantity, so design for production, managing production and item-to-item variation do not present problems. They are simple to support: they rarely fail in service and maintenance is simple.

8.1.2 Engineering in a Changing World

Engineering is a profession subject to continual and rapid change, due to developments in science and technology, components, materials, processes and customer demands. It is also subject to economic and market forces and often to pressures of competition, so costs and timing are crucial. In particular, there are few engineering products that do not face worldwide competition, whether they are produced for specialists or for the public. Engineering managers must take account of all of these factors, scientific, engineering, economic, markets and human, in an integrated and balanced way. They must also balance short term objectives with long term possibilities, so they must be able to weigh the advantages and risks of new technologies.

No other field of management operates over such a wide range or in the face of so much change and risk. It is not surprising that many organizations have made the mistake of separating the management of people from that of technology, instead of facing the challenge posed by the new management.

The philosophy will not guarantee success, particularly in competitive situations. As in sport, the best are more likely to win. As in sport, there is also an element of luck: a good project can fail due to external forces such as politics or global economic changes, or a simple idea might be fortuitously timed to coincide with a market trend or fashion. However, again as in sport, there is little chance of success if the approach to the business and its practice is not of the best in every way. There are no minor leagues or second divisions in engineering business, and no amateurs. Survival depends on being able to play at the top. The philosophy and methods taught by Drucker have been proven to provide the basis for winning.

8.2 From Science to Engineering

The art of engineering is the application of scientific principles to the creation of products and systems that are useful to mankind. Without the insights provided by scientific thinkers like Newton, Rutherford, Faraday, Maxwell and many others, engineering would be an entirely empirical art, based on trial and error and experience, and many of the products we take for granted today would not be conceivable. Knowledge and a deepening understanding of the underlying scientific principles, often as a result of scientists and engineers working as teams, drives further development and optimization across the whole range of engineering. By themselves, theories have no practical utility, until they are transformed into a product or system that fills a need. Engineers provide the imagination, inventiveness, and other skills required to perceive the need and the opportunity, and to create the product.

In its early days, engineering was a relatively simple application of the science that was known at the time. There was little distinction between science and its engineering application. The products were also easily understandable by most people: anyone of reasonable intelligence could see how a steam engine or electric telegraph worked, and they were described in children's encyclopedias. Today, however, most products of engineering effort involve multi-disciplinary effort, advanced technology related to materials, processes, and scientific application, and considerable refinement and complexity. Most people cannot understand the electronic control system of an electric power tool, the principles of a laser disc recording system, or the stress calculations for a turbine blade. This complexity and refinement have been driven by advances in science and in its application, and by the ceaseless human motive to improve on what has been achieved before.

As in pure science, engineering ideas must be based on knowledge and logic. To be useful they must also take account of several other factors from which scientists can remain aloof, such as economics, production, markets and timing. We can create both revolutionary and evolutionary

change, with the objective of creating products perfectly adapted to the preferences and constraints of their markets. The only limitations are those imposed by the laws of physics and by the extent of our imagination and ingenuity.

8.2.1 Determinism

Applying mathematical principles to problems of science and engineering enables us to predict cause-and-effect relationships, to select dimensions and parameter values and to optimize designs. Scientists take for granted the determinism provided by mathematics, and scientific theory is often derived directly by mathematical deduction. However, not all problems in engineering can be quantified in ways that are realistic or helpful. Lord Kelvin wrote:

"When you can measure what you are speaking about and express it in numbers, you know something about it; when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind".

Of course, the knowledge we need in engineering is often of a "meagre and unsatisfactory kind". This does not mean that we must avoid quantification of such information or beliefs. However, it is essential that we take full account of the extent of uncertainty entailed. Kelvin's aphorism has led many engineers and managers into uncritical and dubious quantifications, which then often appear in analyses of costs, benefits, risks, or other parameters. Analyses and "models" that are based on dubious inputs, particularly those that pretend to levels of precision incompatible with the level of understanding of causes and effects, are common manifestations of the "garbage in, garbage out" principle.

There are situations in which attempts at quantification, in a predictive sense, can actually confuse and mislead. This is particularly the case in problems of quality, reliability and safety. For example, the yield of a process, such as electronic or mechanical assembly, is influenced by many factors, including component and process tolerances, machine settings, operator performance and measurement variability, any of which can make large differences to the process output. Any prediction of future yield or reliability based on past performance or on empirical evidence is subject to very large uncertainty: the yield or reliability might suddenly become zero, or be greatly reduced, because of one change. When this is corrected, yield or reliability might improve slightly, or by a large amount, depending on what other factors are involved. Yield, reliability, and factors that are dependent on them, can be predicted only for processes that are known to be fully under control. "Fully under control" is a condition that is rare in engineering, though of course we often strive to attain it. However, the more tightly a process is controlled, the greater is the divergence if perturbations occur and are not detected and corrected. In cases such as these, predictions should be based on intentions, and not merely on empirical models or past data, which can give a spurious and misleading impression that causes and effects are all understood and controlled.

8.2.2 Variation

There is a further aspect of uncertainty that affects engineering design and manufacture, but which is not a problem in science, and that is variation. Products and components must operate in variable environments of temperature, humidity, mechanical stress, *etc*. The processes of manufacture, assembly, test, and measurement used to make and verify the product will all be variable. The extent and nature of the variations will in turn be variable, and often uncertain. For example, resistor values might be specified to be within ±5%, but a batch might arrive wrongly marked and be of a different tolerance, or even a different nominal value, and a machining process might be subject to a cyclical disturbance due to temperature change.

Variation exists in the behavior and performance of people, such as machine and process operators, as well as in the machines themselves. Variation in human behavior can be particularly difficult to understand, predict, and control, but might be the critical factor in a production operation.

Whereas variation that occurs in nature is passive and random, and improvement is based entirely on selection, the variations that affect engineering can be systematic, and we must control and minimize them by active means. Understanding, prediction, and control require knowledge of the methods of statistics, as well as the nature of the processes and of the people involved.

Statistical methods are used to analyze the nature, causes, and effects of variation. However, most statistical teaching covers only rather idealized situations, seldom typical of real engineering problems. Also, many engineers receive little or no training in statistics, or they are taught statistics without engineering applications. Since variation is so crucial to much modern product performance, this lack of understanding and application can have severe consequences. Conversely, proper understanding and application can lead to impressive gains in performance and productivity.

8.3 Engineering in Society

The business of engineering exists within the framework of society at large, at all levels from local to international. Engineering contributes enormously to society: nearly every product and service used by modern society depends upon engineering. Even non-engineering products and services such as food and banking depend upon engineering: engineering products are needed for food production, processing, packaging and retailing, and banks rely upon computers and telecommunications. At the same time, engineering depends upon the supply of the right kind of people and on the attitudes of society. Despite the benefits that engineering has bestowed, these attitudes are not universally favorable. Many people perceive engineering as being not entirely honorable, or as a profession that lacks the esteem and rewards of others such as entertainment, medicine, law and finance. Partly this is due to the fact that engineering is so wide ranging, from making electric toasters to designing spacecraft. Engineering is often perceived as being associated with militarism and with damage to the natural environment. These attitudes become reinforced by people such as teachers, journalists and politicians who influence others, particularly young people, when their future directions are being determined.

Engineering is hard work, both to learn and to practice. Many other professions seem to be easier, and this is a further reason why people turn away.

The future of engineering therefore depends upon how it is managed within society. Engineering managers should attend not only to the internal affairs of their organizations, but must be conscious of the local, national and international social pressures that influence the effects of their decisions. They should in turn work to shape these influences so that they develop favorably towards engineering, and to society as a whole.

8.3.1 Education

Education is the lifeblood of engineering. Future engineers are formed by the early exposure of children to science and mathematics. Their directions are influenced by their aptitudes, so those with average or above-average abilities in these subjects are potential engineers.

Teachers of mathematics and science are mostly qualified in these disciplines, so they must be expected to teach them well and to generate interest among their students. They are not in general expected to be good teachers of other subjects in which they are not qualified, even if the subjects are in some way related. Very few teachers are engineers. School curricula have in the past not normally included engineering as a subject, so there is little tradition of engineering education or experience in primary and secondary education in modern society.

Since modern economies depend to such a large extent on the supply of engineers, it has been fashionable in many advanced countries to try to stimulate this by introducing engineering, or "technology", into schools. This has generally been a flawed approach, for three reasons. First, teachers have been expected to teach topics in which they are not qualified or experienced. Second, and probably more significant, is that since engineering is based on science and mathematics, these basics

must be mastered before they can be applied to the learning of engineering. Of course there are overlaps between what can be called science and what can be called engineering, but the practical content of schoolwork should be planned to illustrate principles and demonstrate basic applications, and not to be premature exercises in engineering design. Third, all time spent on "technology" must be taken away from teaching of basic principles. In Britain, for example, all school children are required to study "technology"[1], regardless of their aptitudes or inclinations and despite the fact that few teachers are competent to teach the subject. This combination of unqualified teachers and misguided teaching has had the opposite effect to that intended: not surprisingly, young people are dissuaded from taking up an engineering career, and for those that do their formal engineering training begins with less knowledge of the fundamentals than they would have had under the traditional teaching regime.

Of course, it is appropriate for schools to encourage an interest in engineering, as they should for all later courses of study. However, this effort should not be part of the mainstream curriculum. If engineering topics are taught they should be dealt with separately, for example as voluntary activities. The fact that modern economies need engineers is not a rational justification for teaching children engineering. We also need doctors, architects and hotel managers, but we do not teach these professions in schools.

The effect of social pressures and inappropriate school teaching, as well as of recent "progressive" trends in school education, has led to a decline in the entry of young people, particularly the most able, into engineering. Engineering colleges and universities have had to reduce their entrance standards. They have had to expend more initial effort and time on teaching the basics of science and mathematics to make up for the deficiencies in school education. This leaves less time for teaching what should properly be taught at this level, thus inevitably reducing the knowledge on graduation.[2]

There is a need for a spread of engineering graduate knowledge, from those who will work at the frontiers between science and engineering in research and in new applications to those who will be mainly involved in the practical business of design, development, test, production and maintenance. Engineering also covers a wide range of topics, specializations and depths of specialization. Higher education must therefore provide this spectrum of output, whilst ensuring that there is no general difference in the esteem and status of the different courses and of the institutions providing them. However, there has been a trend in many countries, particularly in the United Kingdom, to place greater emphasis on academic aspects. The policy-makers and teaching staff perceive practical courses, and the institutions that offer them, as being somehow of lower status than those offering academic degrees and a research programme. These institutions then attract the more talented students, many of whom then find that their courses offer less in the way of practical engineering than they would have expected. Few university engineering courses include more than fleeting training or experience in manufacturing methods such as workshop skills. Practically none teach testing or maintenance.

Stability is a critically important factor at all levels of education. Students, parents, teachers, and employers can be disorientated and disaffected if they are not familiar with the education system. Instability and rapid change make it difficult to guide young people and to compare standards. As a result standards fall, even when the changes are supposed to improve them, and students and employers lose faith in them. It is far better to encourage progressive improvements in existing systems than to impose dramatic changes, yet governments have imposed sweeping changes and continue to do so in countries in the West. The results have almost always been a general

[1] The term has come to be associated almost entirely with "information technology" (IT). Children are taught how to use PCs, but not much else that is technological.

[2] In the UK this trend has continued steadily downwards during the 10 years since these words were written. Stupidity at work?

depression in standards, morale and respect for education, particularly in science and engineering.[3]

Teachers, at all levels, are the developers of the future talents needed by society. Sadly, in some of the most advanced Western countries, particularly in Britain and the United States, the status and rewards for teachers do not attract the best[4]. Teachers have a more fundamental impact on the future well being of advanced societies, and of their relative competitiveness, than any other profession. Doctors, accountants and lawyers, and even engineers, do not influence the long-term quality of society to anything like the extent that teachers do. Teachers should enjoy the same status and rewards as other professions, and this is the only way to guarantee that teaching will attract the necessary share of the most talented. This is particularly important for teachers of science, mathematics and engineering, for whom prospects in industry are usually better than for those with qualifications in subjects such as languages or history. The common practice of remunerating teachers at a standard rate, regardless of specialization and usually regardless of performance, is an appropriate ingredient in a policy of industrial decline, which no government intentionally supports but some nevertheless have managed to achieve.

It should be possible for professional people such as scientists and engineers to move between other employment and teaching in order to bring experience to the classroom and the lecture hall. This is particularly important for training young engineers, because of the practical nature of the subject and to keep pace with the change. Unfortunately this flexibility is reduced because few good engineers are attracted by the lower rewards for teachers, particularly in schools and non-degree-level training institutes. The formal pedagogical qualifications demanded for working as a teacher, particularly in schools, is also a barrier to easier movement of experienced engineers into teaching.

The proper role of government in engineering is to ensure the provision of educated, motivated people. Education, starting from primary school and continuing through various forms of adult education, particularly vocational training and university, cannot be managed by industry. Engineering managers can obtain capital, plant and materials, limited only by their finances, so long as they operate successfully in a commercial economy. However, they cannot ensure the provision of the talents they need, except by competing for the supply available. If the supply is limited it imposes long term but intangible constraints on all aspects of performance.

The constraints are long term for the simple reason that it takes a generation to influence the quality of education. They are intangible because even if managers can find the numbers of people they need, if the quality of their education has not developed their knowledge, skills and attitudes to their full potentials, the shortfalls cannot be measured in terms of inventiveness, productivity, and effectiveness of management. Their employers can and should continue to develop them, since there is no end to an individual's potential to learn, but industry cannot make up for widespread, long-term inadequacy in a nation's educational provision. Individual companies can ensure that they select and develop the best, but the burden on industry as a whole can seriously restrict national competitiveness. The relative decline of the UK and US engineering economies over the last 30 years or so has been due largely to the reduction in educational standards, particularly in relation to science and engineering.

More so than in any other profession, engineering education is never complete. Every engineer requires continual updating as methods, materials, technologies and processes change, as systems become more complex, and as multi-disciplined approaches become increasingly necessary. Therefore engineering education should always emphasize the need for continuation and should stimulate further development. Employers should ensure that their people are given the opportunities and motivation to continue to learn,

[3] The 10 years since this was written show that this self-destruction continues, with lessons unlearnt. More stupidity at work?

[4] UK government interference in how and what schoolteachers teach, and the loss of classroom discipline, have made teaching an unenviable career choice.

for example by linking advancement to training. Many universities and other institutions provide excellent short courses as well as post-graduate degree courses. Engineering managers should be aware of which courses are most appropriate to their work and should make use of them and help to develop them.

Of all the issues in engineering management, education is the one with the longest time-scale. It also has the widest impact, since it affects the whole supplier chain. Employers have a duty to promote continuing education, but they should not be expected to teach people what they should have learned at school or college, and they should be able to expect that the people they employ will be numerate, literate and motivated to learn more. Companies operating where engineering education is excellent will enjoy the effects for a generation. Those working in countries in which standards of education have been allowed to fall will carry an extra burden until long after improvements are made.

8.3.2 "Green" Engineering

Protecting and improving the natural environment is a concern of many engineers and engineering companies. This concern is now also expressed in politics and in legislation. In many countries environmental pressure groups such as Greenpeace make life interesting for engineers involved with products and processes that are noisy, noxious, non-biodegradable, or nuclear. There is no doubt that the pressure groups have benefited society, but, like most pioneering movements, their targets and methods sometimes appear irrational to engineers.

The most notable achievements of the environmental movement as far as engineering is concerned, and which have involved enormous engineering effort and cost, have been the noise reduction of aircraft jet engines, the reduction of lead and other emissions from vehicle engines, and the cleaning of rivers and emissions from coal- and oil-fired power stations.[5] They have secured many other less dramatic improvements on behalf of society, and they have forced the legislation that governs environmental issues. They have also had a negative impact in frightening society and politicians concerning the safety of nuclear power, although even here they have forced the nuclear power industry to banish complacency in their operations.

We are on the verge of an environmental explosion similar to the quality "systems" explosion described earlier. Standards are being written[6] and armies of consultants, inspectors and auditors are being formed. Engineers and the bodies that represent them must be sympathetic to public anxiety, and must help to educate legislators, the media and the public without appearing to be defending vested interests or covering up problems.

8.3.3 Safety

Public perceptions of risk are not always as rational as engineers would like. When the risks are difficult to understand or quantify the gap in understanding is increased. For example, public fears of nuclear and electromagnetic radiation are based, to a large extent inevitably, on ignorance and on the invisibility of the radiation. These fears are reinforced by the fact that even the specialists are uncertain about the long-term effects of radiation exposure. To a lesser extent there is also fear of software. Engineers know that software is intrinsically safer than people or hardware performing the same function, since software cannot degrade or wear out and it is not subject to variation: every copy is identical. Software can contain errors, but properly managed design and tests can ensure that it is correct in relation to safety-critical functions, if not in every possible but remote eventuality.[7]

The employers of engineers must ensure that safety liabilities are minimized by providing

[5] In 2006 we can add CO2 and ozone-depleting emissions that influence global warming, and lead-free solder. In other respects the "greens" have generated fears that are less well grounded, such as about the effects of electromagnetic radiation from power lines and telephones.

[6] ISO14000 was published in 1996.

[7] As pointed out earlier, software has not been the cause of any recent disasters.

training and a system that works to eliminate all foreseeable risks from products, processes and operations. For most engineering companies it is now essential that a manager is appointed to coordinate safety issues.

8.3.4 Business Trends

One of the major features of modern business that influences the task of managers is the continuing pace of company acquisitions, mergers and disposals. These often occur across national borders, as business becomes more multinational. They nearly always lead to displacement of people and force changes in organizations and methods. They present opportunities for some, but uncertainty and loss for others. Since the main justification for the moves is usually financial, changes are often forced down by new managers in order to generate quick savings.

Another important trend is the transfer of manufacturing work overseas in order to reduce costs. This is an understandable move, but it can be unsettling to the important interface between design and production.

Much of modern business is driven by short term pressures, and this seems to be an increasing trend. Companies feel threatened by competitors, possible acquirers and shareholders if they do not generate profits and share price growth. Some of the reward contracts for CEOs and other board level people motivate them towards short term greed rather than the long term good of the business. As a consequence of these pressures, companies shed staff and cut investments in training and research. Of course it is necessary to seek to operate the business as economically as possible, but, as Drucker emphasized, the main duty of top management is to ensure survival of the business, and this means taking account of the long term. Short term economies, especially when driven as campaigns with defined targets ("reduce staff across the board by 5%"; "cut capital spending by 20%"; "cut indirect expenses (training, travel, *etc*.) by 50%", *etc*.), are often applied, but they can be very damaging and expensive in ways that accountants might not appreciate. The financial benefits soon appear on the balance sheet, but the damage to the business in the longer term is less apparent.

There is an unfortunately "macho" attitude to much of modern management, largely driven by these pressures and trends. This seems to have been fostered by books and articles on management by fashionable "gurus", presenting panaceas and "paradigms". The contributions from the management training schools have not resisted this trend. Maybe this is tolerable in enterprises that are not critically dependent on skill, training, teamwork and long-term effort and investment. However, "macho" management of engineering is counterproductive and damaging.

8.4 Conclusions

Science is difficult. Scientific work requires intelligence, knowledge, powers of induction and deduction, and patient effort. Engineering is even more difficult. There are greater problems in terms of resources and time. Variations in human performance and design parameters make outcomes more uncertain and difficult to predict. Aspects such as production, market appeal, competition and maintenance must be considered. Several technologies might be involved, and the development teams must be multi-disciplined. Technologies, in materials, components, and methods, are continually changing, and the team must keep abreast of these. Engineers must be aware of the scientific principles and mathematical methods that are the foundations of their work. They must also be aware of the limitations of applying these to the real world of engineering, which involves variation, uncertainty, and people. Naive application of basic principles is the mark of the novice. Appreciating the complexities of the real world is the mark of experience. It is often the application of new ideas, regardless of how simple they might at first appear, that causes the greatest problems in engineering development.

However, in spite of these difficulties, or maybe more accurately because of them, engineering is often performed very well. People respond to challenges, and we see the results in the remarkable new products that flow from

engineering teams, particularly in competitive markets.

The principles of management, on the other hand, are basically very simple and unvarying. No difficult theories are involved. Perversely, management is often performed very badly, or at least in ways that fall far short of releasing the full power of people and the teams they form. Sub-optimal management is commonplace in engineering.

Successful engineering depends holistically on the blend of scientific application, empirical and mathematical optimization, inventiveness and design of the product and of its manufacturing processes, and the leadership of the project. There is no other field of human enterprise that requires such a wide range of skills; skills that can be developed and maintained only by a combination of education and continual training and experience.

Managers of creative people need to understand and abide by the simple principles in the performance of their difficult task of leadership. Carl von Clausewitz, writing in his classic book **"***On War", stated: "*the principles of war are very simple. Wars are lost by those who forget them*".

8.4.1 In Conclusion: Is Scientific Management Dead?

Despite the wisdom of Drucker's teaching and the dramatic positive effects of its application, "scientific" attitudes to management still persist widely in Western industrial society. This is reflected in much of the modern literature and teaching on management and in the emergence of bureaucratic procedures, regulations and standards. Many managers, it seems, are unaware of the new management or are inhibited from applying it by the pressures and constraints of their work situation.

Engineering is the epitome of modern civilization. Like science and most art, it is truly universal. Like art, engineering is creative, and it can even create beauty. More than science and art it influences and changes all lives. However, not all of the results of engineering have been beautiful or beneficial, and the people engaged in its many forms are as human as the rest. Also, engineering is so widespread a discipline, and so much of it is perceived to be routine and unglamorous, or hardly perceived at all by the wider public, that its profession is often undervalued. Very few engineers achieve national or international recognition outside their profession. Even fewer have attained the kinds of reputations enjoyed by great writers, artists or scientists[8]. To a large extent this reflects the fact that few engineers work alone. In a world-class engineering product such as a high-speed train or a mobile telephone, every electronic component, plastic molding and fastener is the product of engineering teamwork, as is every subsystem and the complete train system or telephone network. No credits are published, so the engineers' names are not listed as are, for example, the directors, producers, makeup artists, gaffers, focus pullers, sound recorders and others who contribute to the making of a movie or a TV film.

Engineering is therefore largely anonymous and the satisfactions are more personal, to the individual and to the team. Though engineers' names do not appear in lights they have the satisfaction that, in well managed teams and organizations, they can all influence the products and services in ways that are more fundamental than are allowed to gaffers and focus pullers.

Engineering and engineering management are not governed by any particular codes of ethics, as for example the Hippocratic Oath taken by the medical profession. All professions are governed by law and by normally accepted standards of ethics. In addition, many engineering societies and institutions issue codes of practice, but these are not enforceable or supported by disciplinary frameworks. The profession of engineering has served society well without such additional regulation, and there is no reason why it should not continue to do so and to improve its contributions. Since engineering management is a continuous, long-term activity, high ethical standards are essential for successful leadership and competitive progress.

All work should provide satisfaction to those engaged in it and to those who will benefit from it.

[8] Or writers and "artists" who create pretentious nonsense, or entertainers, or the generality of the modern "celebrity" class.

However, mere satisfaction is barely sufficient. Work and its results should provide satisfaction beyond expectation, and happiness and fulfillment to those most directly involved. As Deming himself has stated, his famous 8th point for managers ("*drive out fear*"), needs now to be re-stated as "*create joy in work*". Striving for happiness in work is not a naive or merely altruistic objective. It is the logical culmination of the most influential teaching of management. It is also the common observation of people at work, including the managers who make it happen, that the correlation between happiness and performance is very intense, yet subtle and fragile.

Happiness can generate quality, inventiveness, teamwork and continuous improvements that transcend "scientific" plans and expectations. Happiness at work must be based on shared objectives and challenges, not on self-satisfaction or fear.

It must be tempered by efficiency and discipline, and reinforced by learning and by the freedom and duty to contribute to the common effort. It must be of a quality that inspires and encourages effort, but not adulation or blind subservience.

Generating and strengthening happiness at work of such quality, and maintaining it in the whole of the organization despite the problems and changes that human enterprises must encounter, is the most difficult but most satisfying and rewarding task of managers.

This is the fundamental challenge for modern managers. In free societies, from which the fear of tyranny and global war has hopefully been removed, human creativity and productivity can be developed to their fullest when the work of individuals and of teams creates and increases happiness.[9]

References

[1] O'Connor PDT. The new management of engineering, 2004. at http://www.lulu.com/

[2] Drucker PF. The practice of management, Heinemann, Portsmouth, NH, 1955.

[3] Taylor FW. The principles of scientific management, Harper and Row, New York, 1911.

[9] More than ten years since I first wrote this sentence, this message still seems apt. History has not ended, and the world still faces real and imagined dangers. I would merely add the words of advice: "Creating happiness is the first role of statesmen". I would also quote the words of the American Declaration of Independence about peoples' "unalienable rights" to "life, liberty, and the pursuit of happiness." Creating happiness is the first role of managers, at all levels.

9

Engineering *Versus* Marketing: An Appraisal in a Global Economic Environment

Hwy-Chang Moon

Graduate School of International Studies, Seoul National University, Seoul, Korea

Abstract: The global manager should consider engineering first before marketing because optimal engineering efficiency creates more values than customized marketing efficiency. Although the debate over the global standardization continues in the area of global strategic management, global firms need to conduct this new type of global strategy. Foreign consumers actually prefer global products to locally customized products in many industries such as automobiles, electronics, food, and others in which engineering applications are important. Therefore, the most important task of the global firm is to change local products to global products through enhanced engineering.

9.1 Introduction

Innovation telecommunications is growing faster than ever before. Michael Armstrong [1], Chairman and CEO of AT&T, said, "*It took radio 30 years to reach 50 million people; it took 13 years for TV to do the same; but the World Wide Web reached twice as many users in half the time*." The number of Internet users will soon reach a "critical mass" and the Internet will be treated as a valuable business platform. The future will move even faster. Bill Gates [8], Chairman and CEO of Microsoft Corporation, said, "Business *is going to change more in the next 10 years than it has in the last 50 years*." We have witnessed that all these predictions are becoming true.

Globalization has been accelerating with these rapid developments in telecommunication technology. Telecommunications break down national trade barriers and create seamless global trading, global shopping, and global manufacturing. The environment of international business has thus been dramatically changed. In this globalizing business environment, there have been debates on what the global standards are and whether business people should follow the global standards. There are basically three approaches to global standards: international organization-driven, government-driven, and corporate-driven standards. International organizations such as the World Trade Organization set new rules on global standards in such areas as E-commerce. Rules and principles formulated by international organizations are sometimes mandatory, but are advisory in many cases. Governments set new standards in product specifications, safety rules, and so on.

[1] This chapter, in parts, is based on Moon [21] and is has been adapted with permission.

These standards are often mandatory and necessary rather than advisory. Global firms pursue management strategies and techniques that can be regarded as global benchmarking or global standards by other firms.

This study focuses on corporate-driven standards. In particular, this chapter addresses strategic issues concerning global standardization and local responsiveness. A corporate-driven global standard can be defined as the standardization of the best product and management in a competitive global market. Firms usually prefer a standardization strategy that minimizes production and management costs but may also prefer a customization strategy that responds to local differences, thereby increasing the local market share. Standardization and customization are thus two conflicting forces or trade-offs that firms must consider simultaneously.

The standardization of market strategies has been a continuing topic of debate and research since Levitt's [13] article. Debates on the standardization *vs*. customization (or segmentation) strategy in the world market are documented well in scores of articles (*e.g.*, Levitt [13], Douglas and Wind [6], Bartlett and Ghoshal [3], Varadarahan, Clark and Pride [30], McCutcheon, Raturi and Meredith [16], Gupta and Govindarajan [11], Chen and Paliwoda [5], Capar and Kotabe [4], Gabrielsson and Gabrielsson [7], London and Hart [14]).

In theory and practice, the opportunity cost of a standardization strategy may be lost sales, while a customization strategy may sacrifice the firm's production and/or marketing efficiencies. However, the debate itself is often pedagogical. In addition, most scholars have chosen examples selectively and interpreted subjectively in order to support one of the two extreme arguments. On the other hand, by recognizing that the world market is neither extremely homogenous nor heterogeneous, a compromising strategy has been introduced. For example, a word that captures the global and local perspective is “glocal”, a new concept for a new globally competitive world [10]. However, this study argues that the most challenging issue is not to choose one of the two extremes, nor to compromise the two, but how to increase the degree of standardization by enhancing the product values.

In the next section, the standardization issue for value creation will be revisited, including an attempt to clearly explore its assumptions and criticisms. Counter-arguments will also be provided. In the section that follows, strategic implication of global standardization and new challenging issues will be discussed. A new model for dynamic globalization will then be introduced. Finally, the new organization of global firms will be discussed to pursue this new global strategy.

9. 2 Creating Product Values with Low Cost and High Quality

According to Levitt [13], companies must learn to operate as if the world were one large market, ignoring regional and national differences. Historical differences in national tastes or modes of doing business will disappear. An emerging similarity of global customer preferences will be triggered by developments in both production technology and in communication and transportation networks. Such conditions in turn will lead to standardization strategies for product and other marketing mix elements, as well as manufacturing. Companies which are able to push costs and prices down while pulling quality and reliability up will inevitably attract customers to the firm's globally available and standardized products. Levitt believes that multinational corporations will have minimal needs for local adaptation in the evolving “global village”.

In contrast, Quelch and Hoff [27], for example, challenged the “standardization imperative” for global managers. Despite the promised economies and efficiencies to be gained with standardization strategies, many managers appear reluctant to take the global marketing plunge. These managers see customers and competitive conditions as differing significantly across national boundaries. This perception (and some bad experiences) represents the basis for much of the skepticism about standardized strategies.

Levitt's argument was further criticized by Douglas and Wind [6]. They questioned three of Levitt's assumptions: (1) that consumer tastes are becoming homogenous worldwide; (2) that

consumers are willing to sacrifice personal preferences in return for lower prices; and (3) that economies of scale (EOS) are significant with standardization. It is useful to examine Douglas and Wind's criticisms on Levitt's assumptions. Counterarguments will then be discussed.

9.2.1 "Consumer Tastes Are Becoming Homogenous"

Douglas and Wind claimed that evidence is lacking to show that consumer tastes are becoming more similar globally. Indeed, they contended that the world market is probably becoming more diverse. For example, Coca-Cola markets Georgia Coffee, a canned coffee drink, in Japan, but the product is not accepted by U.S. and other buyers around the globe. However, this is one of a few examples of customization. Many other products are easily transferable across countries. Keegan, Still and Hill [12] reported that multinational firms selling consumer packaged goods perceived few problems in transferring products between markets as dissimilar as the U.S. and less developed countries (LDCs). They found that about 1200 (54.4%) of the 2200 products sold by 61 subsidiaries had been transferred from home-country markets (U.S. or U.K.) into LDCs. This means that over half the items in LDC lines are "international products", that is, their commercial appeal extends over multiple markets.

While there may be a lack of substantive evidence of movement towards a more homogenous global market, the same is true in support of an increasingly heterogeneous global market. Despite the lack of empirical data, more scholars seem to agree with the homogenization trend. Sheth [28], for instance, argued that there is evidence of increasing international standardization of both product quality and product safety standards. Porter [25] also noted a change towards more homogenization of needs internationally.

9.2.2 "Consumers Are Willing to Sacrifice Personal Preference in Return for Lower Prices"

A low price appeal resulting from standardization offers no long-term competitive advantage to the firm, according to Douglas and Wind. They saw the inevitable vulnerability of this pricing strategy as stemming from these factors: a) new technological developments that lower costs; b) attacks from competitors with lower overhead and lower operating or labor costs, and c) frequent government subsidies paid for emerging country competitors. Any or all of these, they claimed, may undermine the effectiveness of low price strategy.

What they did not consider, however, is that a low price strategy linked to reduced average cost which results from a firm's technological advantage *does* endure. Standardization, thereby, offers a long-term competitive advantage. In fact, Levitt emphasized both low price and high quality. He suggested that if a company could push costs and prices down and at the same time pull quality and reliability up—thereby maintaining reasonable concern for buyer suitability—customers would prefer its world-standardized products.

Whether a firm can pursue more than one generic strategy is an important issue in the area of strategic management. Porter [25] classified two basic types of competitive advantage that a firm could possess: low cost and differentiation. These two basic types of competitive advantage combined with the scope of activities (broad target or narrow target) lead to three generic strategies: cost leadership, differentiation, and focus. The focus strategy has two variants, cost focus and differentiation focus [24]. According to Porter [23, 24], the underlying implication of generic strategies is that a firm has to make a choice about the type of competitive advantage that it seeks to gain. A firm could choose a cost leadership or differentiation in a broad competitive scope; a cost or differentiation focus in a narrow target scope. Porter argued strongly that businesses should compete on the basis of just one (not the combination) of the four generic strategies in order to be successful.

However, there are some criticisms of Porter's framework. As a matter of fact, cost leadership and differentiation are not mutually exclusive, but often complementary. Differentiation, which increases demand and market share by satisfying consumers, may produce economies of scale and speed up the descent along the cost curve [17]. On the other

hand, many cost-reducing skills may also enhance the quality, design, and other differentiated features of the product. Global players are concerned about both cost leadership and differentiation [18]. An important issue of standardization is not to give up quality, but to serve the global market with a recognized and branded product at a reasonable price.

9.2.3 "Economies of Scale Are Significant with Standardization"

Douglas and Wind pointed out three weaknesses in Levitt's Economies of Scale (hereafter EOS) justification for standardization: a) flexible factory and automation enable EOS to be achieved at lower as well as higher levels of output; b) the cost of production is only one and often not the critical component in determining the total product cost; and c) strategy should be not only product-driven but should take into account other components of the marketing mix.

The arguments of Douglas and Wind are true in particular industries. However, there are still many industries where the benefits of EOS are significant with standardization. An example of the magnitude of EOS is found in the paper industry. In the production of uncoated paper for printing, an expansion from 60,000 to 120,000 tons brings with it a 28% drop in fixed costs per ton. For this same expansion, labor costs can be reduced by 32% as new technical opportunities for production open up (Oster [22]). Prolonged benefits from EOS are significant in many mature industries such as steel and automobiles.

9.3 Strategic Implications of Global Standardization

In evaluating the standardization strategy, Levitt focused on perceived and real similarities, while Douglas and Wind stressed the perceived and real dissimilarities. The correct strategy for any particular firm appears to be highly empirical and circumstantial in determination. The more challenging issue is whether we can predict which of the two strategies, standardization or segmentation, would be appropriate, given stated conditions and industries.

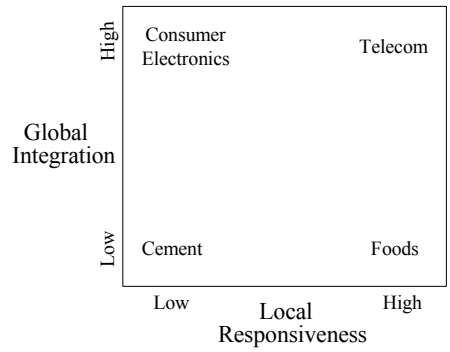


Figure 9.1. I-R framework

The preference for a standardization strategy identified by previous research is determined mainly by the type of product or industry. Bartlett [2], for example, offered a model as shown in Figure 9.1 to illustrate how forces for global integration strategy versus national responsiveness strategy may vary from one industry to the next. Bartlett [2] and also Ghoshal [9] suggested that the consumer electronics industry (radio and TV) is characterized by low responsiveness benefits and high integration benefits. The reasoning is that EOS in electronics product development and manufacturing are important sources of competitive advantage. In contrast, for branded packaged foods, firms may experience variations in local (foreign) tastes, buying habits, distribution channels, and promotional media. Food industry firms would, as a result, possibly benefit by the use of country-differentiated strategies. Douglas and Wind [6] also pointed out that standardization may be more appropriate for industrial rather than consumer goods, and for consumer durables rather than nondurables.

However, there are several problems with these traditional views. Firstly, Bartlett's model, for example, is not clear in distinguishing product standardization from the standardization of the other marketing mix elements, *i.e.*, distribution, promotion, and pricing. The distribution and promotion strategies of Coca-Cola Co. may differ across national borders, but the basic product is standardized. From this viewpoint, at the least,

product strategy can often be efficiently standardized over multiple markets. Simon-Miller [28] also argued that where the product itself is standardized or sold with only minor modifications globally, its branding, positioning, and promotion may reflect local conditions.

Secondly, what is more important is the firm's strategy, not the industry condition. Bartlett [2] argued that within any industry companies can and do respond in many different ways to diverse and often conflicting pressures to coordinate some activities globally, and to differentiate others locally. In his example of the auto industry, Toyota had a world-oriented strategy with a standardized product, while Fiat built its international operations on various governments' interest in developing national auto industries. If this is true, *i.e.*, if different firms have different strategies in a single industry, then an industry-based framework such as the one shown in Figure 9.1 may not be very useful. Therefore, a new framework is needed to explain why and how a firm (not industry) pursues a standardization strategy, while others in the same industry may not. Why, for example, is Kentucky Fried Chicken more standardized and globally accepted than other competing products in the "same" (fast foods) industry?

Finally, the strategic recommendations of previous researchers are based on static rather than dynamic conditions, whether these are either for the choice of the two strategies of standardization or customization, or a compromise of the two. Bartlett and Ghoshal [3] found that managers in most worldwide companies recognize the need for simultaneously achieving global efficiency, national responsiveness, and the ability to develop and exploit knowledge on a worldwide basis. To achieve these multiple goals, they suggested the transnational strategy. However, it is doubtful whether this strategy is really optimal and desirable. Would not more astute managers seek to implement a global strategy, focusing on transnational similarities rather than differences? The global strategist, recognizing the risks but being aware of the trade-offs, would seek to offset consumer resistance with his or her extended product package, rather than customize the product to precisely meet the local consumer needs. In the next section, a new model will be developed to explain the dynamic behavior of global firms, which improve country-specific products to global products.

9.4 The Dynamic Nature of the Global Strategy

Products can be classified into two categories: global and country-specific. The global product is output efficiency-based, more easily standardized, and universally offered, and accepted by consumers worldwide. Examples are industrial products and consumer durables. The country-specific product is quite sensitive to environmental factors. Sales are more closely tied to political, economic and cultural forces, meaning that localized or national strategies seem preferable. Processed food and clothing items are examples.

In a dynamic setting, even country-specific products may become candidates for global

products as shown in Figure 9.2.

This is where both industry and firm are driven by the search for higher technological content and stricter quality control. Coca-Cola, McDonald's, Kentucky Fried Chicken, and Levi Strauss, for example, all offer products that are more globally acceptable than parallel products with country-of-origin other than the U.S. However, note that these products—food and clothes—are all ethnic products that may be positioned in the lower right-hand corner in Figure 9.1 where forces for national responsiveness are high.

Let us take a closer look at the food industry, for instance, in which strategic positioning can be

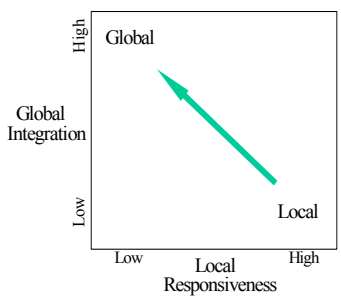


Figure 9.2. Dynamic globalization strategy

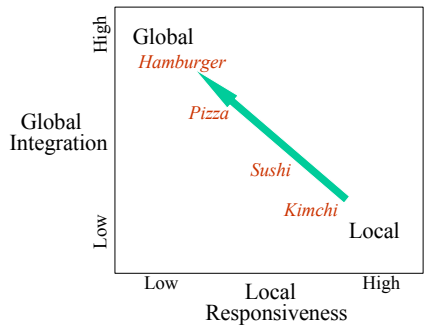


Figure 9.3. Different strategic positioning

diverse. There are several foods along the dynamic globalization arrow in Figure 9.3, ranging from kimchi that is the most localized food to the hamburger that is the most globalized food. It is important to note how a firm can enhance the local product to global product.

Kimchi is a spicy, fermented pickle that invariably accompanies a Korean meal. The vegetables most commonly used in its preparation are celery cabbage, Chinese turnip, and cucumber. The prepared vegetables are sliced, highly seasoned with red pepper, onion, and garlic, and fermented in brine in large earthenware jars. Dried and salted shrimp, anchovy paste, and oysters are sometimes used as additional seasonings. During fermentation, which takes approximately one month depending on weather conditions, the kimchi jars are stored totally or partially underground in cellars or sheds built expressly for this purpose. Kimchi is very unique in taste and thus country-specific to Korea.

Sushi is a Japanese food, consisting of cooked rice flavored with vinegar and a variety of vegetables, eggs, and raw fish. Sushi began centuries ago in Japan as a method of preserving fish. It is told that the origins of sushi came from countries of Southeast Asia. Cleaned raw fish was pressed between layers of rice and salt and weighted with a stone. After a few weeks, the stone was removed and replaced with a light cover, and a few months after that, the fermented fish and rice were considered ready to eat. It was not until the 18th century that a clever chef named Yohei decided to forego the fermentation and serve sushi in something resembling its present form. Anyhow, raw fish is a major ingredient of sushi. Still, many people think sushi means raw fish, but the literal translation means “with rice.” So, sushi used to be very unique and country-specific to Japan. However, when sushi is introduced in other countries, the ingredients are significantly changed. In particular, raw fish is often replaced with other ingredients such as avocado. Sushi has been evolved from a country-specific food into a globally accepted product.

Pizza is a dish of Neapolitan origin consisting of a flattened disk of bread dough topped with olive oil, tomatoes, and mozzarella cheese. Pizza is baked quickly and served hot. The popularity of pizza in the United States began with the Italian community in New York City; the first pizzeria appearing there in 1905. After World War II the pizza industry boomed. In the United States, sausage, bacon, or ground beef, mushrooms, peppers, shrimps, and even oysters are sometimes added. Thus, pizza originated in Italy but is now well accepted in the global market.

The hamburger is customarily eaten as a sandwich. Between two halves of a round bun, mustard, mayonnaise, catsup, and other condiments, along with garnishes of lettuce, onion, tomato, and pickle, constitute the classic dressing. In the variation known as the cheeseburger, a slice of cheese is melted over the patty. The patty itself is often seasoned or augmented with chopped onions, spices, or bread crumbs before being cooked. The hamburger is probably the most global food, but it too used to be a local product. The hamburger is named due to the city of its origin, Hamburg, Germany. In the 1850s it was brought by German immigrants to the United States, where in a matter of decades it came to be considered an archetypal American food.

How can the hamburger become a global food? First of all, the hamburger is probably the most efficient food in terms of the function as a food. It contains almost all the ingredients for the nutritional requirements of food in a small, convenient size. This function as a near complete food is well accomplished with reliable quality and at an affordable price by global firms such as McDonald’s. The company’s strategy is to maintain rigorous, standardized specifications for

its products, raw ingredients, and store management worldwide. The company has standardized recipes for its products. Menus in international markets are a little diverse, but most of the products are quite standardized in terms of ingredients and even the temperature of the food. When McDonald's entered Russia, the company found that local suppliers lacked the capability to produce quality products. To solve this problem, McDonald's built the world's largest food-processing plant in Moscow at a cost of $40 million. McDonald's also tightly controls the operating procedures of stores around the world. Therefore, the most important strategy of McDonald's is to enhance the economic values (*i.e.*, reliable quality and affordable price) of the product by effectively maintaining the standardized, strict specifications of the product engineering.

The above examples show that successful global firms can move the country-specific strategy in a more global direction if they can make the perceived benefits of better quality and reasonable price outweigh the need for buyers to satisfy their specific localized preferences. Therefore, the most important strategic implication is that the real issue of globalization is not the forced choice between the two extremes, nor a compromise of these two, but rather how to increase the degree of engineering efficiency through standardization. A high level of technology and quality control may redirect the firm's strategic choice away from national responsiveness towards higher global standardization.

One more important thing is that a global firm can pursue a strategy of product diversity only if the introduction of a new or customized product does not hurt the overall efficiency. An example is the product lines of Coca-Cola: Coke, Diet Coke, Classic Coke, New Coke, and so on. The product strategy of Coca-Cola is not completely segmented, since the formulas for Coca-Cola products are not without overlap or similarity. The firm makes only slight changes in the basic ingredients for all. The availability of flexible manufacturing enables the firm to produce and market slightly differentiated products to different target market groups, without sacrificing the benefits of global EOS. Coca-Cola would not have introduced New Coke or Classic Coke if the development of this product were to significantly impede the company from achieving its engineering efficiency. Benefits from efficiently engineering the product and principal business functions should be emphasized first for a successful global firm.

Levitt [13] suggested that although the earth is round, marketers should view it as flat. However, one further step can be suggested: "Do not just treat it as flat, but make it flat". Many multinational marketers may still insist on viewing the world through the lens of localized tastes and unique buying habits. Correct understanding of the behavioral context in foreign markets is at first very important for the global manager. However, really successful global managers may have to be able to inform and persuade local consumers through communications. Some consumers in LDCs, for example, enjoy American-type soft drinks, but they prefer them at room temperature and sweeter in comparison with North American taste. They might be persuaded to prefer less sweet drinks through education that excess sugar is not good for their teeth or general health. They might also be persuaded to prefer colder soft drinks, as refrigerators become more common in their households.

Coming up as fast as communication tools are supra-national electronic media, which transcend country boundaries. These media will permit the use of standardized and simultaneous promotional strategies across vast regions and multiple markets. These developments in global telecommunications, together with parallel innovations in transportation and an expansion of international advertising agency services will facilitate media and message access to some unfamiliar markets. With these tools the most important task of global managers is to find the common need of global consumers and to develop global products, rather than to customize their product to the local markets.

9.5 A New Strategy for Dynamic Globalization

In the integration-responsiveness (I-R) framework, several different strategies can be contrasted as shown in Figure 9.4.

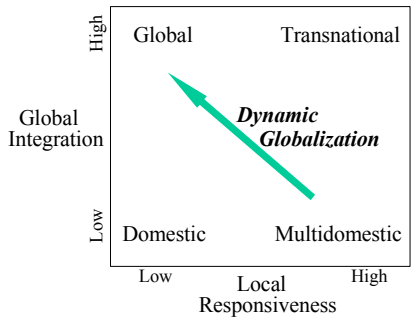


Figure 9.4. Types of international strategies

Type 1: Centralized Organization: Standardized Strategy

Levitt [13] argued that there is a new commercial reality: the emergence of global markets for standardized products. According to him, the global corporation operates at relatively low cost as if the entire world were a single entity; it sells the same things in the same way everywhere. Levitt's global strategy is thus located in the upper left corner (high integration and low responsiveness) of the I-R model.

Type 2: Decentralized Organization: Customized Strategy

Douglas and Wind [6] critically examined the key assumptions underlying the philosophy of the integration strategy, and the conditions under which it is likely to be effective. Based on this analysis, they proposed that the responsiveness strategy is more common than the integration strategy because international markets are more heterogeneous than homogenous. Their strategy is thus located in the lower right corner (low integration and high responsiveness) of the I-R model. This type of firm can be called a multinational [6] or multidomestic firm [26, 19].

Type 3: Mixed Organization: Transnational Strategy

According to Bartlett and Ghoshal [3], each of the above two approaches is partially true and has its own merits, but none represents the whole truly. They suggested the need for simultaneously achieving global integration and local responsiveness. To achieve global competitive advantage, costs and revenues have to be managed simultaneously, efficiency and innovation are both important, and innovations can arise in many different parts of the organization. Therefore, instead of centralizing or decentralizing assets, the transnational firm makes selective decisions. They call this the transnational solution, which can be located in the upper right (high integration and high responsiveness) of the I-R model.

Type 4: Flexible Organization: Dynamic Globalization

However, none of these strategies adequately explain the dynamic nature of global firms that improve country-specific products to global products by recognizing global needs and persuading global consumers with value-added products. This strategy implies the dynamic shift from a multidomestic firm to a global firm as the arrow indicates in Figure 9.4. The new paradigm should be a flexible organization that enables the firm to educate or persuade local consumers, through enhanced engineering efficiency.

It is important to understand the relation between the exploration of new possibilities and the exploitation of old certainties. This complementary aspect of firm's asset portfolio is particularly important in understanding the entry modes of multinational firms [20]. March [15] argued that adaptive processes, by refining exploitation more rapidly than exploration, are likely to become effective in the short run but self-destructive in the long run. The static global strategy of deciding whether the international market is homogeneous or heterogeneous, in order to most effectively exploit a firm's existing products or capabilities, is related to the exploitation of old certainties. However, the dynamic global strategy of introducing new global products or improving country-specific products to global products is related to the exploration of new possibilities.

The truly global firm can achieve this exploration goal by enhancing the product's economic values, such as price and differentiation, so that local consumers give up their local

preferences for the increased economic value of the product. In other words, the most important task of global managers and organizations is not to decide whether the international consumer is global, local, or even glocal, but to change local consumers to global consumers by providing products in which product values outweigh local tastes.

The debate on standardization versus customization is an important subject in the international marketing field and thus related examples and cases are primarily consumer products. However, very important implications can also be derived for engineering products and engineering applications to consumer products. In today's global economy, the need for customization in the foreign market is often overstated with an overemphasis on differences in consumer tastes across nations. However, the introduction of a customized product is costly and sometimes risky when the customized product is deviated from engineering efficiency. Foreign consumers actually prefer global products to locally customized products in many market segments such as automobiles, electronics, and other products in which engineering applications are important. The global manager should consider engineering efficiency first before marketing efficiency because optimal engineering efficiency creates more values than customized marketing efficiency.

9.6 Conclusions

Despite numerous articles on this issue, the debate over international standardization continues. This is partly because there is a lack of empirical data, but mainly because most scholars merely deal with selective examples for their particular purposes. The main problem with existing studies is that they are static rather than dynamic. Their strategic recommendations are mostly based on the perceived and static dissimilarities or similarities of international markets. This chapter argues not that the global market is homogenous or heterogeneous, but that the most successful global firm should be able to change more heterogeneous local consumers to more homogenous global consumers through enhanced engineering.

The global market place is not purely homogenous. Managers are frequently urged "to tailor for fit" in each different country environment. If they focus too much on the differences, however, the global screening process may undervalue the available markets. In many cases, environmental differences among national markets can be dealt with over time through appropriate strategies. This chapter suggested a new strategic guideline for global firms to pursue this new task of dynamic globalization.

In today's globalized and also localized economy, international managers selectively choose globalization and customization to maximize profits. However, the most important role of the global manager is not just to find profits but to add value to product and management by reducing local differences and unnecessary waste. Therefore, the debate on global standardization should focus on how to shift local product to global product, rather than on whether global standardization is good or not. This study has demonstrated that a preferred strategy is dynamic globalization and engineering efficiency is often more important than marketing efficiency in creating values. Further empirical studies would be necessary to establish whether the ideas presented in this study will make an impact on the success of global firms.

References

[1] Armstrong CM. Communications: The revolution continues. AT&T Web site, CEO Club of Boston, Boston College, Nov. 5, 1998.

[2] Bartlett CA. Building and managing the transnational: The new organizational challenge. In Michael E Porter, editor. Competition in global industries. Boston: Harvard Business School Press, 1986.

[3] Bartlett C.A, Ghoshal S. Managing across borders: The transnational solution. Boston: Harvard Business School Press, 1989.

[4] Capar N, Kotabe M. The relationship between international diversification and performance in service firms. Journal of International Business Studies 2003; 34(4): 345–355

[5] Chen J, Paliwoda S. Adoption of new brands from multi-branding firms by Chinese consumers. Journal of Euro-Marketing 2002; 12(1): 63–77.
[6] Douglas S, Wind Y. The myth of globalization. Columbia Journal of World Business 1987; winter: 19-29.
[7] Gabrielsson P, Gabrielsson M. Globalizing internationals: Business portfolio and marketing strategies in the ICT field. International Business Review 2004; 13(6): 661–684.
[8] Gates B. Digital nervous system – enterprise perspective. Microsoft Web site. Speech in New York, 24 March 1999.
[9] Ghoshal S. Global strategy: An organizing framework. Strategic Management Journal 1987; 8: 425–440.
[10] Gross T, Turner E, Cederholm L. Building teams for global operations. Management Review 1987; June: 32–36.
[11] Gupta A, Govindarajan V. Managing global expansion: A conceptual framework. Business Horizons 2000; 43(2): 45–54.
[12] Keegan W, Still R, Hill J. Transferability and adaptability of products and promotion themes in multinational marketing – MNCs in LDCs. Journal of Global Marketing 1987; 1(2): 85–103.
[13] Levitt T. The globalization of markets. Harvard Business Review 1983; May-June: 92–102.
[14] London T, Hart S. Reinventing strategies for emerging markets: Beyond the transnational model. Journal of International Business Studies 2004; 35(5): 350–370.
[15] March J. Exploration and exploitation in organizational learning. Organization Science 1991; 2(1): 71–87.
[16] McCutcheon D, Raturi A, Meredith J. The customization-responsiveness squeeze. Sloan Management Review 1994; winter: 89–99.
[17] Miller D. The generic strategy trap. The Journal of Business Strategy 1992; Jan.-Feb.: 37–41.
[18] Moon HC. The dynamics of Porter's three generics in international business strategy. In: Rugman Alan M, (editor). Research in global strategic management 1993; 4: 51–64.
[19] Moon HC. A revised framework of global strategy: Extending the coordination-configuration framework. The International Executive 1994; 36(5): 557–574.
[20] Moon HC. Choice of entry modes and theories of foreign direct investment. Journal of Global Marketing 1997; 11(2): 43–64.
[21] Moon HC. The new organization of global firms: From transnational solution to dynamic globalization. International Journal of Performability Engineering 2005; 1(2): 131–143.
[22] Oster SM. Modern competitive analysis, New York: Oxford University Press, 1990.
[23] Porter ME. Competitive strategy: Techniques for analyzing industries and companies, New York: The Free Press, 1980.
[24] Porter ME. Competitive advantage: Creating and sustaining superior performance, New York: The Free Press, 1985.
[25] Porter ME. The strategic role of international marketing. The Journal of Consumer Marketing 1986a; 3(2): 7–9.
[26] Porter ME. Competition in global industries: A conceptual framework. In Michael E Porter, editor. Competition in global industries, Boston: Harvard Business School Press, 1986b.
[27] Quelch JA, Hoff E. Customizing global marketing. Harvard Business Review 1986; May-Jun: 59–68.
[28] Sheth J. Global markets or global competition? The Journal of Consumer Marketing 1986; 3(2): 9–11.
[29] Simon-Miller F. World marketing: Going global or acting local? The Journal of Consumer Marketing 1986; 3(2): 5–7.
[30] Varadarajan R, Clark T, Pride W. Controlling the uncontrollable: Managing your market environment. Sloan Management Review 1992; Winter:39–47.

10

The Performance Economy: Business Models for the Functional Service Economy

Walter R. Stahel

The Geneva Association, Route de Malagnou 53
CH-1208 Genève, Switzerland

Abstract: The industrial economy creates wealth through the optimization of production processes and related material flows up to the point of sale; more growth means a higher resource throughput; a decoupling of growth and resource consumption is not possible. The shift to a more sustainable economy, to create wealth with substantially reduced flows of materials and energy, needs new business models. This chapter shows new business models to achieve the EU Lisbon objectives for 2010 – more growth and more jobs – while simultaneously reducing the resource consumption of industrialized countries. The new business models are grouped under the name of the performance economy, there common denominator is that they enable entrepreneurs to achieve a higher competitiveness with greatly reduced resource consumption and without an externalization of the costs of waste and of risk. The change from an industrial to a performance economy is full of opportunities but also obstacles. This chapter summarizes some of the major issues involved in such a shift; many others depend on the economic sector concerned and the national framework conditions in place. It also proposes two new metrics to measure the path towards the sustainability of corporations and to give sustainable investors a reliable guide for historic analysis and future projections.

10.1 Introduction

The dominating industrial economy is focused on the optimization of production and related material flows up to the point of sale (POS) as its principal means to create wealth. More resource throughput means more wealth – a situation which is still valid in situations of a scarcity of goods and services. Highly industrialized countries, however, need to develop economic models in which wealth creation and resource consumption are decoupled, and which achieve this economic optimization over the full life cycle of goods – production, utilization and re-marketing of goods and molecules.

One such economic model is the performance economy [4]) (see Figure 10.1), which bridges the gap between the 2010 Lisbon Objectives of the European Union – higher growth and more jobs – and the sustainability objective to considerably reduce the resource consumption – energy and materials – especially of industrialized countries:

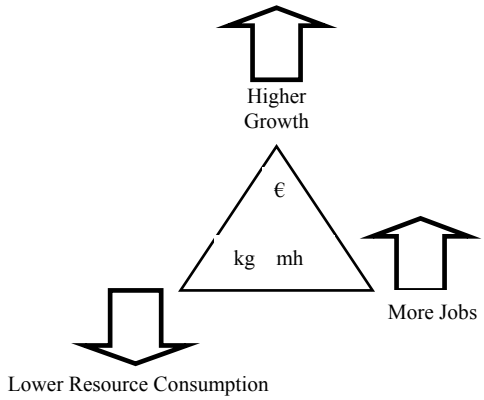


Figure 10.1. The objectives of the performance economy

By thinking "smart", companies and governments can economically profit from technological progress and at the same time contribute to sustainable development. But in order to measure the success of the performance economy, new metrics in the form of decoupling indicators are needed linked to:

- producing performance: **'$**-per-kg' ratio to measure wealth creation in relation to resource consumption, by using business models focused on intellectual asset management;
- managing performance over time: "man-hour-per-kg" ratio to measure job creation in relation to resource consumption, by using business models focused on phasical asset management;
- selling performance: business models that enable entrepreneurs to achieve a higher competitiveness without externalizing the costs of waste and risk.

A functional service economy that optimizes the use (or function) of goods and services and thus the management of existing wealth (knowledge, physical goods and nature) is an integral part of the performance economy. The economic objective of the functional service economy – to create the highest possible use value for the longest possible time while consuming as few material resources and energy as possible – means shifting from a production-oriented industrial economy toward a performance economy.

Sustainability

Sustainability depends on several interrelated systems. Each is essential for the survival of humans on Earth. This means that priorities cannot be argued over nor can there be speculation about which of these systems humankind can afford to lose first. In fact, humans cannot risk losing ground in any of these areas:

- The eco-support system for life on the planet (*e.g.,* biodiversity), a factor of the regional carrying capacity of nature with regard to human populations and human life styles.
- The toxicology system (qualitative, sometimes accumulative), a direct danger to man and increasingly the result of humankind's own economic activities.
- The flows-of-matter system (quantitative), a factor of planetary change (toward a re-acidification) and thus a danger to human life on Earth.
- Social ecology – the system of societal and economic structures, factors contributing to our quality of life.
- Cultural ecology – the system that defines cultural values and attitudes of producers and consumers.

The last two areas carry the idea of a sustainable society [1]. They encompass the broader objective of the longevity and sustainability of our civic and economic structures.

This insight was at the basis of the movement that coined the English term "sustainability" anew in the early 1970s. The emergence of the "green" movement and its use of the term sustainability missed the wider perspective of a sustainable society because they were based on the original term "sustainability" coined by Prussian gentleman foresters 200 years ago, a concept well known to the foresters of the early USA. The broader perspective includes considerations such as full and meaningful employment and quality of life. That perspective is necessary for understanding the importance of the social, cultural, and

organizational changes needed to create a more sustainable economy.

10.2 The Consequences of Traditional Linear Thought

Current economic systems are the result of linear thinking. For example, the terms "added value," relating exclusively to production, and "waste" to the end of the first (and often only) use phase of goods, are notions of a linear industrial economy. Similarly, manufacturers' liability for quality stops shortly after the point of sale (POS), at the end of the warranty period. At the POS, the buyer becomes responsible for the utilization and disposal of the goods purchased without knowing what materials are incorporated in the goods and without the operation and maintenance skills necessary to exploit the full technical product-life of the goods.

In contrast, cycles, lakes and loops have no beginning or end. In a true loop economy there is thus no added value or waste in the linear sense. A loop economy is similar to natural systems, such as the water cycle, but in contrast to nature has to search for the highest conservation of economic value. Moreover, quality has to be guaranteed and maintained over the full life cycle of goods.

Present national accounting systems and the use of the gross national product (GNP) as a measure of success is again an inheritance of the linear industrial economy. Adding income and expenses together is an indication of activity, not of wealth and well-being: waste management, car accidents, pollution control, and remediation costs all constitute positive contributions to the GNP at the same level as the manufacturing of goods. This shows a basic deficiency of national accounts. In this old frame of reference, sufficiency and (waste) prevention corresponds to a loss of income which is economically undesirable. From a sustainability and performance economy view, waste and loss prevention (*e.g.*, accidents) is a reduction of costs that contributes to substantial national savings. For instance, waste management in Germany costs the economy (but contributes to GNP) in excess of US $545 billion per year. Waste prevention could reduce the need for this management cost and contribute to national wealth through sufficiency.

When discussing the benefits of moving toward a more sustainable society and searching for metrics to gauge such change, it is important to keep the inability of the non-sustainable national accounting systems in mind to measure, *e.g.*, the contributions of sufficiency strategies.

10.3 Resource-use Policies Are Industrial Policies

The choice of the best waste-management strategy is often a self-fulfilling prophecy. The promotion of recycling strategies – closing the material loops – conserves the existing economic structures and is thus easy to implement. Unfortunately, an increase in the amount of secondary resources can cause an oversupply of materials and depress the prices of virgin and recycled resources alike. The result is a problem of oversupply and sinking resource prices that jeopardize the economics of recycling. Future technical innovation in recycling will include improvements in design for the recyclability of goods and new recycling technologies, both of which cannot overcome the basic price squeeze mentioned [3]. Increased recycling does not reduce the flow of material and energy through the economy but it does reduce resource depletion and waste volumes, that is the beginning and end of the linear economy.

In contrast to recycling, strategies for higher resource efficiency reduce the volume and speed of the resource flows through the economy. One of the keys to resource efficiency is the take-back strategy: closing the (product and material) *responsibility loops*. However, strategies of higher resource efficiency counter the validity of the present calculus of economic optimization that ends at the point of sale. At first sight, closed responsibility loops even seem to violate traditional task definition in the economy: Industry produces efficiently, consumers use quickly, and the state disposes efficiently.

Strategies to close the product responsibility loops, such as the voluntary or mandatory take-back of consumer goods, impose structural changes

and new business models and are thus more difficult to implement than the recycling of materials. These strategies are driven by innovative corporate approaches, such as Xerox's asset management programme, as they are more competitive as well as more sustainable. These strategies will become even more competitive as the functional service economy develops, energy and resource prices rise and framework conditions change accordingly [9]. Future technical innovations that can be expected in this field are those that enable the use of remanufactured and technologically upgraded components and goods as well as commercial innovations to keep goods in use as long as possible.

Coming changes in framework conditions may include increased taxes on the consumption of non-renewable resources, and/or bonuses on resource consumption reductions, such as tradable CO_2-emission rights on non-manufacturing activities, such as remanufacturing and other utilization optimization services.

Higher resource efficiency through an optimization of the use of goods can be measured as "resource input per unit of use" over long periods of time and will cause substantial structural change within the economy. Again, the change will be helped by the fact that these strategies increase competitiveness. An early adoption may thus give a considerable long-term advantage to companies that dare to change first (first mover advantage). Among the strategies for higher resource efficiency are those for a longer and more intensive use of goods, those for dematerialized goods and those for innovative system solutions (Table 10.1). Among the innovations to emerge from a promotion of higher resource efficiency are both new technical and new commercial strategies to improve use.

A reduction in the flows of matter through the economy can be achieved by decreasing the volume of flow (through innovative multi-functional products and a more intensive use of products and system solutions) or by slowing the speed of flow (*e.g.*, through the remanufacturing and remarketing of goods to extend their service life).

The biggest potential is hidden in innovations at system level, to redesign components, goods, and systems that reduce material use in manufacturing and in reducing the costs of operating and maintaining the goods in use (see Figure 10.2).

10.4 The Problem of Oversupply

The economies of industrialized countries are characterized by several key factors [2]:

- Their populations account for only 20% of the world population but for 80% of world resource consumption.
- Their markets for goods are saturated and the stocks of goods represent a huge storage of resources. For built infrastructures, there is also an increasing financial burden with regard to operation and maintenance costs of ageing infrastructures.
- Their economies suffer from oversupply, which indicates that the old remedy of a higher economy of scale (centralization of production to reduce manufacturing costs) can no longer solve the economic problems or the sustainability issue. The reason for this is that the costs of the services that are instrumental for production are a multiple of the pure manufacturing costs; a further optimization of production therefore does not make economic sense.
- Incremental technical progress is faster than product development: substituting new products for existing ones will increasingly restrain technological progress compared with the alternative of a fast technological upgrading of existing goods.

The situation for the economies of many developing countries, however, is radically different. These countries will continue to experience a strong demand for basic materials for the construction of their infrastructures and will continuously suffer from a shortage of affordable resources and mass-produced goods, including food, shelter, as well as infrastructure and services

Table 10.1. Resource efficiency and business strategies in the service economy

Resource efficiency objectives	**Implementation of strategies**	
	Closing material loops (technical strategies)	**Closing liability loops** (commercial/marketing strategies)
Reduce the volume of the resource flow	**Ecoproducts** • dematerialized goods • multifunctional goods	**Ecomarketing** • shared utilization of goods • selling *utilization instead*
Reduce the speed of the resource flow	**Remanufacturing** • long-life goods • product-life goods • cascading, cannibalizing	**Remarketing** • de-curement services • away-grading of goods and components • new products *from waste*
Reduce the volume and the speed of the resource flow	**System solutions** • Krauss-Maffei plane transport system	**Systemic solutions** • lighthouses • selling results instead of goods • selling *services instead of goods*

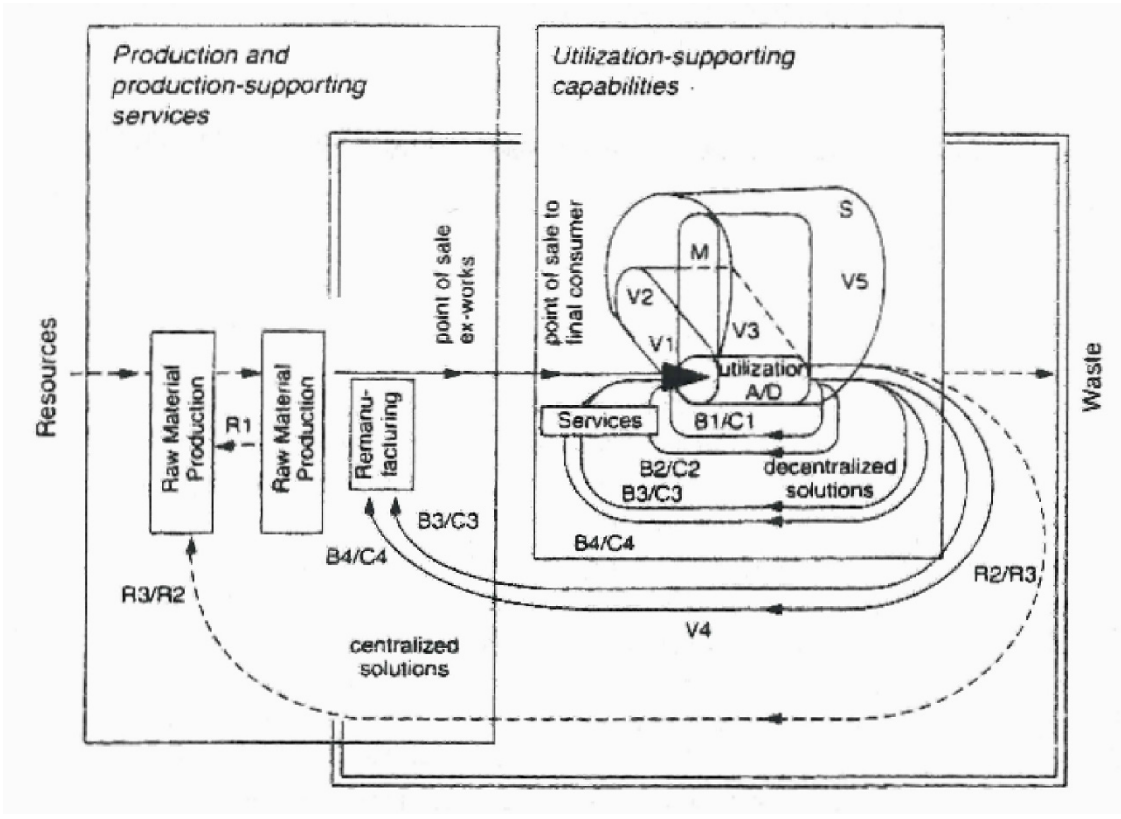


Figure 10.2. Strategies for higher resource efficiency (adapted from [11])

for health and education. Resource efficiency in industrialized countries will ease World market pressure on the prices of resources.

10.5 The Genesis of a Sustainable Cycle

A great deal of change in how we think about economics is necessary for understanding a "life after waste" industrialized society. A critical change is to shift to a service economy in loops detailed in Figure 10.2 [2]. Cycles have no beginning and no end. Economically, the most interesting part of the cycle and new focal point is the physical management of the stock of existing goods in the market. Economic well-being is then no longer measured by exchange value and GNP but by the use-value of a product and the wealth presented by the stock of existing goods. This is not only true for durable goods but equally for areas such as health and education, where the yardstick must be a better health of the population and a higher qualification of children, not the expenses to achieve this.

Long-term ownership of physical assets becomes the key to the long-term (rental) income of successful companies, and with that ownership comes unlimited product responsibility that includes the cost of risk and cost of waste. Strategies of selling the use of goods instead of the goods themselves (*e.g.*, Xerox selling customer satisfaction) and business models that provide incentives to customers to return goods to manufacturers become keys to long-term corporate success. The adaptability of existing and future goods to changes in users' needs and to technological progress (to keep them current with technological progress) becomes the new challenge for designers and engineers. The economic structure must maximize the return from these new resources: a fleet of existing goods in a dispersed market. An adaptation of today's economic, legal, and tax structures to these new requirements may become a decisive competitive advantage for countries to attract and breed successful economic players for a sustainable functional performance-focused service economy.

Several multinational companies such as Schindler, Caterpillar and Xerox have already started to successfully implement these new strategies. Schindler sells "carefree vertical transport" instead of elevators, a strategy that provides all the services needed by customers (*i.e.*, maintenance, remanufacturing, and technological updating of elevators). In addition, there is a telephone connection linking every elevator 24 hours a day to an emergency service center. In collaboration with the decentralized maintenance crews of the manufacturer, this system ensures that no person ever gets stuck for more than a few minutes in an elevator that has stopped functioning for technical reasons.

Xerox's asset management program is focused on selling customer satisfaction that is photocopying services instead of photocopiers. Asset recovery is now part of a new business process that includes an asset re-uses management organization. Xerox has decoupled manufacturing volume from turnover and profits, regionalized activities, and changed its skill pool and employee responsibilities accordingly.

I. Strategies for slowing down the flow of matter through the economy
   - A. Long-life goods: Philips induction lamp, Ecosys printer
   - B. Product-life extension of goods:
     - B1. Reuse: re-useable glass bottles
     - B2. Repair: car windscreen, flat tire
     - B3. Remanufacture: re-treaded tires, renovated buildings
     - B4. Technology upgrading: Xerox copier '5088, mainframe computers
   - C. Product-life extension of components:
     - C1. Reuse: refill printer cartridges, roof tiles
     - C2. Repair: welding of broken machine parts, re-vacuum insulating windows
     - C3. Remanufacture: remanufacturing engines and automotive parts
     - C4. Technology upgrading: upgrading of (jet) engines to new noise and emission standards
   - D. Remarketing new products from waste (product-life extension into new fields)

II. Strategies for reducing the volume of matter through the economy
  M. Multifunctional goods: fax-scanner-printer-copier all-in-one, Swiss Army knife, adaptable spanner
  S. System solutions: micro cogeneration of cold or heat and power, road railers
III. Strategies for a cradle-to-cradle product responsibility
IV. Commercial or marketing strategies
  IV1. Selling use instead of goods: operational leasing of cars, aircraft, trucks, construction equipment, medical equipment, photocopiers, rental apartments
  IV2. Selling shared-use services: Laundromats, hotels (beds),
  IV3. Selling services instead of products: lubrication quality instead of engine oil
  IV4. Selling results instead of products: pest-free and weed-free fields instead of agro chemicals, individual transport instead of cars
  IV5. Monetary bring-back rewards: 10-year cash-back guarantee

10.6 The Factor Time – Creating Jobs at Home

How will this shift to a loop economy impact the factor inputs into the economy? The following Figure 10.3 shows the development of the life cycle costs for operating an automobile over 50 years.[1] This analysis is representative for the life-cycle costs of most durable goods.

At the POS, the producer-distributor in an industrial economy sells a durable good to the user-consumer, the sales price being equal to the exchange value. The value embedded in the product is represented mostly by the nonrenewable (depletable) ENERGY + MATERIALS used in the manufacturing and distribution processes; making up nearly 100%. Labor is a small part of the manufacturing input.[2] The sales price remains constant throughout the utilization period, so its relative weight will decrease over time. It is represented by the left upper triangle in Figure 10.3.

During the utilization period, the main resources employed are renewable, mainly in the form of human labour for such service activities as maintenance and repairs. These MANPOWER costs accumulate over the years, up to a ceiling of about 75%, and are represented by the lower right triangle in Figure 10.2.

Spare parts and components make up a relatively stable 20% of life-cycle costs (the dark wedge). These parts have a high potential to be remanufactured in the loop economy, adding up to 15 additional percentage points to the pure manpower input shown in Figure 10.3.

With increasing service-life (years of utilization), the cost share of depletable resources diminishes rapidly, while renewable resources (manpower) increases. A strategy of service-life extension for durable goods – such as infrastructure, buildings, ships, aircraft, equipment and cars – is thus equivalent to a substitution of manpower for energy and materials.[3] This strategy creates jobs at home while at the same time reducing resource throughput in the economy. It also has a much higher value-per-weight ratio than manufacturing, as will be shown later. In addition, it preserves energy investments (also called gray energy) and reduces CO_2 emissions.

Skilled and experienced craftsmen are needed in repair and remanufacturing activities, which can be undertaken in comparatively small workshops, scattered widely throughout the country where there is a need for product renovation and customers for them, as is the case with car-repair workshops. These enterprises can be located in any rural or urban area with high unemployment, making product-life extension a doubly attractive proposition for job creation.

[1] The figures are based on the Life-Cycle Costs of the author's car, a 1969 Toyota Corona Mk II

[2] According to a press communication by Wofgang Bernhard, Head of VW division at Vokswagen AG Wolfsburg, workers at VW need 50 hours to build a car, while the industry average is 25 hours

[3] See also [7]

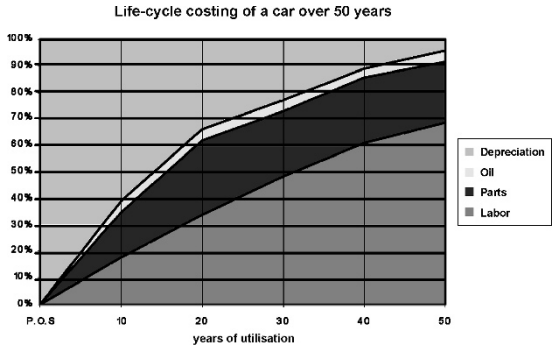


Figure 10.3. Evolution of the life cycle costs for goods in the Lake Economy

10.7 Strategic and Organizational Changes

In contrast to the manufacturing economy, economic success in the sustainable service economy does not arise from mass production but from good husbandry, caring attitudes and stewardship. Economic rewards come from minimizing tasks needed to transfer a product from one user to the next. Local reuse after a quality check or repair by the manager's representative is the smallest possible cycle in Figure 10.2 and the most profitable strategy. A product that can no longer be commercialized (*i.e.*, rented or used) will be remanufactured and upgraded or, in the worst case, be dismantled with the aim of reusing its components for new products. If there is no re-use possibility, the materials can be recycled and used to manufacture new components.

To achieve the smallest cycles, a different economic and organizational mindset is necessary in several areas:

- The industrial structure for manufacturing and remanufacturing activities will have to be regionalized in order to be closer to the market assets. This proximity demands the capability to handle smaller remanufacturing volumes more efficiently. Appropriate methods for such purposes will have to be developed and skilled labor trained. The cost for such a change is offset by dramatic reductions in the purchase of materials and the virtual elimination of disposal costs.
  - Products will have to be designed as technical systems that are part of pre-designed modular master plans. Such plans will facilitate ease of maintenance and ease of out-of-sequence disassembly by workers or robots.
- Components will have to be designed for remanufacturing and technological upgrading according to the commonality principle. This principle was first used by Brown Boveri Company in the 1920s to design its revolutionary turbo compressors. It has been perfected by Xerox in the 1990s in the design of its copiers. The commonality principle promotes standardized multi-product function-specific components that are interchangeable among different product lines.
  - Goods and standardized components will increasingly be designed to be maintenance free, self-protecting and fault tolerant, which greatly reduces operating costs (such as service interventions, repairman training and spare-parts management).
- New technologies aimed at optimizing the resource efficiency and safety of products and components over long periods of time will have to be developed. These include spare less repair methods, in situ quality-of-function monitoring systems, and memory chips to register life-cycle data.
  - Business models to sell performance instead of goods (Table 10.2 explains the differences), such as the "pay by the hour" for jet engines of GE and Pratt & Witney, integrate many of the above issues into the economy.

- New professions and job qualifications will emerge, such as operation and maintenance engineers. The salesperson of the past will have to become customer advisor able to optimize generic products for the needs of specific users, and to upgrade existing products according to the wishes of the user as technology advances. For the first time since the beginning of the Industrial Revolution, the economy will offer workplace mobility rather than rely on worker mobility. The more immaterial goods that are transported, the greater the feasibility of telecommuting. Flexible work periods and part-time work are compatible with and even a necessity for, providing services and results around the clock.

Table 10.2. Selling performance *versus* selling products

Efficiency strategy **Sale of a product** [industrial economy]	**Sufficiency strategy** **Sale of a performance** [functional service economy]
The object of the sale is a product	The object of the sale is performance, customer satisfaction is the result
Liability of the seller for the manufacturing quality [defects]	Liability of the seller for the quality of the performance [usefulness]
Payment is due for and at the transfer of the property rights ['as is where is'-principle]	Payment is due pro rata if and when the performance is delivered ["no fun no money" principle]
Work can be produced centrally/ globally [production], products can be stored, re-sold, exchanged	Work has to be produced in situ [service], around the clock, no storage or exchange possible
Property rights and liability are transferred to the buyer	Property rights and liability remain with the fleet manager
Advantages for buyer: • right to a possible increase in value • status value as when buying performance	Advantages for the user: • high flexibility in utilization • little own knowledge necessary • lost guarantee per unit of performance zero risk • status symbol as when buying product
Disadvantages for buyer: • zero flexibility in utilization • own knowledge necessary [driver licence] • no cost guarantee • full risk for operation and disposal	Disadvantages for user: • no right to a possible increase in value
Marketing strategy = publicity, sponsoring	Marketing strategy = customer service
Central notion of value: high short-term exchange value at the point of sale.	Central notion of value: constant utilization value over long-term utilization period.

- Users (ex-consumers) will have to learn to take care of the rented or leased products as if they owned them, to enjoy the new flexibility in product-use offered by a use-focused service economy. Whereas in the industrial economy, misuse and abuse of products lead to a financial punishment inthe form of increased maintenance cost for the owner-user, in the service economy they may lead to the exclusion of a user from the use-focused system.

10.8 Obstacles, Opportunities, and Trends

Many of the obstacles that need to be overcome on the way to an economy optimizing multiple service-lives or use-cycles are embodied in the logic of the present linear industrial economy. The definition of quality, for example, is based on the absence of manufacturing defects only (limited to 6 or 12 months) and on the newness of components in new goods. The logic framework of a functional economy requires a demand-side definition of quality based on unlimited customer satisfaction and the guarantee of a system functioning over longer periods of time.

The definition of "quality" in the performance economy integrates

- technology management (efficiency),
- risk management (preventive engineering) and
- the factor time (sustainability management),

and redefines quality as the three-dimensional vector of a long-term optimization of system functioning, which is a synonym for performance (Figure 10.4).

A functional service economy needs an appropriate structure. The characteristics include a regionalization of jobs and skills, such as mini-mills for material recycling, remanufacturing workshops for products, decentralized production of services (*e.g.*, rental outlets), local upgrading and take-back, supplemented by centralized design, research, and management centers. Such an economy will consume fewer resources and have higher resource efficiency, and its production will be characterized by smaller regionalized units with a higher and more skilled labor input. Transport volumes of material goods will diminish and be replaced by transports of immaterial goods such as recipes instead of food products, software instead of spare parts.

The signs on the horizon clearly point to a use-focused economy:

- The European Community-directives on product liability and more recently on product safety and the draft directive on service liability all stipulate a 10-year liability period, or impose a manufacturers disposal liability (end of life vehicles, WEEE).
- Some car manufacturers offer a total cost guarantee over three or five years, which includes all costs except tire wear and fuel.
- Industry shows an increasing willingness to accept unlimited product responsibility and to use it aggressively in advertising, through money-back guarantees, exchange offers, and other forms of voluntary product take-back and is learning to make product retake and remarketing a viable business division.
- Out-sourcing has rapidly become a generally accepted form of selling results instead of (capital) goods or services.

Companies and regions that initiate the change toward a sustainable society rather than suffering the consequences of it through the actions of their competitors will have a head start and be able to position themselves strategically. An old, but in the age of market research somewhat forgotten, truth of economies will play its heavy hand again: Real innovation is always supply driven – the role of demand is one of selection [2].

10.9 New Metrics to Measure Success in the Performance Economy

To measure shift from an industrial to a performance economy, we need new metrics in the sense of decoupling indicators, which can be used for individual goods by the customer at the POS,

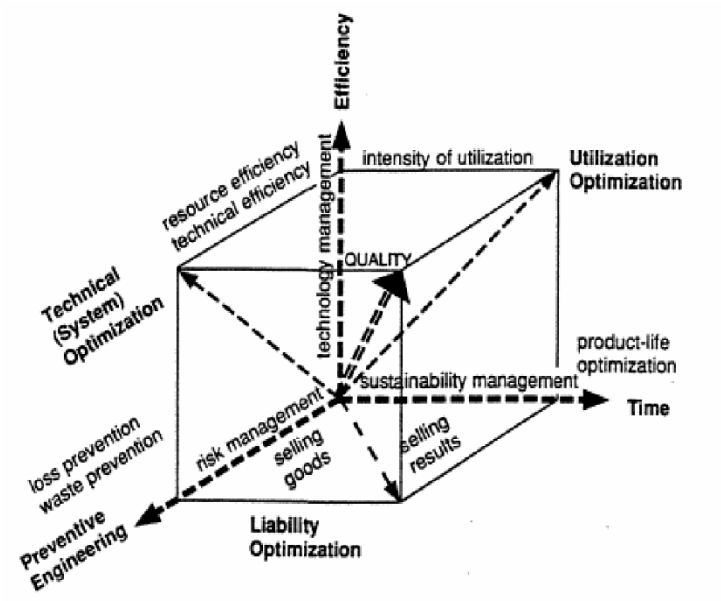


Figure 10.4. The quality cube of the performance economy (adapted from from [6])

but also calculated on an annual basis for plants, corporations, economic sectors or nation states.

These new metrics in the form of decoupling sustainability indicators were already mentioned in the Introduction:

- producing performance: "$-per-kg" ratio to measure wealth creation in relation to resource consumption;
- managing performance over time: "man-hour-per-kg" ratio to measure job creation in relation to resource consumption;
- selling performance: new business models that enable entrepreneurs to achieve a higher competitiveness without externalizing the costs of waste and risk.

OECD coined the term DEI – decoupling environmental indicator. The term decoupling refers to breaking the link between *environmental bads* and *economic goods.* It refers to the relative growth rates of a direct pressure on the environment and of an economically relevant variable to which it is causally linked. Decoupling occurs when the growth rate of the environmental pressure (EP) is less than that of its economic driving force (DF) over a given period. One distinguishes between *absolute and relative decoupling.* Decoupling is said to be absolute when the environmental variable is stable or decreasing while the economic variable is growing. Decoupling is relative when the environmental variable is increasing, but at a lower rate than the economic variable.

The decoupling indicators of the Performance Economy go beyond the OECD's DEIs, which are environmental and ecological, as they also include the social pillar of sustainability.

10.10 Regionalization of the Economy

The performance economy will lead to a regionalization of economic activities for a number of reasons.

Producing performance through, *e.g.*, nano- and life-sciences means in some cases to localize production for technical reasons, such as

- lab-on-a-chip – micro high-tech production units that can produce small quantities of the desired substances much more efficiently than a big production unit;
- some nano-products, such as nano carbon tubes (NCT), cannot be transported and have to be produced at the place of their integration in other goods;
- the leasing of smart materials imposes the leasing of the final goods in the performance economy as well as a loop economy (take-back guarantees).

Maintaining performance over time through, *e.g.*, remanufacturing and remarketing is under the axiom of the loop economy, which says that the smaller the loop, the higher the profitability is cheaper remanufacturing services are best done regionally

Business models of selling performance instead of goods are based on locally available services. As services cannot be produced in advance and stored but have to be delivered at the location of the client when needed, a decentralized service structure available 24 hours 346 days a year are necessary in many cases.

In addition, these business models mean sustainable profits without an externalization of the cost of risk. Business interruptions in the global economy will become more frequent through the criticality of transport systems and networks, be it for physical goods, energy or data. Terrorism and pandemics are just two reasons that can lead to a shut-down of the world economy for a few days or weeks. Just-in-time production and delivery chains can then no longer be guaranteed.

10.11 Conclusions

The shift in the economy towards a more sustainable society and a functional service economy has begun some time ago. However, most experts are unaware of the fundamental change, probably because they interpret the signs on the horizon in terms of the old industrial economic thinking. A performance economy will not solve all the problems of this world, and especially not the inherited problems from the past (*e.g.*, pollution cleanup and unemployment of overspecialized production workers); nor will it make the manufacturing sector superfluous. However, the industrial sector could well be split into high-volume producers of global standardized components and regionalized assemblers (*e.g.*, computer components and DELL) and regional remanufacturers and remarketeers of products active in the physical asset management of industrialized regions.

References

[1] Coomer JC. Quest for a sustainable society. Elmsford. New York: Pergamon Policy Studies, 1981.

[2] Giarini Orio, Stahel Walter R. The limits to certainty - facing risks in the new service economy. Boston. MA.: Kluwer, 1989/1993.

[3] Jackso Tim. Clean production strategies: Developing preventive environmental management in the industrial economy. Lewis, Boca Raton, FL, 1993.

[4] Stahel Walter R. The performance economy. London: Palgrave, 2006.

[5] Stahel Walter R The utilization-focused service economy: Resource efficiency and product-life extension. In: Allenby BR, Richards DJ, editors. The greening of industrial ecosystems. Washington. D.C.: National Academy Press, 1994; 178–190.

[6] Stahel Walter R. The functional economy: Cultural and organizational change. International Journal of Performability Engineering 2005; 1(2):121–130.

[7] Stahel Walter R., Reday-Mulvey, Geneviève Jobs for tomorrow, the potential for substituting manpower for energy. Report to the Commission of the European Communities, Brussels, and Vantage Press, New York, 1976/1981

11

Cleaner Production and Industrial Ecology: A Dire Need for 21st Century Manufacturing

Leo Baas

Erasmus University Rotterdam,
Room M7-16, P.O. Box 1738, 3000DR Rotterdam,
The Netherlands

Abstract: The chapter discusses the dissemination of the concepts of cleaner production and industrial ecology as an operationalization within the framework of *sustainability systems* in the industrial practice. Experiences in cleaner production and industrial ecology projects show that an open, reflective and on-going dialogue must be designed to develop trust, transparency and confidence to ensure real involvement of diverse stakeholders in charting the future of their organizations and regions as part of the transition to sustainable societies. The integration of ecological, economic, social and cultural dimensions of corporate activities become a dire need for a sound use of scarce resources in the 21st century.

11.1 Introduction

Cleaner production and industrial ecology are known concepts worldwide, however, their dissemination is not an easy process. The concepts of *cleaner production* can be described as "the continuous application of an integrated, preventive environmental strategy to both processes and products to reduce risks to humans and the environment [1]". *Industrial ecology* is described as "an integrated system, in which the consumption of energy and materials is optimized and the effluents of one process serve as the raw material(s) or energy for another process [2]".

As a process of dissemination of new concepts, the cleaner production paradigm was introduced to industrial leaders as a prevention-oriented paradigm for achieving cleaner industry and more sustainable communities; this was viewed as an important way to supplant or supplement the old paradigm of pollution control. In the cleaner production paradigm, the conceptual approach was to catalyse the transition from *waste management policies and approaches at the end-of-the-pipe,* to *"environment included"* in *industrial innovation policies for waste prevention* and *waste minimization* at the sources of the problems [3]. Industrial routines are embedded in unsustainable practices that are difficult to change. The complexity and uncertainties of new concepts are often approached with ignorance and mis-perception. Nevertheless the integration of economic, environmental and social dimensions in industrial activities is increasingly perceived as a necessary condition for a sustainable society.

This chapter discusses the dissemination of the concepts of cleaner production and industrial ecology as an operationalisation within the framework of *sustainability systems* in the industrial practice. At first in Section 11.1.1, some reflection is given to climate change as new environmental policy incentive in the context of global trends and their local adaptation processes. In Section 11.2 the dissemination of new preventive concepts is reflected upon at the macro, meso and micro levels in societies. The practical experiences with the dissemination of cleaner production and industrial ecology concepts are connected to the theoretical notions of embeddedness in Section 11.3. For insight in the challenges of the introduction of industrial ecology concepts, the results of industrial ecology programs in the Rotterdam harbor and industry complex are described in Section 11.4. This section is followed by an analysis of the lessons learned on the introduction and dissemination of the concepts of cleaner production and industrial ecology as interaction between theory and practice in Section 11.5. Finally, conclusions and recommendations for a dire need for manufacturing sustainability systems are formulated in Section 11.6.

Climate Change as Environmental Policy Incentive

Climate change worries many persons in the world, because direct effects are also seen all over the world: from the melting ice in Greenland to the vanished snow at the top of the Kilimanjaro in Tanzania [4]. Nevertheless, the responsibility at the environmental policy level is still diffuse. Both at the public and private policy levels much depends on the sense of emergency [4] of responsible managers in combination with the emerging elaboration of social responsibility.

In the past decade, global trends in environment related issues within multi-national corporations have incorporated different dimensions in the concepts of environmental management (ecology), cleaner production (ecology, economy), industrial ecology (ecology, economy) and corporate social responsibility (ecology, economy, social aspects).

The trends in production facilities have been:

- Outsourcing of (mass) production by the northern corporations: to China, Vietnam.
- Near-sourcing of production: USA to Mexico; Western Europe to Central Europe.
- Emerging national mass production facilities: such as in China, India, Vietnam.

These trends involve that working with preventive concepts needs to estimate the context of their embeddedness in the society and the involvement of relevant partners.

At a global environmental policy level implementation processes are related to agreements and strategies such as:

- Johannesburg Declaration on Sustainable Development [5].
- United Nations Millennium Declaration [7].
- UNIDO's Corporate Strategy with focus on Environmentally Sound Technologies and CP market mechanisms [8].
- UNEP's incorporation of Human Development through the Market [8].

It has also to be taken into account that the world population urbanization trend is expected to grow to 60% of the world population living in urban areas in 2040 (developing countries are expected to grow to an urbanization grade of 50% in 2020) [10].

Worldwide the urban problems are concentrated upon: water management, energy, air pollution, and mobility. A recent publication [11] concludes the fact that the following activities and product groups cause 70% to 80% of the total environmental impacts in society:

- Mobility: automobile and air transport.
- Food: meat and dairy, followed by other types of food; and
- The home, and related energy use: buildings, and heating-, cooling-, and other energy using appliances.

In the meantime, tourism, including many aspects of the above mentioned activities, has become the biggest economic sector in the world [4].

The environmental impacts of urban problems can be covered by cleaner production system approaches. Experiences with the dynamic aspects

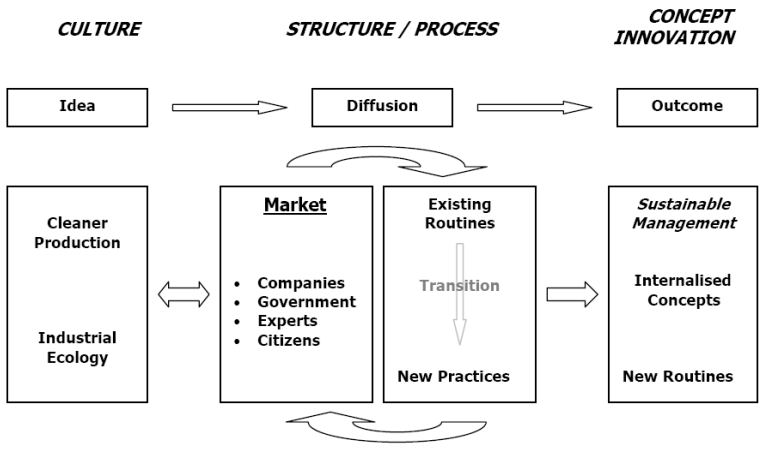


Figure 11.1. The arena of transition processes of new concepts

of the introduction and dissemination of cleaner production and industrial ecology reflect several theoretical notions that are worthwhile to consider in discussing future trends (n*othing is more practical than a good theory*) [11].

11.2 Different Levels of the Dissemination of Preventive Concepts

All considerations about the introduction of (new) concepts such as cleaner production and industrial ecology face an institutionalized arena with routines on environmental performance that challenge *changes in routines* in the competition to achieve better market positions. As the preventive approach is presented as a better business practice, the cleaner production concept provides *prevention as vision* as a label, the *cleaner production assessment* in an organization as instrument for problem analysis, the *cleaner production options* and the integral approach of *continuous improvement* as solutions, and the *cleaner production demonstration projects* as part of a *cleaner production dissemination infrastructure* as the applications of successes.

The *arena* of transition processes of new concepts is visualized in the following model shown in Figure 11.1 [3].

It is assumed that a representative of one of the four societal categories in the market of concept transition processes figure will explore a new concept such as cleaner production and industrial ecology knowledge dissemination. Committed to the new concept, the introducing actor(s) will approach organizations to explore it. After the introduction, acknowledgement and acceptance of the concept, learning (explicit or implicit) and change processes connected to the new concept affect expertise at the individual and organizational levels. In this thesis, the concepts of cleaner production, industrial ecology and sustainability are connected to the micro, meso and macro levels. The different levels are used in relation to system boundaries such as single organizations, organizations located in regions or as members of an industrial sector, and society. There are also levels within an organization that affect the dissemination of a new concept. For instance, for the introduction of cleaner production, the focus is on single organizations; outside actors can introduce the concept and the translation by internal actors might affect the routines. The introduction of industrial ecology goes beyond single organizations, which means that actors outside the companies will influence the overall processes in a dependent manner in relation to the individual company managers.

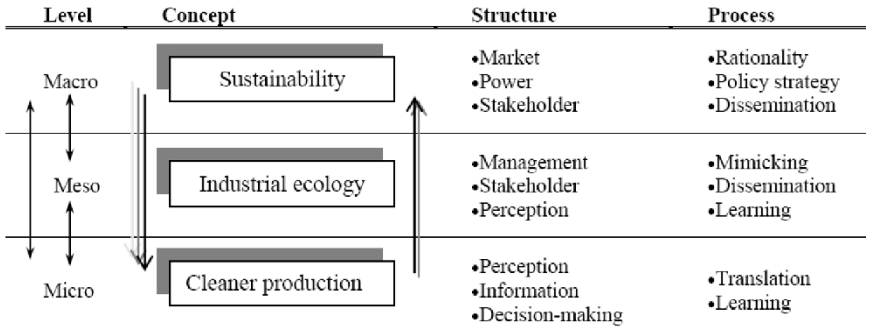


Figure 11.2. The multi-level concept innovation model

The different levels of preventive concepts involve the issue of system boundary. Although one might analyze cleaner production at the micro level of companies and industrial ecology at the meso level of industrial estates, [3] a systems approach of the concept of cleaner production involves the interconnection to industrial ecology and sustainability can be labeled by c*leaner production systems* or s*ustainable consumption and production systems* (see Figure 11.2).

The capacity and capability to break through existing routines is part of an eventual organizational change. Learning processes related to the new cleaner production concept face the techno-structure based on an engineering perspective at the micro level that dominates its translation. The learning processes for industrial ecology face a (plant) management perspective that is limited to the system boundary of their organisation. At first glance, the translation of the new concept is mainly based on mimicking. Both mimicking and dissemination include learning processes. Mimicking involves above all the reception or passive translation of knowledge, while dissemination includes a process of knowledge transfer. At the macro level policy strategy development, both at the private and public organizational levels, is subjected to the influence of translation processes of stakeholders.

Normative concepts – such as the *prevention is better than cure* approach of cleaner production projects – assume implicitly the involvement of all members of the organization in identifying and implementing both non-technical and technical improvements. The following individual and organizational learning processes are experienced according to different dimensions such as:

- Individual learning by members of an organization to look after and cope with incremental (first order) and radical (second order) changes in their organizations [13].
- Different levels at the individual and organizational learning level with single-loop, double-loop, and triple-loop learning processes [14].
- Different types of learning effects: *Learning by doing*, *learning by interaction*, *learning by using*, and *learning by learning* [15].
- Different ways of learning: Strategic or tactical learning [16].

11.3 Practical Experiences and Types of Embeddedness

Several conclusions can be drawn from the shift from environmental technology towards cleaner production [3]. Industrial environmental protection started on a pollution control basis with control technologies. The 1970s can be characterized as a pure technology engineering approach to control pollution. In the 1980s, public policy development included the emergence of integrated environmental policies and new economic and voluntary instruments.

During the cleaner production emergence phase, university experts set up cleaner production

research projects, whilst during the growth phase consulting firms mediated the dissemination of results. This process has been repeated in many countries in Europe. UNEP and UNIDO organizations also mimicked the dissemination of the concepts through demonstration projects, instruction manuals and in a later phase dissemination policies with stakeholder involvement. Another aspect of the institutionalization process is professionalization, in the shape of specialized expertise, national, regional and global expertise networks and expert and scientific journals.

In general, during the emergent phase of a new approach, there is space to reflect about further development. However, the status of the *cleaner production assessment method* meant that the label embodied an encoded knowledge approach that became the basis for preventive developments. As a result, it created a trade-mark that was not open to further dialogue. Although the cleaner production assessment was designed with several feedback loops, in practice the assessment developed as a one-loop learning process, ending with a *cleaner production plan* after the feasibility phase. The engineering approach, based on encoded knowledge, largely dominated the characteristics of the cleaner production concept. Furthermore, demonstration projects had to show practical results. All these activities developed in the direction of a mature phase of institutionalization and stronger internationalization. Also, professionalization and specialization are characteristics of a mature phase. However, societal dissemination processes ask for more ingredients in continuous social change processes and this has been hardly the case [3].

The year 1989 can be regarded as a starting point because of the re-emergence on the environmental agenda of industrial ecology in the wake of an article by Frosch and Gallopoulos [2]. The U.S. Academy of Engineering promoted the concept very much. Also a link with the Japanese Ministry of Trade and Industry was established and strengthened in the course of several workshops in the period 1993–1994 [17].

The most famous reference in the field of applied industrial ecology is the *Industrial Symbiosis*[1] project in Kalundborg in Denmark [18]. Every book (including this book), numerous articles and conferences about industrial ecology make repeated reference to the Kalundborg industrial area. The Kalundborg situation has been copied all over the world since the mid-1990s. In discussions of, and references to, the Kalundborg system it is seldom reported that that Industrial Symbiosis program grew organically on a social-economic basis in a small community where plant managers knew and met each other in a local community atmosphere.

In the last 30 years of the community's evolution, a partnership grew between several industrial plants, farmers and the municipality of Kalundborg. This partnership led to huge improvements in the environmental and economic performances of the Kalundborg region [19]. The core partners in Kalundborg are a power station, an oil refinery, a plasterboard factory, an international biotechnological company, farmers and the municipality. These partners voluntarily developed a series of bilateral exchanges such as:

- The refinery provides the plasterboard company with excess gas.
- The power station supplies the city with steam for the district heating system.
- The hot cooling water from the power plant is partly redirected to a fish farm.
- The power plant uses surplus gas from the refinery in place of coal.
- The sludge from the biotechnological company is used as fertilizer in nearby farms.
- A cement company uses the power plant's desulphurized fly ash.
- The refinery's desulphurization operation produces sulphur, which is used as a raw material in the sulphuric acid production plant.
- The surplus yeast from the biotechnological company is used by farmers as pig feed.

[1] The Industrial Symbiosis label was introduced by the spouse of a plant manager in Kalundborg in Autumn 1989 (According to Jørgen Christensen in New Haven, 8 January 2004).

In practice the concept of eco-industrial parks evolved from waste exchange between companies towards integrated regional ecosystems. The implementation of industrial ecosystems was considered on existing (*brown fields*) and new (*green fields*) industrial areas. An industrial ecosystem must be designed in relationship with the characteristics of the local and regional *ecosystem* but its development must also match the resources and needs of the local and regional *economy*. According to Lowe [19], these dual meanings reinforced the need for working in an inquiry mode: learning from the experiences of other communities developing industrial ecosystems is important.

A compressed air pilot study in an industrial symbiosis project in the Rotterdam harbor and industry complex (INES project) [3] presented instructive challenges. A feasibility study showed that the usage of compressed air was lower than expected (7,000 Nm^3/hr instead of the presumed 12,000–15,000 Nm^3/hr). The results meant that the economy of scale needed for cost reduction was insufficient. Compounding the problem of diminished economies of scale, the supplier was very busy with the installation of a larger system for the delivery of compressed air to the largest refinery in the region. As a result, they gave less priority to the INES compressed air sub-project. In addition, not all of the potential users were enthusiastic about the INES sub-project, although they did not reject participation completely. Another compressed air supplier, however, learned about this project. This company was able to start a new project by building the trust required for the exchange of knowledge with four other firms and by reducing the scale of the investment needed for the installation. The supplier invested in the installation and the pipelines, and now runs the process, maintains the system and is responsible for a continuous supply. This central installation for four companies has been in operation since January 2000.

Preliminary results show savings of 20% in both costs and energy, and a reduction of CO_2 emissions (as a result of the reduction in energy use) of 4,150 metric tons each year. In 2002 another three plants and in 2003 seven plants more, joined that system. This construction provided new business opportunities for the utility provider. They designed a new utility infrastructure for compressed air and nitrogen for 10 companies in the Delfzijl industrial park in the north of the Netherlands (aluminum, chemical and metal-working companies) that opened under the management of the utility provider in 2004 [21].

It can be concluded that the industrial ecology concept is increasingly becoming widely accepted. Also, institutionalization – as with the initiation of a scientific Journal on Industrial Ecology in 1997 and the start of the International Society on Industrial Ecology in 2001 – draws attention to the issue of industrial ecology. The complex system of eco-industrial parks involving different companies and actors (including their different activities and targets) that is required for the existence of industrial ecology in a region is an important, but time-consuming variable. In the Netherlands, several local authorities were encouraged to set up successful eco-industrial parks through a deliberate policy-making process; the consulting firms involved developed various planning methods with several functions. However, the vision of sustainability was scarcely explicitly defined, the categories *symbiosis* and *utility sharing* were not sufficiently considered, the companies were not sufficiently involved in the development process, and the steering instruments could only enforce options with a limited environmental benefit [3].

Considering the practical experiences of the introduction and dissemination of cleaner production and industrial ecology from a systemic perspective, the concepts are addressing material and energy streams as they result from human activities. These activities do not occur in a vacuum, they are embedded, *i.e.*, they are shaped by the context in which they occur. The following five dimensions can be described [21]:

11.3.1 Cognitive Embeddedness

The manner in which individuals and organizations collect and use information, the cognitive maps they employ in making sense of their environment, the mental disposition of individuals. Themes that can be derived from this are:

Bounded rationality: following economic approaches, we often assume individuals and organizations to behave according to a rational actor model. A more realistic view is that action is that rationality is bounded, in the sense that individuals and organizations have limited capacities for information processing and decision-making. It has consequences for our ability to deal with complex, multi-value problems such as sustainable development. In the cleaner production and industrial ecology concepts, boundaries of departments, hierarchical decision-making, and between companies have to be faced.

Systems thinking: individuals have different strategies for problem solving. Some of these are more suited to systemic problems than others. It is difficult and often neglected to what extent such strategies can be identified in participants in cleaner production and industrial ecology initiatives.

Characteristics of change agents: cleaner production and industrial ecology deal with social change processes. Individuals that act as change agents within or between organizations have special backgrounds and capabilities [23]. The knowledge about the ways in which these characteristics emerge, and how they can be successfully employed within cleaner production and industrial ecology networks, is still limited.

11.3.2 Cultural Embeddedness

This dimension addresses the influence of collective norms and values in guiding economic behavior, such as the shaping of preferences, and the influence of ideologies in shaping future visions. A tendency to externalize normative issues, or to take normative positions for granted, both in our scientific activities and in the subject matter s often experienced. Referring to the latter, some interesting topics are:

Collective cognitive maps: social groups (industrial sectors, regions, national societies, product chains) tend to develop a collective view on the world and ways in which problem should be addressed (both cleaner production as well as industrial ecology itself are such a map). This narrows the search for innovations and solutions for social and ecological problems with respect to the development of maps, and how do they restrain or enhance the development of cleaner production and industrial ecology. Although the concept of industrial ecology was new in the area, the traditional waste exchange results in the INES project 1994–1997 were disappointing in the view of the researchers [3].

Industrial systems fulfil and help define consumer preferences. These preferences are to a great extent culturally determined. How preferences have developed over time, and in what ways has industry influenced them to increase material consumption, is another issue for further research in the 21st century.

Defining what is *legitimate*; the definition of what is acceptable industrial behavior is a social construction, as is the definition of what constitutes acceptable government intervention in industrial activities. This helps to explain why legitimate behavior differs from country to country. Consequently, it is difficult to copy successful practices of cleaner production and industrial ecology from one country (or even region) to another.

Defining what sustainable, cultural embeddedness is directly implies that sustainability cannot be defined objectively. The major consequence of this is that it needs to be defined in local contexts. What are processes to do so, and what mechanisms make existing definitions difficult to change?

11.3.3 Structural Embeddedness

Structural embeddedness emphasizes the way in which relationships between actors influence their actions. This dimension is the one which has gotten most attention as organizational contribution to the field of cleaner production and industrial ecology. Industrial networks have been analysed [24], and co-ordination mechanisms have been discussed [25]. However, linking these structural features to other dimensions of embeddedness remains a relatively unexplored territory.

11.3.4 Political Embeddedness

Political embeddedness is acknowledging the fact that processes of power influence economic actions. This includes the role of the state in the economic process. The role of power is hardly discussed systematically. This maybe has to do with the fact that it is one of the more difficult concepts of sociology in terms of empirical analysis. Nevertheless, actors are not equally able to influence each other's actions and system outcomes, and this has to be taken into account. In relation to the industry-government relationship the *new institutionalism* paradigm formulated by Jordan and O'Riordan [26] is interesting. They cluster various definitions of *institution* as a conglomerate of types of policy networks, standard operating procedures and barriers to rational decision-making, structures of political power and legitimacy, national policy styles, international regimes, and pre-determined social commitments. This means that many stakeholders influence developments in this conglomerate of positions and approaches on the basis of their power (the ability to get what one wants, usually at the expense of the interests of others [27] and/or status.

State promotion of cleaner production and industrial ecology: Although research indicates the importance of spontaneity and emergence in successful examples of cleaner production and industrial ecology, many governmental actors have sought to promote cleaner production and industrial ecology. For the dissemination of new concepts, this means first that standard operating procedures and other routines [28] have important consequences for decision-making processes regarding cleaner production and industrial ecology – by regulating the access of participants and the patterns of negotiation and consultation. Regulation can entail affecting the participants' allocation of attention, their standards of evaluation, priorities and perceptions, identities, and resources. Secondly, in this process, the individual's motivations and perceptions are determined by their own preferences, but also by the importance of the role given to them by the company ("…where you stand depends upon where you sit…" [29]). Thirdly, standard operating procedures can become reifications into specific ideologies or worldviews within entire departments.

Market power: Relationships between firms are asymmetrical. This has effects in terms of their abilities to start or raise barriers to changes in product chains. In eco-industrial parks it is often observed that certain companies such as electricity works, refineries, chemical and food processing companies are in the core of industrial symbiosis activities.

Exit, voice and loyalty: Industrial actors often have an economic/rational management approach [30] to operational organizations. Their approach determines the economic conditions for environmental projects and outcomes. Their function is described within the system boundary of their organization. Their position (responsibility for decision-making), scope (compliance and mandate), perspective (value of the project or concept), commitment and the authority that the actors draw from this, influence the outcomes and the intensity of changes at the aggregated level of industrial ecology. Contrarily to cleaner production demonstration projects, were employees of different organizational were involved, participants in industrial symbiosis are limited per company. When the environmental awareness that many people have cannot be deployed in the work environment, an external compensation will be sought, for instance through membership of an environmental advocacy organization [31].

11.3.5 Spatial and Temporal Embeddedness

Spatial and temporal embeddedness cover the way in which geographical proximity and time influence economic action. The dimensions of space and time are implicit in many accounts of industrial ecology in peculiar, yet it is believed that they deserve explicit treatment. Physical proximity has been identified as crucial in, for instance, complex forms of learning and the building of trust. Porter [24] points to four issues on the strategic agenda for a breakthrough of cluster management: the choice of location, local commitment, the upgrading of a cluster, and working collectively. Time is important as the

evolution of industrial systems typically involves long time periods [31].

11.4 Industrial Ecology Programs in the Rotterdam Harbor Area

In this section, the perspective of sustainability embeddedness issues will be applied to the Rotterdam Harbor and Industry Complex. The Rotterdam Harbor and Industry Complex (HIC) has been an environmental sanitation area in the period 1968–1998. The regional Environmental Protection Agency and Water Authority regulate all companies in the area. Many, but not all,[2] companies are involved in different covenants,[3] concerning environmental performance targets, such as covenants on the reduction of hydrocarbons, the chloro-fluorocarbon reduction program, the implementation of environmental management systems, and the four-year environmental management plan of a company. The INES project in the Rotterdam harbor industrial area started with the participation of 69 industrial firms in 1994 [25]. The project was initiated by an industrial association Deltalinqs, active in the joint interests of industrial companies in the Europoort/ Botlek harbor area near Rotterdam.

Originally, the Deltalinqs approach to environmental problems was very defensive. Later, a more constructive attitude was developed through the stimulation of environmental management in companies. The development from environmental management systems to sustainability projects can be characterized in four phases in the period 1989–2007.

11.4.1 Phase I: The Development of Environmental Management Systems

Following the national trend of self-regulation, Deltalinqs in 1989 started to develop an approach to promote environmental management systems in 70 member companies. During the period 1991–1994 it stimulated the companies' own responsibility through separate meeting groups for six branches of industry. Facilitated by a consultant, companies exchanged information and experiences on the implementation of environmental management systems. In a co-ordinating group, experiences were exchanged among these groups. This structure was evaluated positively by the participating environmental co-ordinators of the firms. Deltalinqs started to search for funds, which led to the start of the Industrial Ecosystem program (INES project) in 1994.

11.4.2 Phase II: INES Project (1994-1997)

Based on assessments of the resources, products and waste streams of companies 15 industrial ecology projects were defined and pre-feasibility studies were performed. Although the projects had a limited scope in terms of the product chain links and preventive approaches, sharing of utilities was found to be a first possibility for developing alliances within the region. After a complex decision-making process within the INES-project team (consisting of the two university researchers, the Deltalinqs project leader, a consultant, and a company representative) three projects were selected for further development. They were seen as good prospects for development within the INES-framework due to their economic potential, environmental relevance, and company participation potential. The projects were:

- *Joint systems for compressed air:* The use of compressed air systems constituted a significant (7% to 15%) part of electricity use of companies. The companies participating in the pilot project were an air supplier, an organic chemical company, an inorganic chemical company, an aluminum-processing company and a cement company. It was assumed that the companies in the pilot project could achieve the following results in the economic and environmental spheres: the price of compressed air can be lowered by approximately 30% and energy consumption could be reduced by approximately 20%.

[2] An USA multinational corporation perceives the covenant as a risk for unexpected liabilities; they prefer to participate in separate projects of the covenant that are within the management policy of their organization

[3] Voluntary agreements between the government and industry

When the real use of compressed air was measured, it was found that it was much lower than expected (7,000 Nm^3/hr instead of the anticipated 12,000 to 15,000 Nm^3/hr) [33]. Another finding was that the total energy consumption could be reduced in two ways. Firstly, by lowering pressure, preventing or reducing leaks, and by a re-design of the existing pipeline system, companies could save approximately 20%. Secondly, by installing a central supply through a ring pipeline system, companies could save approximately another 20%.

- *Waste water circulation*: The reduction of diffuse sources had high priority for the Water Authority, and was consequently of interest to companies. The project increased the awareness that water management improvement can facilitate a remarkable reduction in water emissions and the use of clean water. The use of the so-called pinch technology[4] showed how it is possible to use a certain water quality at the highest level of need of the company's production process or an industrial ecology cluster of companies. By doing this, re-use of several wastewater streams could result in a 10% reduction of total water use.
- *Bio-sludge reduction system*: The total, annual amount of waste bio-sludge produced by 12 companies was about 57,000 tons, including a 3% dry component of 1,900 tons. The actual logistics and treatment costs were approximately €1,200 per ton of dry component. Due to the implementation of primary waste minimization within the companies, a bio-sludge reduction of between 10% and 20% was expected, which could result in annual savings worth between €250,000 and €500,000.

In this phase, these projects did not result in immediate innovations; the projects mirrored political demands and were to a great extent end-of-pipe oriented. However, they created awareness for efficiency improvements at the company level (waste water cascading, compressed air). In the latter case, this actually decreased the necessary economies of scale for a collaborative system. In at least one case, an identified sub-project was commercialized. This concerned the flaring of natural gas that occurred as a by-product of oil drilling in the Rotterdam harbor. Through the INES project, a contract for utilizing this natural gas was made with a company within one week.

11.4.3 Phase III: INES-Mainport Project (1999-2002)

In 1998, the results from the INES program were evaluated by the Board of Deltalinqs, which took time given their meeting only twice every year [33]. Nevertheless, Deltalinqs used this period to acquire new funding, and thus the insights from the first INES program and the learning process that arose from it, led to a second INES program, called the INES Mainport project 1999–2002.

The INES Main port project was a four-year program focused on initiating and supporting industrial ecology initiatives, coordinated again by Deltalinqs. The INES Main port project took the feasibility studies of the INES 1994–1997 program and focused on the following themes: water, CO_2/energy, utility sharing, rest products/waste management, soil, and logistics. At the same time, a more strategic process was initiated. The project initiated a strategic decision-making platform, in which the following societal actors were involved: Deltalinqs – supervising the projects; representatives from major companies in the area; the Dutch National Industry Association; the Dutch National Ministries of Economic Affairs (EZ), and Environment & Spatial Planning (VROM); Province of Zuid-Holland; Municipal Port Authority; Regional Environmental Agency (DCMR); Regional Water Management Agency (RWS/directory Zuid-Holland); Provincial Environmental Association (MFZH); and the Erasmus University.

[4] The functional specification of the wastewater was researched for re-use at the highest level in production processes.

11.4.4 Phase IV: Inclusion in the Sustainable Rijnmond Program

Starting on 1 January 2003, the industrial ecology programs were included under the label of *Sustainable Enterprises in the Rotterdam Harbor and Industry Complex* (HIC) on the ROM-Rijnmond program.[5] The project (which is to run until 2010) aims to strengthen the Rotterdam harbor and industrial area as international gateway and to improve the living quality of the residential areas by integrating the environment in the physical planning of the Rijnmond region. This project, which includes a strategic discussion platform made up of relevant stakeholders, was intended to be part of the driving mechanisms towards a sustainable region. In 2003, it presented its 45 page vision document, [35] based on the concept of transitions, a then emerging theme in the national environmental policy agenda. The vision was summarized in the following statement:

> *"A world striving towards lowering carbon-intensity of the economy provides an attractive perspective for industrial centres that are able to process carbon related streams in a highly efficient, clean, and sustainable way. Rotterdam harbor is ideally suited to be such a centre. It has the ambition to be in 2020 the preferred location in Europe for the haulage and processing of carbon-related fuels and raw materials. It can only make this ambition a reality by being a trendsetter in economically feasible reductions of CO_2 emissions related to these activities, and by acting as a field of experimentation for innovations on themes such as clean fossil fuels, clean energy carriers such as hydrogen, syngas, heat, electricity and biomass as a gateway to a carbon-extensive future."*

The program runs for the period 2003-2010 and is led up by a small ROM Rijnmond staff bureau of a strategic platform that involves representatives of the Ministries of Economics and Environment, the province of Zuid-Holland, the Development Board of Rotterdam, the Port Authority, the industry association Deltalinqs, a plant manager, the Sustainable Mobility Program manager, representatives of the Universities of Delft and Rotterdam, and the representative of an environmental advocacy organization. Thanks to the historical development within several programs the strategic platform could build on the built-up trust between the members of the different organizations and the conditions for successful projects that earlier failed.

A long-term vision *To C or not to* C [35] was developed and established in 2003. The conclusion was that Rotterdam port activities were heavily based on fossil carbon energy sources such as oil and gas. Because of both climate change, dependency on fossil energy sources in political and ecological sensitive regions, as well as the development of new technologies for less or non-fossil carbon based energy supply, the vision is that the Rotterdam Energy Port should anticipate these developments by stimulating innovation, the development of new markets and a transition path towards a sustainable region on the basis of renewable energy, mobility and physical planning. The strategic platform functions as stimulator and *sustainability conscience* of all involved stakeholders in these Rotterdam Energy Port developments. The members of the strategic platform also share the reflective learning processes from projects within and around their own organizations as a basis for the construction of the *ecological concept learning and innovation* transition model of Figure 11.3.

Within this context a large project of the application of the rest heat (in total 2,200 MW in the area) was kept under study, under the condition that coupling the rest industrial heat of Shell Pernis (and later of Esso/Exxon and BP) to the Rotterdam city district heating system should be economically viable and that the responsibility for the coupling between industry and city should be organized clearly. In 2002, the Rotterdam municipality

[5] The ROM-Rijnmond programme (Physical Planning and Environment in the Rijnmond area) is based on a policy covenant signed by all the government bodies and industry in the Rijnmond area on 9 December 1993.

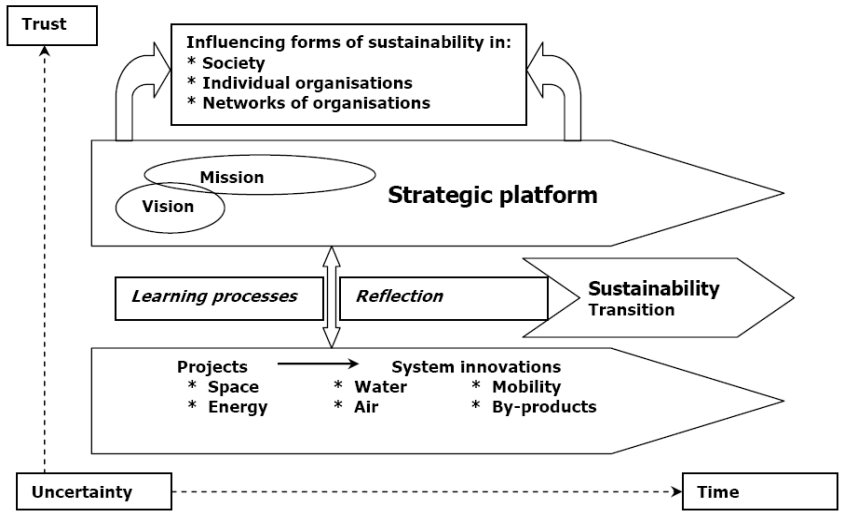


Figure 11.3. Reflective learning in the transition from projects to sustainability system innovations

decided to provide a guarantee for the extra funds that had to be invested in a heating system with temporary equipment in a new residential area nearby the Shell industrial site in Pernis. When all conditions for realization were finally met in 2004 (including liberalization of the Dutch energy market, and reductions of CO_2 demanded by the national government), the coupling of the 6 MW of Shell's rest industrial heat with the city's district heating system would make the temporary equipment redundant; 3,000 houses started to benefit in the Hoogvliet residential area in 2007. The heat supply system will be extended to 100 MW for the application to 50,000 houses[6] [36]. The feasibility study *Grand Design Project* [37] has analyzed that 900 MW can be applied for the heating of 500,000 houses in 2020.

In addition to the planned projects it is experienced that other initiatives are taken. The knowledge of the feasibility study of the compressed air project (see Section 11.4.2) stimulated another company to start compressed air delivery in a joint pipeline system. The air supplier started with the delivery of compressed air to four companies in 2000. Preliminary results showed savings of 20% in both costs and energy, and a reduction of CO_2 emissions (as a result of the reduction in energy use) of 4,150 metric tons each year. In 2002 another three plants, in 2003 seven plants more, and in 2005 three joined that system. [3]. This construction provided new business opportunities for the utility provider.

They designed a new utility infrastructure for compressed air and nitrogen for 10 companies in the Delfzijl industrial park in the north of the Netherlands (aluminum, chemical and metal-working companies) that opened under the management of the utility provider in 2004 [37].

On the basis of sensitivity for the concepts two young professionals at the Rotterdam Port Authority started a private initiative. Their exploration of industrial ecology possibilities resulted in the most well-known industrial symbiosis project in the Rotterdam harbor area. They started the production of fresh king-size shrimps in the *Happy Shrimp Farm* [39], constructed on the basis of rest heat and CO_2 delivery in February 2007.

[6] This is the part of the Hoogvliet/Rotterdam South river border delivery.

11.5 Lessons Learned on the Introduction and Dissemination of Cleaner Production and Industrial Ecology

The cleaner production and industrial ecology concepts are faced with business economics routines of the general *rule of thumb* approach that environmental investments should show a pay back of the investment within a maximum of three years. Although the concepts are being promoted as the *common good* for the economy and ecology of organizations and describe the relationship between the costs of environmental protection and the efficiency of the production process as a *win-win* concept, this usually triggers an *environment* perspective instead of the intended *innovation* perspective.

At the level of single-loop learning, incremental steps such as good housekeeping and regional efficiency improvements have gained credibility as part of these new concepts. In order for radical breakthroughs to sustainability to occur, the approach needs to be different. Continuous learning processes play an important role in this approach, see Table 11.1.

Various experiences demonstrate clearly that the *cleaner production concepts need a broader approach in order to be accepted*: cleaner production involved a radical new perspective, but progress within organizations and their surroundings only took place in small, incremental steps. From this it is clear that various levels of management and the crucial professional educational backgrounds in organizations have different "personal and social clocks" as regards the recognition, acknowledgement and acceptance of new approaches.

At the level of the subject boundary the question can be raised as to whether cleaner production is limited to a system's perspective. As an analogy, the example of a car can be used: one can study the development of cleaner cars, but this does not say much about the sustainability of transportation systems in general. This does not mean that cleaner production concepts are irrelevant, but in a sustainability hierarchy, a holistic approach such as a *cleaner production system* is needed. On the one hand, one can debate whether this is a radical technological process change or a product change; at least it is a breakthrough concerning material substitution, a change that may play a longer term catalytic role. On the other hand, one can debate whether there are ups and downs in continuous improvement. That is to say that continuous improvement is not a straight-line evolutionary process and that sometimes companies seem to move backwards.

The industrial ecology concept is becoming increasingly becoming widely accepted. It is obvious that the Kalundborg Industrial Symbiosis experience is used as the main example worldwide. In the Kalundborg industrial area, [18] company managers developed bilateral links for the shared use of waste and energy; these agreements evolved over several decades. They performed this intentionally in an open economic system of modification and survival. One can say, without labeling this with the metaphor of an industrial ecosystem, that they mimicked elements of the ecosystem. Once environmental problems had been thrust upon the political agenda, it was realized at

Table 11.1. Cleaner production application as result of the type of cleaner production learning processes and their elaboration in organizational change

Learning process	Organizational change: Incremental change	Organizational change: Radical change
One-loop learning process	Cleaner production assessment in demonstration project	Cleaner production innovation
Continuous learning process	Cleaner production assessment implementation and continuous improvement	Cleaner production re-designing

Table 11.2. Industrial ecology application as result of the type of industrial ecology learning processes and their elaboration in organizational change

Learning process	Organizational change: Incremental change	Organizational change: Radical change
One-loop intervention: single lesson given from outside	Industrial ecology assessment in demonstration projects	Industrial ecology innovation
Continuous intervention: learning within a region, as a routine	Industrial ecology implementation	Industrial ecology re-design

one point that all the different links can be labeled an industrial symbiosis, for which Kalundborg is now world famous. However, the human activity system cannot fully mimic an eco-system, because one has to take into account the fact that the various actors in the system have targets and intentions that may not be known to each other. Those targets and intentions can be conflicting and without any knowledge of this, the foundations of an industrial ecology system can be weak from the start. If industrial ecology is viewed as a process, this is the first phase to elaborate. The further dimensions of this type of change can also be applied in the industrial ecology concept, as portrayed in Table 11.2.

In relation to industrial ecology, a similar development can be observed. Despite the fact that industrial ecology is perceived as a normal business practice (waste exchange and energy sharing), the industrial ecology assessments in demonstration projects generated mainly first order changes of knowledge about the concept.

However, the implementation of that knowledge in practice is time-consuming and difficult, and only a few incremental first order changes are usually made. Often the concept is found to be attractive but its operationalization is strongly path-dependent on the originator of the plan. Also, until now, the industrial ecology concept has had a strong engineering focus. The social conditions and organization of the concept have scarcely been explored.

The lack of awareness about and the utilisation of the concepts of change management within both cleaner production and industrial ecology assessments lead most of the assessments to be limited technical approaches that usually do not include the social and psychological dimensions of organisational change. Existing experience and implicit knowledge are almost never utilised in the process of exploration and development of the new cleaner production and industrial ecology pathways. The question is whether industrial ecology on a longer time frame will be an essential part of the sustainability system. The number of companies, their diversity in size and type, and the intensity of their interactions are major variables in the system. Here the links between individual companies and the links between companies and society are to be tested according to the criteria of sustainability. This system demands a holistic approach based on new world views. The production process is an element at the level of individual companies (at the micro level) but the output of by-products is also the function of the *servant of the network* [40] at the meso level (Table 11.3).

The interconnectedness of cleaner production and industrial ecology to sustainable regional development can be linked to regional education and innovation institutes. Also, new employment for the region and informational, social and cultural contributions complete the holistic worldview at the macro level (Table 11.4).

In this triple bottom line approach, government agencies and relations between companies and regulating agencies must also be changed. The integration of environmental management within companies means more self-regulatory responsibility for the companies and as a result, important changes have to take place in the relations between industry and regulatory agencies. Regional learning that involves multi-loop learning processes within and among organizations is

Table 11.3. The type of concept and the involvement of actors and the main characteristics of focus and perspective in business management

Concept / Issue	End-of-pipe technology	Cleaner production	Industrial ecology	Sustainability
Actors	Environmental co-ordinators; Environmental technology specialists	Environmental managers; Plant managers	Eco-industrial park management; Plant managers; Physical planners	CEO; Division Managers; Plant managers
Focus	Pollution control	Pollution prevention	Pollution prevention, Recycling and Utility sharing	Production for needs in balance with socio-economical and eco-system
Perspective	Waste	Production process, Products, Services	Production process, product chain and energy carriers	Re-engineering and innovation of production, products and energy carriers

Table 11.4. The three concepts challenge for sustainability: from weak to strong

Three Concepts Challenge	From WEAK	to STRONG
Cleaner production	*One hit* intervention in EMS	Integration in decision-making
Industrial ecology	Waste exchange	Material flow, logistic & social industrial park management
Sustainable development	Lip service to policy integration; Faint social awareness and little media coverage	*Triple bottom line* performance of all relevant stakeholders

essential. Until now this more integrated approach has scarcely been used in an optimal way anywhere in the world.

11.6 Conclusions and Recommendations

There are many different perceptions of the impact of cleaner production. A simple one is: "The picking of low hanging fruit in new areas and organizations" ("..although it is not as easy a process as is often suggested..") [41]. A more complex one is: "A time consuming process in more advanced phases like business re-engineering or re-structuring" [3].

Because so many actors and organizations are involved, the development of industrial ecosystems is site-specific. An important distinction can be made between existing and new industrial areas. The design of an industrial ecosystem must take into account the characteristics of the local and regional *ecosystem* but its development must also match the resources and needs of the local and regional *economy*. These dual requirements reinforce the need for working in an inquiry mode [19]. In combination with learning processes involving the experiences of other communities, developing industrial ecosystems in an interactive

dialogue with stakeholders is a practical route towards the implementation of sustainability projects in a long-term perspective.

In the life-cycle of dealing with environmental issues, we are for answering the question whether environmental management is needed as an independent concept, beginning to understand that negative impacts on our surroundings are indicators of the inefficiency of industry, due to wastage of materials and energy. So, how can we influence other choices in production, products, services, and logistics in such a way that negative impacts are reduced? In this perspective, can we imagine that the emergence of an advanced clean industry is noticeable? The answers to these questions have evolved to the concepts of *sustainable enterprises* [42] and *corporate social responsibility* [43], [44], and s*ustainable regions and communitie*s [45]. The long-term sustainable development of regions ask for new institutional arrangements and the facilitation of initiatives such as organizational research, information, conferences, think tanks, vocational training providers, specialized training and general education [46].

It is recommended that in order to make more effective progress with cleaner production and industrial ecology in the future, the following should be done:

1. All cleaner production efforts, in the case of application in the design, start-up and growth life-cycle phase need to be made with a comprehensive organizational support and involvement and should also include the stakeholders throughout the life-cycle of the products and services that the organization provides to society.
2. Multi-loop learning processes should be used both within single companies and between clusters of companies. This should also increasingly involve the wider citizen population in sustainable regional development planning and implementation.
3. Cleaner production and industrial ecology concepts and approaches should be integrated vertically and horizontally from the policy and strategic levels down to the detailed operational levels of both individual companies and clusters of companies.
4. The implementation of industrial ecology should be integrated within the regional economy, ecology, technology, culture, and sustainability plans of the region.
5. Trust, transparency and confidence must be developed through an open, reflective and on-going dialogue designed to ensure real involvement of diverse stakeholders in charting the future of their organizations and regions as part of the transition to sustainable societies.
6. On the basis of cleaner production and industrial ecology and conditions of trust, transparency and confidence, the concepts of sustainable enterprises and communities can integrate all social, economic, environmental and cultural dimensions.

In stimulating and facilitating the above recommendations several partnerships create added value:

At the macro level, international policies and agreements, such the United Nations Millennium Declaration, Clean Development Mechanisms, Global Environmental Forum, Environmental Sound Technologies, and Human Development through Markets, must be integrated in an economic, ecological and social regional framework.

At the meso level, municipalities, industry associations, and education institutes/knowledge centers can join in integrated public private partnerships to generate and facilitate sustainability programs. The local situation provides the context whether it be government-driven, such as is the case in several Asian countries for eco-industrial park development, or voluntary partnership-driven. Also regional approaches for cleaner production in partnerships in developing countries can have a broad scope [47].

At the micro level, various disciplinary approaches such as industrial (eco) design, environmental management accounting and sustainable banking must be integrated.

Overall, the emerging education initiatives for initial Master's courses on sustainability subjects

must be strongly stimulated. Where UNESCO initiated the UN Decade on Sustainability in Higher Education 2005–2014, [48] the concepts of cleaner production, industrial ecology and sustainability can be educated within a cleaner production systems approach.

All together, the ecological, economic, social and cultural dimensions of nations and corporate activities are best combined in the label *nations and corporations taking their responsibility for working towards social, economic, environmental and cultural sustainability*.

References

[1] Baas L, Hofman H, Huisingh D, Huisingh J, Koppert P, Neumann F. Protection of the North Sea: Time for clean production. Erasmus Centre for Environmental Studies 11, Rotterdam 1990.

[2] Frosch RA, Gallopoulos NE. Strategies for manufacturing. In: Managing planet earth. Scientific American Special Issue, September 1989; 144–152.

[3] Baas L. Cleaner production and industrial ecology; dynamic aspects of the introduction and dissemination of new concepts in industrial practice. Eburon, Delft, 2005

[4] Creating Solutions for Industry, Environment & Development. UNEP, 9th International Conference on Sustainable Consumption and Production. Arusha, Tanzania 2006; 10–12 December.

[5] Mandler JM. Stories, scripts and scenes: aspects of social theory. Lawrence Erlbaum Associates Publishers, Hillsdale NJ, 1984.

[6] World Summit of Sustainable Development. Johannesburg Declaration on Sustainable Development Johannesburg 2004; Sept. 4

[7] UN General Assembly United Nations Millennium Declaration. UN 8th Plenary meeting 55/2. New York 2000; Sept. 8.

[8] UNIDO Cleaner Production Expert Group Meeting. Baden, Austria 2006; October 29–31.

[9] UNEP/Wuppertal Institute Collaborating Centre on Sustainable Consumption and Production, and UNEP. Creating solutions for industry, Environment & Development 9th International Conference on Sustainable Consumption and Production. Background Paper. Arusha, Tanzania 10–12 December, 2006.

[10] UN-Habitat Responding to the challenges of an urbanizing world. Annual report. Nairobi, 2005.

[11] Tukker A, Jansen B. Environmental impacts of products: A detailed review of studies. Journal of Industrial Ecology 2006; 10(3): 159–182.

[12] Billsberry J. There is nothing so practical as a good theory: how can theory help managers become more effective. In: Billsberry J, editor. The effective manager: Perspectives and illustrations. Sage, London, 1996; 1–27.

[13] Bateson G. Steps to an ecology of mind. Ballentine Books, New York, 1972.

[14] Snell R, Chak AMK. The learning organization: Learning and empowerment for whom? Management Learning 1998; 29(3):337–364.

[15] Vickers I, Cordey-Hayes M. cleaner production and organizational learning. Technology Analysis & Strategic Management 1999; 11(1):75–94.

[16] Dodgson M. Organizations learning: a review of some literatures. Organization Studies 1993; 14(3):146–147.

[17] Richards DJ, Fullerton AB (editor). Industrial ecology: U.S.-Japan perspectives. Report on the U.S.-Japan Workshop on Industrial Ecology. March 1–3, 1993, Irvine CA. National Academy of Engineering, Washington D.C, 1994

[18] Gertler N. Industrial ecosystems: Developing sustainable industrial structures. Master's thesis MIT, MA, 1995

[19] Christensen J. Kalundborg Industrial symbiosis in Denmark. Proceedings Industrial Ecology Workshop; Making business more competitive. Ministry of Environment, Toronto 1994.

[20] Lowe EA, Moran SR, Holmes DB (eds.). Fieldbook for the development of eco-industrial parks. Indigo Development, Oakland, 1996

[21] Voermans F. Delfzijl krijgt persluchtnet (Delfzijl starts a compressed air network). Petrochem 2004; June, 6(22).

[22] Baas L, Boons F. Industrial symbiosis in a social science perspective. Discussion proposal for the 3rd Industrial Symbiosis Research Symposium. Birmingham (GB) 2006; 5–6 August.

[23] Vliet F van. De Change Agent en zijn Resources; Een modelmatige benadering van regionale technologische veranderingsprocessen (The change agent and his resources; a model approach of regional technological change processes. Delft, Ph.D. thesis (in Dutch), 1998.

[24] Porter ME. Clusters and the new economics of competition. Harvard Business Review November 1998; December: 77–90.

[25] Boons FAA, Baas LW. The organization of industrial ecology: the importance of co-ordination. Journal of Cleaner Production 1997; 5(1-2):79–86.

[26] Jordan A, O'Riordan T. Institutional adaptation to global environmental change (II): core elements of an `institutional' theory. CSERGE Working Paper GEC 95-21 Norwich/London 1995.
[27] Lukes S. Power: a radical view. Studies in Sociology, London 1974.
[28] Saunders P. They make the rules: Political change and learning. Westview Press, Boulder, 1976.
[29] Allison GT. The essence of decision: Exploring the cuban missile crisis. Harper Collins Publishers, Boston, 1971.
[30] Burrell G, Morgan G. Sociological paradigms and organizational analysis. Ashgate Publishing, Brookfield, 1979.
[31] Baas L. Woorden en Daden; Evaluatierapport INES Mainport Project 1999–2002. (Words and actions; Evaluation report of the Mainport Project 1999-2002). Erasmus Universiteit, Rotterdam, 2002; Dec.
[32] Baas L, Boons F. the introduction and dissemination of the industrial symbiosis projects in the Rotterdam Harbour and industry complex. International Journal on Environmental Technology and Management 2007; 7(1):1–28.
[33] Silvester S. Air-sharing, End report INES project phase 3a. Erasmus Studiecentrum voor Milieukunde, Rotterdam, 1997; 24 January.
[34] Baas L Developing an industrial ecosystem in Rotterdam: Learning by … what? Journal of Industrial Ecology 2001; 4(2):4–6.
[35] ROM-Rijnmond. To C or not to C. Rotterdam 2003.
[36] ROM_Rijnmond. Rijnmondse Routes. Rotterdam 2005.
[37] ROM Rijnmond R3. Grand Design; Warmte voor Zuidvleugel Randstad (Heat for the Southern part of Zuid-Holland). Rotterdam 2006; February.
[38] Voermans F. Delfzijl krijgt persluchtnet (Delfzijl starts a compressed air network). Petrochem 2004; 6(22).
[39] Greiner B, Curtessi G. The happy shrimp farm. Rotterdam 2005; Oct.
[40] Wallner HP. Towards sustainable development of industry: networking, complexity and eco-clusters. Journal of Cleaner Production 1999; 7(1):49–58.
[41] Dieleman H. De arena van schonere productie; mens en organisatie tussen behoud en verandering (The Arena of cleaner production; mankind and organization between conservation and change). Ph.D. thesis Erasmus Universiteit Rotterdam, 1999.
[42] Cramer J. Ondernemen met hoofd en hart; duurzaam ondernemen: praktijkervaringen (Enterpreneurship with head and heart; sustainable enterprises: experiences in practice). Van Gorcum, Assen, 2002.
[43] Cramer J. Learning about corporate social responsibility – The Dutch experience. IOS Press, Amsterdam, 2003.
[44] Werther WB, Chandler D. Strategic corporate responsibility: Stakeholders and global environment. Sage Publications Inc., Thousand Oaks, 2005.
[45] Corbett MN, Corbett J. Designing sustainable communities: Learning from village homes. Island Press, Washington DC/Covelo, 2000.
[46] Hart M. Guide to sustainable community indicators. Hart Environmental Data, North Andover, MA, 1999.
[47] Mbembela PJK. Managing environmentally harmful economic activities in informal settlements: The case of the Dar es Salaam City – Tanzania. IHS Master Thesis Rotterdam, 2006.
[48] UNESCO. The UN decade for education for sustainable development 2005-2014. http://portal.unesco.org/education/en/ev Accessed 12 December, 2005.

12

Quality Engineering and Management

Krishna B. Misra

RAMS Consultants, Jaipur, India

Abstract: All production processes employ materials, men and machines. Each of these elements has some *inherent variability* in addition to *attributable variability*, which can be controlled to an irreducible economic minimum. The subject of quality engineering and management is about reducing the variablity in products and processes, quality costs and to provide maximum satisfaction to the customers through improved product performance. The subject has grown considerably since 1930, when Shewhart first developed his statistical approach to quality. Several developments that have taken place since then are presented in this chapter along with quality planning, control, assurance and improvement, which form the backbone of any quality program.

12.1 Introduction

Quality is a world wide concern of manufacturers. However, the word quality has had different connotations when used by different people. The definition has also undergone changes and its meaning has been extended over time but it can be definitely called an attribute that is generally used to reflect the degree of perfection in manufacturing of a product. It is easy to realize that this degree of perfection is inversely proportional to the variability present in the process. All manufacturing processes involve materials, men and machines and they all have some element of *inherent variability* in addition to *attributable variability*, which can be controlled to an irreducible economic minimum. Reducing variability in production is synonymous with improving the quality of the product.

The reason for material variation can be traced to inadequate care taken in the purchase of material (quality assurance), or on account of poor material specifications or due to urgency of purchase compromising the quality specifications, *etc*.

The source of variation due to machines is the natural limits of capability that every process has, which is also known as *process/machine capability,* and any attempt to reduce this range would cost heavily in terms of money. If the process is incapable of acceptable operation within design limits, then we have the option of separating nonconforming from conforming products, using more precise process or change in the design of the product or system in order to achieve an optimum design at minimum total cost.

The third source of variation is man himself and this is the most important contributor to variability. In fact, man's decisions or actions directly influence the extent of variability to a very large extent.

It is not difficult to realize that quality is inversely proportional to the variability, and one must try to reduce all sources of variability if quality is to be improved.

12.1.2 Definition

The most widely accepted definition of quality is: quality of a product is a measure of the degree of conformance to applicable design specification and workmanship standards. Obviously, this definition concerns itself with the manufacturing phase of a product. Several other definitions of quality have been put forward by several eminent practitioners but the central concept remains the same: the quality of a product is considered satisfactory if the product is able to satisfy the requirements of the consumer. Alternatively, it is an attribute of a product, which if incorporated into a product meant for a specific purpose or use, will satisfy a consumer. However, it is definitely agreed that bad quality affects reliability because inferior workmanship is likely to shorten the life of a product and thus its reliability. Earlier, in western management ensuring quality was left to the quality inspectors. However, it was Deming's work using statistical tools and scientific management philosophies in Japan that gave quality effort an impetus, importance and respectability, it has been acquired over time and quality tends to become all pervasive. Deming's 14 points for management provided the roadmap for quality movement in Japan and elsewhere.

There are others, mostly engineers, who do not quite agree with statisticians and have the notion that it is an engineering design effort, by which the performance of a product can be increased. They may as well be called as proponents of reliability and see quality as a necessary but not sufficient characteristic. There are others (mostly statisticians) who consider reliability effort as a part of the quality program. We will discuss the difference in the definitions of quality and reliability a little later in this paper, but it can be said with certainty that quality professionals themselves have struggled with the definition of quality for quite some time.

Crosby [1] defines quality as conformance to requirements or specifications. Juran [2] provides a simple-looking definition of quality as the fitness for use.

Deming [3] defined two different types of quality, *viz.*, *quality of conformance* and *quality of performance*. Quality of conformance is the extent to which a firm and its suppliers surpass the design specifications required to meet the customer's need. Sometimes, another aspect of quality is added to the definition of quality, *i.e.,* quality of design, which implies that the product must be designed to meet at least the minimal needs of a consumer. *Quality function deployment* is a system of product design based on customer demands with participation from all concerned. The quality of design has an impact on the quality of conformance, since one must be able to produce what was designed.

Quality of performance, on the other hand, is a measure, arrived at through the research and sales/service call analysis, in assessing how well a product has performed when put to use. It signifies the degree to which the product satisfies the customer or the user. This measure, incidentally, is synonymous with the concept of reliability and leads to redesign, new specifications, and to a product improvement program on a continuous basis for any manufacturing concern through interaction with the user or the customer.

Feigenbaum [4] defines quality as: the total composite product and service characteristics of marketing, engineering, manufacture, and maintenance through which the product and service in use will meet the expectations of the customers.

Taguchi [5] defines quality as the loss imparted to the society from the time a product is shipped. He also divides quality control effort into two categories; online and off-line quality control. On-line involves diagnosis and adjustment of the process, forecasting and correction of problems, inspection and disposition of product and follow up on defective shipped to the customer. The off-line quality control is quality and cost control activities carried out at the product and process design stages during the product development cycle. Taguchi's concept of quality, relates to determining the ideal target values (parameter design) and evaluating losses due to variation from the target value. Thus the objective of a quality program is to minimize

total losses to the society, which means both the producer and the consumer.

Therefore, it is not without confusion that one may want to settle for a practical definition of quality. However, whatever definition of quality one might settle for, no one can deny that to ensure the basic objective of high quality, a designer must be able to translate the needs of the consumer into an engineering design, including specifications and tolerances; the production engineer must be able to design a production process that will produce the product meeting these specifications and tolerances; of course while ensuring minimum waste, emissions or pollution of the environment.

12.1.3 Quality and Reliability

Obviously, the widely accepted definition of quality did not concern itself with the element of time and could not say whether a product would retain its quality over a period of time nor did it mention the product's performance under a set of given conditions of use or environment. Neither of these elements form a part of quality but are inherent in the definition of reliability, which is defined as the ability that a product will perform a specified function over a specified time without failure under the specified conditions of use. One proceeds to eliminate or minimize the failures during the product's mission time and their causes and to improve upon the design [6]. Moreover, quality definition does not make itself expressible in terms of a probability figure, which reliability does. However, the quality of performance comes closest to the definition of reliability as far as satisfying the user's requirement is concerned and the concept of quality of design can help build reliability at the design stage. However, whether reliability is a part of the quality effort or whether quality is reliability during the manufacturing phase is a question over which statisticians and engineers often differ.

12.2 Quality Control

Quality control (QC) is the most important activity during manufacturing and aims to provide and maintain a desired level of quality of a product. In fact, QC is the name given to a set of techniques and means [7]: used to manage, monitor, and control all those steps that are necessary in production of a product of desired quality.

Juran [2] provides the definition of control as "The process of measuring quality performance, comparing it requirements, and acting on difference". Feigenbaum [4] defines control as a "process for delegating responsibility and authority for a management activity while retaining the means of assuring satisfactory results". This definition is sufficiently generic to apply to any activity, which may include products or services, and involves four steps of control, *viz.*,

- setting standards
- appraising conformance
- acting when necessary
- planning for improvements

The activities that need control include workmanship, manufacturing processes, materials, storage and issue of parts and materials, engineering design changes and deviations, production and incoming material inspection and tests, vendor control and many related activities. The most important concern in quality control is workmanship, which can be achieved by good manufacturing methods and techniques, and through inspection of manufactured product. If performed during the manufacturing the inspection is called an *in-process* inspection and if it is performed on finished product is called the *final inspection.*

Off-line Quality Control

The procedures involved in off-line quality control deal with measures to select parameters of product and processes in such a way that the deviation between the product or process output and the standard is minimized. This is mainly achieved through product and process design in which the goal is to produce a design within the constraints of resources and environmental parameters.

Experimental design is an important tool for improving the performance of a manufacturing process in the early stage of process development as this can result in improved process yield reduced

variability and closer conformance to target requirement reduced development time and thereby in reduced overall costs. The principles of design of experiments and the Taguchi method [7] help to come up with off-line process control procedures. Chapter 17 of this handbook on robust engineering deals with a certain aspect of the problem and illustrates it through an example.

On-line Quality Control

Instead of taking off-line quality control measures, it may be necessary to take online quality measures to correct the situation. When the output differs from a specified norm, the corrective action is taken in the operational mode on a real time basis for quality control problems. In fact, this forms the basis of online statistical process control methods. The most effective method of controlling the process is the most economic and positive method. It is for this reason that quality control engineers use control charts, as it is always better to control the method of doing things while the process is being performed, than to correct things after the job has been done. Since most processes are dependant on men and machines, inspection becomes a necessity to ensure that the product made is good. Quality control also concerns new design, control and change of specifications. Since QC affects the performance of a product over its lifetime, QC must be stringently implemented.

Classical quality control was achieved by observing important properties of the finished product and accepting/rejecting the finished product. As opposed to this technique, statistical process control uses statistical tools to observe the performance of the production line to predict significant deviations that may result in rejected products.

By using statistical tools, the operator of the production line can judge for himself if a significant change has been made to the production line, by wear and tear or due to other reasons, and even take measures to correct the problem – or even stop production – rather than producing a product outside specifications. The simplest example of such a statistical tool may be the Shewhart control chart.

12.2.1 Chronological Developments

Quality control has evolved constantly during the last century. The period between 1920 and 1940 was called the inspection quality control period by Feigenbaum [4], since the inspectors were designated to check the quality of a product by comparing it with a standard. If discrepancies were noticed, the deficient products were either rejected or reworked. The processes, however, were becoming more and more complex and side by side statistical aspects of quality control were also being developed. Shewhart [8] can be said to have laid down the foundation of using control charts to control the variables of a product. Acceptance sampling plans were developed to replace the 100% inspection and the 1930s saw the extensive use of sampling plans in industries. This gradually laid the foundation of statistical quality control and the period 1940–1960 was called the period of statistical quality control by Feigenbaum [4]. Statistical quality control became further popularized when W. Edwards Deming visited Japan in 1950 and taught Japanese industries the principles of SQC. Japanese were quick to embrace this new discipline and proved that a competitive edge can be achieved in the world market through SQC. J.M. Juran further helped strengthen Japanese management's belief in quality programs when he visited Japan in 1954. Later, in 1980, he wrote his excellent text [2]. The next phase of *total quality control* started in the 1960s. The concept of *zero defects* was spawned during this period when the Martin Company of Orlando delivered a Pershing missile to Cape Canaveral with zero nonconformity. As the people started getting round the idea of the involvement of shop floor workers in the quality improvement programs, the impetus for TQC got a boost. Organizing *quality circles* in industries, an idea that originated in Japan, was keenly pursued the world over during this period. The next phase of implementation of total quality control started in the 1970s, beginning with the concept of involving everyone in the company right from top management to workers in the quality program; this laid the foundation of the concept of the *total quality system* pursued vigorously during 1980s. Taguchi [5, 9] introduced

the concept of parameter and tolerance design and indicated the use of experimental design as a valuable quality improvement tool. Management saw the need and importance of giving training programs in statistical quality control to all levels of workers in the industry. Terms and concepts like quality management system (QMS), total quality management (TQM), total engineering quality management, product life-cycle management, Six Sigma, and ISO 9000 to promote quality consciousness and development of a distinct quality culture flourished between 1980 and the present. Around 2001, the concept of product life-cycle management (PLM) came into being; this is a holistic business activity addressing many things such as products throughout their life-cycles from cradle to grave, organizational structure, working methods, processes, people, information structures, and information systems.

12.2.2 Statistical Quality Control

The quality of a product can be assessed using the performance characteristics. Performance characteristics of a product are the primary quality characteristics that determine the product's performance in satisfying the customer's requirements. Performance variation can be best evaluated when a performance characteristic is measured on a continuous scale. The characteristics having randomness can be represented by statistical distributions. The quality of the product is defined using a target value, and upper and lower specification limits for each characteristic. We can compare the statistical distribution of each characteristic to decide whether the product should be accepted or rejected. This is called *statistical quality control* (SQC). As we have seen earlier, there are mainly two sources of variations in product characteristics, *viz.,* variability of materials and components and the variability of the production process. Statistical quality control can be applied to identify and control both sources of variability. However when SQC is applied to processes, it is referred to as *statistical process control* (SPC). Here online measurements of product performance characteristics can be made and compared with the specification limits. This will not only inform the operators of the off-specification product but should also identify the sources of variability in the process that need to be eliminated.

12.2.3 Statistical Process Control

Statistical process control (SPC) was pioneered by Walter A. Shewhart [8] and created the basis for control charts. Later on it was pursued by Deming [3], who was instrumental in introducing SPC methods to Japanese industry after World War II. A typical control chart is a graphical display of a quality characteristic that has been measured or computed from a sample versus the sample number or time. The chart contains a center line that represents the average value of the quality characteristic corresponding to the in-control state. Two other horizontal lines, called the upper control limit (UCL) and the lower control limit (LCL) are also drawn. These control limits are chosen so that if the process is in control, nearly all of the sample points will fall between them. As long as the points plot within the control limits, the process is assumed to be in control, and no action is necessary. Shewhart [8] concluded that while every process displays variation, some processes display controlled variation that is natural to the process, while others display uncontrolled variation that is not present in the process causal system at all times. However, a point that plots outside of the control limits on the control chart is interpreted as evidence that the process is out of control, and investigation and corrective action are required to find and eliminate the assignable causes responsible for this behavior. The control points are connected with straight line segments for easy visualization. Even if all the points plot inside the control limits, if they behave in a systematic or nonrandom manner, then this is an indication that the process is out of control.

The underlying assumption in the SPC method is that any production process will produce products whose properties vary slightly from their designed values, even when the production line is running normally, and these variances can be analyzed statistically to control the process. Today, we have a wide variety of control charts [11] for controlling

different quality characteristics. In fact, one can find a discussion of several of these control charts and indexes in [11], and in this handbook, Chapter 14 deals with certain aspects of SPC and discusses some of the control charts and indexes.

12.2.4 Engineering Process Control

Engineering process control is a subject of statistics and engineering that deals with architectures, mechanisms, and algorithms for controlling the output of a specific process. Engineering process control (EPC) is used to control the continuous production processes and is a collection of techniques to manipulate the adjustable variables of the process to keep the output of the process close to the targetted value. This objective is achieved by generating an instantaneous response, opposing the changes to balance a process and take corrective action to bring the output as close to the target as possible. The approach involves forecasting the output deviation from the target that would occur if no control action were taken and then to take action to cancel this deviation. The control is achieved by an appropriate feedback or feedforward control that indicate when and by how much the process should be adjusted to achieve the objective.

In Chapter 15 of this handbook, we shall see how EPC can be applied to control the processes in a product industry.

12.2.5 Total Quality Control

In modern practice, QC begins with the design process and continues through manufacturing and product use. The sum of all these efforts is called *total quality control* (TQC). Quality control, therefore, can also be viewed as an aggregation of all activities directed toward discovering and controlling variations in performance.

According to Feigenbaum [4], TQC encompasses the entire product life-cycle, and involves activities such as:

- marketing
- engineering
- purchasing
- manufacturing engineering
- production
- inspection and tests
- shipping
- installation, maintenance and service

In fact, one can plan for quality during all the above activities, even before the product is produced.

12.3 Quality Planning

Quality planning is at the heart of TQC and is an activity aimed at preventing quality problems; it includes:

- establishing quality objectives
- building quality into the design
- procurement for quality
- control of nonconforming material
- ensuring in-process and finished product quality
- inspection and test planning
- handling and follow-up of customer complaints
- education and training for quality.

Quality guidelines are established by knowing the customer requirements and once these are clearly understood and it is determined that the company policies, procedures, and objectives are in conformity with these requirements, one may proceed to develop an effective quality plan. If necessary, these procedures and objectives can be revised. Comparing the proposed design with the customer requirements, including reliability and maintainability considerations, ensures design quality. A design is finally reviewed for *producibility* and *inspectability* since it is always possible to design a product that satisfies the customer's requirements but cannot be manufactured with the existing technologies. Design quality requires establishing specifications for all important quality characteristics and developing formal product standards. Work instruction and detailed procedures also form a part of this activity.

Inspection and test planning is always integrated with the design and production activities as they

directly influence the quality of the product and involve fixing of inspection points, classification of characteristics according to their criticality, design and procurement of inspection and test equipment, and development of inspection, instructions and test procedures. The material control procedures are often incorporated into the purchase order or a contract.

Sampling [12] rather than inspecting 100% of the manufactured products reduces the cost of inspection and involves making decisions based on the results of limited inspection or tests. However, this is at the cost accepting a risk, usually known as the sampling risk. In fact, there are two types of risks and the first one is known as the product risk, and may result in a good product being incorrectly classified as nonconforming although it is not. The other is known as consumer risk, in which a nonconforming product may be incorrectly classified as conforming. For critical characteristics, there is no acceptable level of consumer risk and it is never sampled except to verify a previous 100% inspection. An exception occurs only when the inspection or test is destructive, where there is no option but to sample. Tests can either be classified as destructive or non-destructive depending upon whether or not they cause damage to the product or raw material. The nondestructive test includes eddy current, dye penetrant, magnetic particles, ultrasonic and X-ray tests, and is often used to check properties of a material or product such as cracks and porosity. The other problem in sampling is to resolve the question of how much to sample. All inspection and test activities involve some degrees of error, since no measuring instrument is perfect. However, there are statistical methods of assessing all kinds of inspection and tests errors. The known size is called a standard, and the process of adjustment of gauges is known as calibration. These form the routine activities of any quality planning.

12.4 Quality Assurance

Quality cannot be the concern of one person or one department, such as quality control department in a manufacturing concern; therefore a system has to be evolved that continually reviews the effectiveness of the quality philosophy of the company. All those who are directly or indirectly connected with the production department must be involved in the task. For example, this group may advise market department about the nature and type of information that may be helpful for the design team based on customer requirements. In fact, the quality assurance (QA) group must audit various departments and assist them to accomplish the company's goal of producing a quality product. The quality assurance department will ensure that means exist in terms of physical resources and manpower within the company to execute the quality plans. If any shortcomings are noticed, the quality assurance group may advise the concerned department to affect those changes. The quality assurance department actually acts as a coordinating agency for the quality needs of a company with respect to the products being manufactured. Thus the formal definition of a quality assurance activity involves all those planned actions necessary to provide confidence to the management and the customer that the product will eventually satisfy the given needs of a customer. Quality control is just a part of the quality assurance task. It is also true that all leading manufacturers depend on several vendors for incoming raw material or components and it will be incumbent on the quality assurance department to assist these vendors in maintaining and controlling the quality of parts supplied by them, since the quality of final product depends heavily on the quality of the parts supplied. In such cases, the quality assurance department's responsibility is also extended to include vendor product quality. In fact, vendors must be considered as partners in the quality program.

QA covers all activities from design, development, production, installation, servicing to documentation. It introduced the sayings "fit for purpose" and "do it right the first time". It includes the regulation of the quality of raw materials, assemblies, products and components, services related to production, and management, production, and inspection processes.

12.5 Quality Improvement

Quality improvement [13] is a continual process in any company and should be the objective of everyone in the company for increasing productivity and cost reduction and thereby increasing profitability. Since improvements are possible through reduction of variability of process and production of nonconforming items, quality improvement is possible by detection and elimination of common causes, in contrast with special causes that can be identified and eliminated through process control. Special causes are those having an identifiable reason, such as tool wear, poor raw material or operator fatigue, but common causes are inherent to the system and are always present, such as variability in characteristics caused by the inherent capability of a machine. Special causes can usually be controlled by an operator but common causes necessarily require the attention of the management.

In fact, there are three stages of the quality improvement program, *viz.*, the commitment stage, the consolidation stage, and finally the maturity stage. In the commitment stage, management accepts to undertake the quality improvement program, and plans and policies are drawn including the organizational structure to implement it. This phase usually concerns itself with identifying and eliminating special causes in the first instance. With the training and education of personnel and support from the management the quality improves and the percentage of nonconformities drops appreciably during this phase. In the consolidation stage, the main objective is to improve the quality of conformance and efforts are made to identify and eliminate common causes by improving process capabilities and investment is made to prevent defects. The causes of all defects must be traced to their origins and adequate measures be taken to prevent them in future. This exercise is likely to minimize the number of items for rework or scrapping, resulting in reduction of total cost. However, the percentage drop of nonconforming items is not as high as in the first stage of implementation. In the maturity stage, the processes are considered to have matured and process parameters are adjusted to create optimal operating conditions and the total cost reduces further as the number of scraps and reworked items reduces, but the rate is slower. The process of improvement continues and the quality improves asymptotically to a zero defect paradigm if the process performance keeps improving. However, one must bear in mind that the quality improvement program pays off only in the long run but the cost of improvement is immediate. This should not detract management or personnel engaged in the improvement program.

12.6 Quality Costs

Quality cost comprises four major components, *viz.*, prevention cost, appraisal cost, internal failure cost and external failure costs. Prevention costs are costs incurred in planning, implementing and maintaining a quality system, which include all the costs of making a product right the first time, such as the development costs of product design, process design and control techniques and salaries. Appraisal costs are the costs of measuring, evaluating and auditing products, components, incoming raw materials to determine the degree of conformance, as well as product inspection and testing and cost of calibration etcat the stage of final acceptance. Internal failure costs are all those costs incurred when products, components, materials fail to meet the quality requirements. These costs also includes the cost of rework, scraps, labour and other overheads associated with nonconformities, including loss of production and revenues. The external failure costs are the costs incurred when the product does not perform satisfactorily after it is delivered to the customer. Warranty and product liability costs are included in this component of the total cost. A quality system in place should reduce the total cost.

12.7 Quality Management System

A quality management system (QMS) is achieved by having an organizational structure, resources, procedure and programs, and processes to implement quality management. The major

objective of QMS is to integrate all processes and functional units to meet the quality goal of a company. Planning is absolutely necessary for the success of a quality program. A strategic plan must be clearly defined. Quality policy and procedural manuals help in guiding the entire quality activity. An organizational structure should be created to establish a line of authority and responsibility.

Several companies are developing their quality systems to:

- reduce the first time failure,
- reduce the costs of customer claims,
- get things right the first time,
- improve service to the customer and to increase competitiveness.

Today, we need to pursue these goals more vigorously in order to minimize environmental pollution and wastes, besides affecting energy savings and conserving material resources.

In this handbook, Chapter 18 discusses how to build a quality management system.

12.8 Total Quality Management

Tobin [14] defines *total quality management* (TQM) as totally integrated effort for gaining competitive advantage by continuously improving every facet of organizational culture. Witcher [15] highlights important aspects of TQM using the following explanation:

Total signifies that every person in the firm must be involved (possibly even customers and suppliers)

Quality indicates the customer requirements are met fully.

Management represents that the senior executives are fully committed.

Feigenbaum [4] defines TQM as the organization-wide impact of TQC. The Department of Defense (DOD) of the US defines TQM as a philosophy and a set of guiding principles of a continuously improving organization. In fact, TQM [16, 17, 18, 19] entails the application of management techniques, quantitative methods and human resources to improve the material services supplied to an organization, all the processes within the organization, and the degree to which the requirements of its customers are met, now and in future. It stresses on optimal life-cycle cost and applies management methodologies to target improvements. A sound quality policy together with organization and facilities is a fundamental requirement for implementing TQM. The important elements of TQM philosophy are the prevention of defects and an emphasis on quality in design, elimination of losses and reduction of variability. It also stresses the development of relationships between employees, suppliers and customers.

TQM starts at the top and top management should demonstrate their commitment to quality and communicate it down to every one in the company through the middle level management. Developing and publishing clear corporate beliefs and objectives or mission statement helps motivating people. Every employee must be able to participate in making the company successful in its mission. This flows from empowerment of people at all levels to act for quality improvement and the efforts of all those who contributed to achieve good results must be recognized and publicized. The management should strive to remove barriers between the departments of the organization. Instead they should inculcate the spirit of team work and establish perfect communication between them. It often requires a mindset to change to breakdown the existing barriers. In fact, implementing TQM is like growing a new culture in the organization. The role of training and education cannot be underestimated and should back up the efforts of implementing TQM so that all employees clearly know what is at stake.

It is often believed that TQM is perhaps the only way of assuring customers what they want first time, each and every time. There is enough evidence to show that this is so. If it were not leading firms like American Express, IBM, Xerox, 3M, Toyota, Ricoh, Cannon, Hewlett-Packard, Nissan and many others may not be so successful. TQM is not just to meet customer requirements but to provide them satisfaction. Some companies, like Rover Cars, have extraordinary customer satisfaction as their corporate mission. Among other features, customer requirement may include

delivery, availability, maintainability, reliability and cost effectiveness. While dealing with a supplier–customer relationship, the supplier must establish marketing activity charged with this task. The marketers must, of course, not only understand the requirement of the customer completely, but also their own ability to meet customer demands. Within organizations, and between customers and suppliers, the transfer of information regarding requirements is often very poor and sometimes totally absent. Therefore a continual examination of the customers' requirements and our ability to meet them is the price of maintaining quality. In fact, TQM philosophy very much relies on using the knowledge base as an asset in an organization. Everybody needs to be educated and trained to do a better job.

12.9 ISO Certification

The objective of International Organization for Standardization (ISO), which consists of representatives from several countries, comprised of more than 180 technical committees, covering many industry sectors and products, is to promote the development of standards, testing, and certification in order to encourage the trade of goods and services. Usually a standards body represents each country. There are two types of standards introduced by ISO, *viz.*, ISO 9000 for quality and ISO 14000 for environment.

ISO 9000 came into being in 1987 followed nearly by 10 years later by ISO 14000. ISO 9001 initially developed four standards (ISO 9000-9004) for different types of industries but in 1995 ISOs were revised and finally in the year 2000, there was only one standard, *i.e.*, ISO 9000-2000, which is the main stay of quality management system for all types of industries and organizations. Likewise, there is ISO 14000 for environment system management. ISO by itself does not audit or assess the management system of organizations to verify that they have been implemented in conformity with the requirements of the standards nor does ISO issue certifications. However, the auditing and certification done by ISO has approved more than 750 certification bodies active around the world.

The basic objective of the ISO 9000 quality standards is for a company to be able to establish quality systems, maintain product integrity, and satisfy customers.

ISO 9000 has become an international reference for quality management requirements in business-to-business dealings, which helps organizations to fulfil:

- customer quality requirements, and is
- applicable regulatory requirements, while aiming to
- enhance customer satisfaction, and
- achieve continual improvement of its performance in pursuit of these objectives.

ISO 14000 is primarily concerned with *environmental management*. This means what the organization does to:

- minimize the harmful effects on the environment caused by its activities, and to
- achieve continual improvement of its environmental performance.

For some firms, the first step in creating a total quality environment begins with the establishment of a quality management system such as enunciated by ISO 9000. For others, it is always debatable whether it is better to implement TQM or ISO 9000 first. However, if one views ISO 9000 as a route to TQM, they are complementary to each another. For companies already on TQM, installing ISO 9000 is comparatively straightforward. However, for companies planning towards TQM, the use of ISO 9000 can act as an instrument to achieve TQM. Nonetheless, it is true that, even with ISO 9000 certification, it cannot be guaranteed that the products and services are of high quality. To produce quality products and services, a company needs TQM to meet expectations.

12.10 Six Sigma

The term Six Sigma [20] was coined by Bill Smith, an engineer at Motorola, in 1986 and is actually a trademark of Motorola that resulted in a saving of US $17 billions by January 2006. It is a measure

of process capability and is related to the defect rate and complexity of a process/ product. Six Sigma is a standard of excellence that allows less than four (or precisely 3.4) defects per million opportunities.

Some of the top companies that have embraced Six Sigma [21] as their company's strategy for quality improvement are: General Electric (GE), Honeywell International, Raytheon, Sony, Honda, Texas Instruments, Hitachi, Canon, Asian Brown Bovery, *etc*. In fact, GE is said to have made a gross annual profit of US $6.6 billion in the year 2000, which was 5.5% of their sales [22].

Six Sigma offers a proven management framework of processes, techniques and training that satisfies ISO 9000:2000 requirements with respect to:

- demonstrating top management commitment to continually improving the effectiveness of the quality management system;
- competence, awareness and training in statistical techniques and quality management;
- continual improvement of the quality management system;
- monitoring and measurement of customer satisfaction;
- monitoring, measurement and improvement of processes and products;
- analysis of data.

In fact, Six Sigma capitalizes on the good points of TQM with a sharp focus on customer satisfaction and thus combines good features of all earlier quality initiatives for quality improvement and does not have very many tools of its own. It is asking tougher and tougher questions until quantifiable answers are received. Through Six Sigma companies question every process, every number, every step along the way to creating a final product.

Six Sigma is a data-driven, systematic approach to problem solving, with a focus on customer impact. Statistical tools and analysis are often useful in the process. However, the Six Sigma project can be started with only rudimentary statistical tools.

For successful implementation of Six Sigma, a company requires the active role of the following:

- *Executive leadership* empowers the other role holders with the freedom and resources to explore new ideas for breakthrough improvements.
- *Champions* are responsible for the Six Sigma implementation in the company and are drawn from the upper management. Champions also act as mentor to black belts.
- *Master black belts* act as full time in-house expert coaches for Six Sigma and ensure integrated implementation of Six Sigma across various departments in the company.
- *Black belts* operate under master black belts to apply the Six Sigma methodology to specific projects.
- *Green belts* are common employees who help black belts implement Six Sigma along with their normal job responsibilities.

When 50% or more employees of a company embrace Six Sigma, the profitability of the company is bound to increase dramatically.

Design for Six Sigma (DFSS) is an important step in designing new products and/or processes and uses Six Sigma as a strategy. It is a way to implement the Six Sigma methodology as early in the product or service cycle as possible. It is a pathway to exceed customer expectations and a means to gain market share. It results in high ROI (return on investment) and reduces warranty costs.

Further, for services, a fusion of Lean and Six Sigma improvement methods is required. Lean Six Sigma is a business improvement methodology that maximizes shareholder value by achieving the fastest rate of improvement in customer satisfaction, cost, quality, process speed, and invested capital. The need for Lean Six Sigma arose from the fact that one cannot just have quality or speed, one needs a balanced process that can help an organization to focus on improving service quality, as defined by the customer within a set time limit.

Recent Six Sigma trends are in the development of a methodology by integrating it with TRIZ for inventive problem solving and product design. It was developed by the Russian engineer Genrich Altshuller [23] and his colleagues in 1946. TRIZ (the Russian acronym for the theory of inventive problem solving) is basically a collage of concepts

and tools to solve manufacturing problems and create new products and has been used by companies like Procter & Gamble, Ford Motor Company, Boeing, Philips Semiconductors, LG Electronics, Samsung and many others.

In order to familiarize the reader with Six Sigma and to explore the future trends, Chapter 16 on Six Sigma has been included in this handbook.

12.11 Product Life-cycle Management

Product life-cycle management (PLM) is the activity of managing a company's products most effectively all through their life-cycles. This allows a company to take control of its products. With products becoming increasingly complex, customers becoming more demanding, the need to have shorter product development times, and the competitive product environment in the market, on-going globalization, outsourcing of product development, mass customization to meet customer requirements, end of life issues, product support over its long life, WEEE-like directives about disposal and recycling would make this job still more difficult. Losing control can have disastrous effects for a company. PLM [24] helps bring better products in the shortest possible time to the market, provides better customer support and reduces the cost of a product. In fact, PLM helps maximize the value of a product over its life-cycle. All companies need to manage communications and information with its customers through customer relationship management (CRM) and its suppliers through supply chain management (SCM)) and the resources within the enterprise through enterprise resource planning (ERP). In addition, a manufacturing engineering company should develop, describe, manage and communicate information about their products through PLM. PLM helps reduce the time to market, improves product quality, reduces prototyping costs, affects savings through the re-use of original data, reduces waste, and results in savings through the complete integration of engineering workflows and thereby provides a framework for product optimization.

The product life-cycle goes though many phases, involves many professional disciplines, and requires many skills, tools and processes. Product life-cycle management (PLM) is more to do with managing descriptions and properties of a product through its development and useful life, mainly from a business/engineering point of view; whereas product life-cycle management (PLC) is to do with the life of a product in the market with respect to business/commercial costs and sales measures.

Within PLM there are two primary areas:

- product data management (PDM)
- product and portfolio management

PDM is focused on capturing and maintaining information on products and/or services through its development and useful life. This is the activity that has the major influence on the time taken to get the product to market and on the cost of the product. Since the quality of the product delivered to the customer is in many ways a function of the quality defined during product development, it is here that major improvements in product quality must be made.

On the other hand, product and portfolio management focuses on managing resource allocation, tracking progress *vs*. plan for projects in the new product development projects that are in process (or in a holding status). Portfolio management is a tool that assists management in tracking progress on new products and making trade-off decisions when allocating scarce resources.

The core of PLM is in the creation and central management of all product data and the technology used to access this information and knowledge. PLM as a discipline emerged from tools such as CAD, CAM and PDM [25], but can be viewed as the integration of these tools with methods, people and the processes through all stages of a product's life. It is not just about software technology but is also a business strategy.

12.12 Other Quality Related Initiatives

There are several other initiatives related to quality improvement that have been introduced from time to time with the basic objective of improving quality of products, and productivity and profitability of the company.

Concurrent Engineering

Concurrent engineering can be defined as a strategy of employing a multi-disciplinary team consisting of specialists from business, engineering, production and customer support to conceptually conceive a product and to carry out its design and production planning all at one time. Inputs from all departments concerned, such as materials, purchase, marketing, finance, engineering design, production, quality, suppliers and customers, *etc*., are available simultaneously through brainstorming sessions to arrive at an agreed design. That is why sometimes it is also known as simultaneous engineering or parallel engineering. This is done to prevent problems with quality and productivity from occurring and eliminates the possibility of engineering changes at a later stage, which helps decrease the lead time and costs. This practice is at variance from sequential engineering followed earlier. Concurrent engineering designs the product within production capabilities so that statistical process control is effective and rework costs decrease. The main advantages of concurrent engineering are a substantial decrease in lead time to market, faster product development, better quality, and increased productivity. For example, the Chrysler Corporation used concurrent engineering to develop the Viper model from the concept stage to full production in less than three years with a budget of US $50 million. General Motors eliminated 900 parts from the 1995 Chevrolet Lumina model in comparison to its 1994 model and reduced assembly time by 33%. Westinghouse Electronic Systems decreased development lead times from 20 months to 9.

Kaizen

Kaizen is the Japanese term for *continuous improvement*. "Zen" in the word Kaizen emphasizes the learning-by-doing aspect of improving production. The Kaizen concept was pioneered by in Japan by Toyota as a daily challenge to all its employees to improve their processes and working environment little by little over time. Kaizen refers to a "quality" strategy and is related to various quality-control systems, including methods of W. Edwards Deming. Kaizen aims to eliminate waste or activities that add to the cost but do not add to the value. It is a rigorous and scientific method of using SQC and an adaptive framework of organizational values and beliefs that keeps workers and management focused on the objective of zero defects.

The Kaizen cycle has four steps:

- Establish a plan to change whatever needs to be improved.
- Carrying out changes on a small scale.
- Observe the results,
- Evaluate both the results and the process and determine what has been learned.

Masaaki Imai made the term famous in his book on Kaizen [26]. Kaizen methodology includes making changes and monitoring results, then adjusting. Large-scale pre-planning and extensive project scheduling are replaced by smaller experiments, which can be rapidly adapted as new improvements are suggested.

Quality Circles

One of the most publicized aspects of Japanese management is the *quality circles* or *Kaizen teams*. The quality circles concept first originated in the 1960s and became very popular around the world, partly due to the phenomenal Japanese success in improving the quality of their products. A quality circle is a voluntary group of workers doing a similar job, who meet regularly during the working hours under the leadership of their supervisor to identify, analyze and solve shop floor problems and possibly recommend solutions to management. These circles were successful in some countries but failed in others, partly due to a lack of enthusiasm in inculcating quality consciousness and understanding on the part of senior management and partly due to different cultural backgrounds.

Just in Time

Just in time (JIT) is an inventory strategy implemented to improve the return on investment of a business by reducing in-process inventory and its associated costs. The process is driven by a series of signals, or *Kanban* that tell production processes when to make the next part. Kanban are called "tickets" but can be simple visual signals, such as the presence or absence of a part on a shelf.

JIT [27] can lead to dramatic improvements in a manufacturing organization's return on investment, quality, and efficiency if implemented correctly.

Actually, the JIT inventory systems have a whole philosophy that the company must follow in order to avoid its downsides. The ideas in this philosophy come from many different disciplines including statistics, industrial engineering, production management and behavioral science. Inventory is seen as incurring costs, or waste, instead of adding value, contrary to traditional thinking. Under the JIT philosophy, businesses are encouraged to eliminate inventory that does not compensate for manufacturing issues and to constantly improve processes so that inventory can be removed. Secondly, by allowing any stock, management may be tempted to keep stock to hide problems within the production system, which include backups at work centers, machine reliability, process variability, lack of flexibility of employees and equipment, and inadequate capacity, among other things.

In short, the just-in-time is an inventory system that allows one to have the right material, at the right time, at the right place, and in the exact amount.

References

[1] Crosby PB. Quality is free. McGraw-Hill, New York, 1979.

[2] Juran JM, Gryna Jr. FM. Quality planning and analysis. 2nd ed., McGraw-Hill, New York, 1980.

[3] Deming WE. Quality, productivity and competitive position. Cambridge, Mass.: Center for Advanced Engineering Study. MIT, 1982.

[4] Feigenbaum AV. Total quality control. 3rd ed., McGraw-Hill, New York, 1983.

[5] Taguchi G. Introduction to quality engineering. Asian Productivity Organization, Available from UNIPUB, White Plains, NY, 1986.

[6] Latino Robert J, Latino Kenneth C. Root cause analysis: Improving performance for bottom-line results. Taylor and Francis, Boca Raton, FL, 2006.

[7] Hansen BL, Ghare PM. Quality control and applications. Prentice-Hall, Inc., Englewood Cliffs, NJ, 1987.

[8] Shewhart WA. Economic control of quality of manufactured product. Van Nostrand, New York, 1931.

[9] Taguchi G. System of experimental design. UNIPUB, White Plains, NY, 1987.

[10] Dehnad Khosrow. Quality control, robust design and Taguchi method. Wadsworth & Brooks, California, 1989

[11] Pearn WL, Kotz Samuel. Encyclopedia and handbook of process capability indices*:* A comprehensive exposition of quality control measures, World Scientific, Singapore, 2006.

[12] Montgomery Douglas C. Introduction to statistical quality control. Wiley, New York, 1986.

[13] Mitra Amitava. Fundamentals of quality control and improvement. Prentice Hall, Englewood Cliffs, NJ, 1998.

[14] Tobin LM. The new quality landscape: Total quality management. Journal of System Management 1990; 41(11):10-14.

[15] Witcher BJ. Total marketing: Total quality and the marketing concept. The Quarterly Review of Marketing, 1990; Winter

[16] Smith S. Perspectives: Trends in TQM. TQM Magazine, 1988; 1(1):5.

[17] Oakland JS. Total quality management. Butterworth-Heinemann, Oxford, 1989.

[18] Hakes C. Total quality management: A key to business improvement. Chapman and Hall, London, 1991.

[19] Besterfield DH, Besterfield-Michna C, Besterfield GH, Besterfield-Sacre M. Total quality management, Prentice Hall, Englewood Cliffs, NJ, 1995.

[20] Harry Mikel J, Schroeder Richard. Six sigma: The breakthrough management strategy revolutionizing the world's top corporations, Random House, New York , 2000.

[21] Shina Sammy G. Six Sigma for electronics design and manufacturing, McGraw-Hill, New York, 2002.

[22] Cottman Ronald J. Total engineering quality management. Marcel Dekker, New York, 1993.

[23] Averboukh, Elena A. Six Sigma trends: Six Sigma leadership and innovation using TRIZ. http://www.isixsigma.com/library/content/c030908a.asp.

[24] Stark John. Product lifecycle management: 21st century paradigm for product realization. Springer, London, 2006.

[25] Nanda Vivek, Quality management system handbook for product development companies. CRC Press, Boca Raton, FL, 2005.

[26] Masaaki Imai, Kaizen: The key to Japan's competitive success, McGraw-Hill/Irwin, 1986.

[27] Hirano Hiroyuki and Makota, Furuya. JIT is flow: Practice and principles of lean manufacturing, PCS Press, Vancouver, 2006.

13

Quality Engineering: Control, Design and Optimization

Qianmei Feng[1] and Kailash C. Kapur[2]

[1]University of Houston, Houston, Texas, USA
[2]University of Washington, Seattle, Washington, USA

Abstract: This chapter reviews the present status and new trends in quality engineering for control, design, and optimization of product and manufacturing processes as well as other processes/systems. Reviews of quality management strategies and programs are presented including principle-centered quality improvement, quality function deployment, Six Sigma process improvement, and Design for Six Sigma. Techniques for off-line quality engineering are presented with emphasis on robust design, signal-to-noise ratios, and experimental design. Approaches for on-line quality engineering are described including acceptance sampling, 100% inspection, statistical process control, control charts, and process adjustment with feedback control.

13.1 Introduction

In the current competitive global market, organizations are under increasing pressure to improve quality of products or services by reducing variation. The application of quality programs, tools and techniques has been expanded beyond the traditional manufacturing industry to healthcare, service, finance, retail, transportation, military defense and many other areas. The traditional quality tools are no longer sufficient to handle emerging challenges due to customized products, low production runs, automated processing, and real-time diagnosing [1]. With the recent advancement in technologies along with more involvement of statistical techniques, quality tools, techniques, and methodologies have been enhanced to meet new challenges. Over the last 30 years, a lot of progress has been made in the field of quality engineering based on research in statistical quality control (SQC), engineering process control (EPC), statistical experimental design, robust design, and optimization methods. The purpose of this chapter is to provide a review on the current status and future trends of quality engineering in terms of control, design and optimization.

The chapter starts with definitions of quality and quality engineering, followed by an overview of quality management strategies and programs including principle-centered quality improvement, quality function deployment, and Six Sigma methodology. The current status and advances in off-line quality engineering are presented with emphasis on robust design. The techniques for on-line quality engineering are then described including acceptance sampling, 100% inspection, statistical process control, and process adjustment with feedback control.

13.2 Quality and Quality Engineering

13.2.1 Quality

Quality has been defined in different ways by various experts and the operational definition has even changed over time. The best way is to start from the original meaning of the word. Quality, in Latin, *qualitas*, comes from the word *quails,* meaning "how constituted" and signifying "such as the thing really is" [2–4]. Merriam-Webster dictionary defines quality as "*….peculiar and essential character…a distinguishing attribute….*"

A product typically has several or infinite qualities. Juran and Gryna considered multiple elements of fitness of use based on various quality characteristics (or qualities), such as technological characteristics (*e.g*., strength, dimensions, current, weight, and ph values), psychological characteristics (*e.g*., beauty, taste, and many other sensory characteristics), time-oriented characteristics (*e.g*., reliability, availability, maintainability, safety, and security), cost (*e.g*., purchase price, and life cycle cost), and product development cycle [5].

Deming also discussed the three corners of quality, which relate to various quality characteristics, and focused on the evaluation of quality from the viewpoint of the customer [6]. The American Society for Quality defines quality as the "*the characteristics of a product or service that bear on its ability to satisfy stated or implied needs*" [7]. Thus, quality of products or services is defined and evaluated by the customer.

Dynamic competition in the global market is forcing organizations to provide products and services with less variation than their competitors. A product must be designed for manufacturability and must be insensitive to variability presented in the production environment and in the field when used by the customer. Montgomery provided a definition of quality related to variability as: "*quality is inversely proportional to variability*" [8]. This concept is also related to an evaluation of quality using quality loss function promoted by Taguchi, which will be discussed in this chapter. Reduced variation translates into greater repeatability, reliability, and ultimately cost savings to both the producer and the consumer and thus the whole society.

It is obvious from the definitions of quality that the emphasis of any quality programs or processes is to meet and exceed customers' needs and expectations, and focus on delight and enthusiasm of the customer.

13.2.2 Quality Engineering

Quality engineering is a series of operational, managerial, and engineering approaches to ensure that quality characteristics of a product are delivered at the required levels from the viewpoint of the customer for the duration of the designed product life. To achieve high quality of a product, quality engineering approaches must be applied over each phase of the product life cycle. Figure 13.1 shows how the cost to fix or solve problems increases as we move downstream in the product life cycle. The early and proactive activities should be taken to prevent problems, because approximately 90% of the life cycle cost is determined by the concept and development phases of the life cycle for many systems.

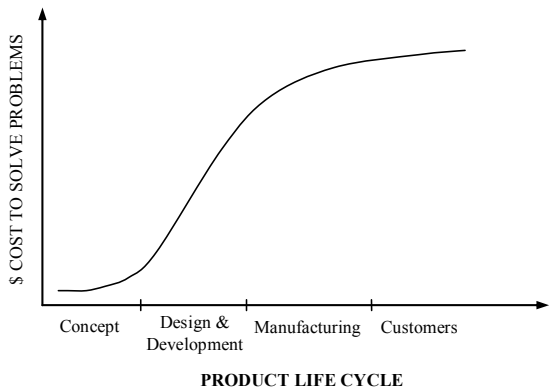


Figure 13.1. Cost to solve problems vs. product life cycle

Various quality engineering approaches can be utilized at different phases of product life cycle [3]. It results in two areas of quality engineering: (1) *off-line quality engineering* that is implemented as part of the research, design and development

phases, and (2) *on-line quality engineering* that is typically applied during production.

As the most efficient and cost-effective quality improvement activity, off-line quality engineering is a systematic methodology to improve the design of products and processes. Three design phases: system design, parameter design, and tolerance design are implemented for off-line quality engineering to make product or process performance insensitive (robust) to uncontrollable variables, which are noise factors. The optimal values of the mean (related to nominal value) and standard deviation (related to tolerance) of quality characteristic are determined by minimizing the variability of the quality characteristic through experimental design and process adjustment techniques. The three design phases were originally developed by Genichi Taguchi, and introduced to American industries in the 1980s [9, 10]. Since then, a lot of research has improved the related statistical techniques of quality engineering proposed by Taguchi and clarified many underlying assumptions and principles.

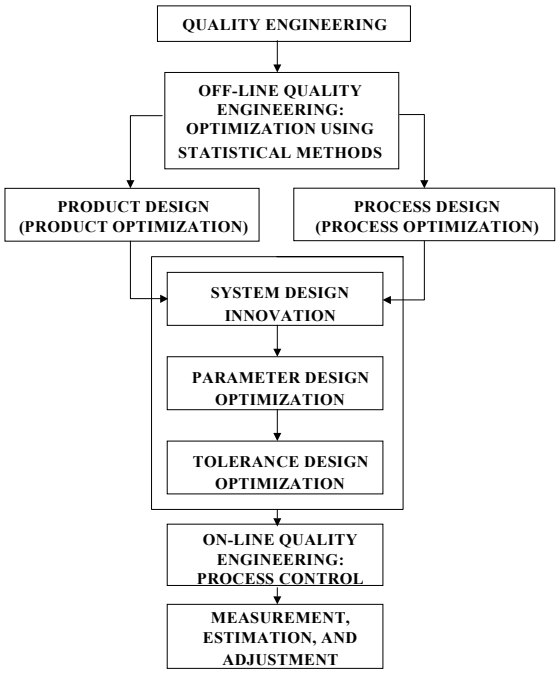


Figure 13.2. Quality engineering

As opposed to off-line quality engineering (Figure 13.2), on-line quality engineering refers to techniques employed to maintain quality during the manufacturing process. Statistical quality control (SQC) or statistical process control (SPC) is a primary on-line control technique for monitoring the manufacturing process or any other process with key quality characteristics of interest. The major goal of SQC (or SPC) is to monitor the manufacturing process, keep the values of mean and standard deviation stable, and finally reduce variability. Some additional quality techniques for on-line quality engineering include acceptance sampling and other quality inspection methods. Acceptance sampling is defined as the inspection and classification of samples chosen from a lot randomly and decision about disposition of the lot.

13.3 Quality Management Strategies and Programs

Off-line and on-line quality engineering provides the technical basis for problem solving in quality improvement, while quality management ensures the effective implementation of such techniques within an organization. In many organizations, the product development process is often based on trial and error and many activities have conflicting goals and objectives. The needs of the customer are not clearly understood. The purpose of quality management is to transform an organization to an integrated and distributed system as shown in Figure 13.3 [11].

There have been many quality management programs devoted to quality improvement and management, including total quality management (TQM), ISO 9000 series, Six Sigma, Lean Sigma, *etc.* The successful implementation of these programs requires that the supportive management system of an organization supervise the overall quality improvement effort, including quality planning, quality assurance, and quality control and improvement [8].

Quality planning (QP) is a strategic process to identify external and internal customers, clarify voice of customers, and develop plans to meet or exceed customers' expectations. Quality function

deployment (QFD) is a very important technique for the strategic quality planning, and the details of QFD will be discussed later.

Quality assurance (QA) contains systematic activities implemented within the quality system that can be demonstrated to provide confidence that a product or service will fulfill requirements for quality [7]. The ISO 9000 series provide generic standards that are applicable to any type of organization to perform quality assurance activities. Also available from the International Standards Organization is the ISO 14000 family, which is primarily concerned with "environmental management."

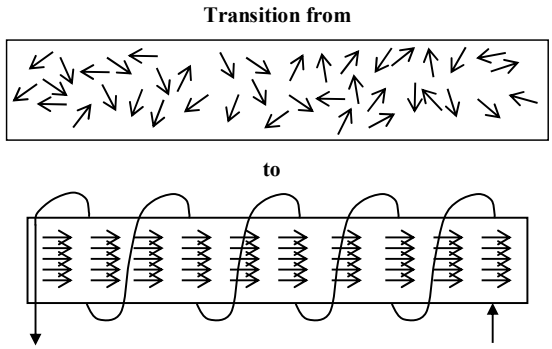


Figure 13.3. Integrated and distributed process

Quality control and improvement involves the activities of quality engineering that are implemented through projects. Six Sigma is a project-by-project approach that integrates the philosophy of quality management and techniques of quality engineering. Six Sigma methodology will be introduced later in this section. Before the emergence of Six Sigma, the implementation of total quality management (TQM) in many organizations enhanced people's awareness of the importance of quality. TQM emphasizes managing quality improvement activities on an organization-wide basis, and integrating the quality system with other organizational activities around the quality improvement goal. However, the importance of technical tools is not very well promoted in TQM.

In this section, the principle-centered quality management strategies will be elaborated by comparing traditional practices and new trends. Several recent quality improvement tools and programs will be reviewed including quality function deployment, Six Sigma, and Design for Six Sigma (DFSS).

13.3.1 Principle-centered Quality Management

Various quality programs stress the importance of quality for management in an organization. To develop consistent ideas for research and development that are useful for the 21st century and beyond, the constancy of purpose for quality and productivity improvement should be emphasized based on these principles. Such principles for quality improvement include [12]:

1. Customer focus and constancy of purpose
2. System focus
3. Process focus
4. Understanding the hierarchical structure and causation
5. Future focus and ideals for quality
6. Continuous improvement
7. Prevention and proactive strategies
8. Scientific approach
9. Integration

Table 13.1 presents the traditional practices versus new trends for each of the principles [12]. In general, the trend for quality management is to integrate organizational culture, values and beliefs, habits, technology, and strategic operations, as shown in Figure 13.4 [12].

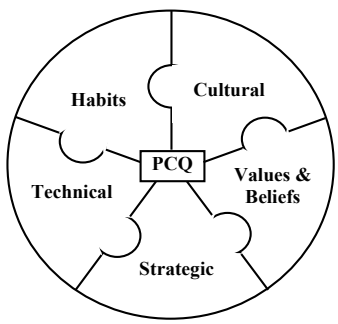


Figure 13.4. Integration for principle-centered quality (PCQ)

Table 13.1. Principle-centered quality: traditional practices versus new trends

	Traditional or past practices	Ideals or new trends
Customer focus	Fads, Trends	Constancy of purpose, Principle-centered
	Internal	External, Customer focus
System focus	Independence or dependence	Interdependence
	Competition	Teamwork, Collaboration
	Focus on control and centralization	Distributed but integrated by enterprise processes
	Quality & Reliability – subsystem optimization	Systems approach and system integration – holistic & synergistic
Process focus	Feedback	Feed forward
	Sequential	Simultaneous
	Ends	Means to achieve higher customer satisfaction
Hierarchical structure	Effect, Ends, Results/objectives	Cause, Means, Process focused
Future focus	Short term thinking	Infinite horizon
	Measurement (statistical estimation)	Improvement and growth, future perfect
Continuous Improvement	Binary	multi-state, continuous
	Specifications or tolerances or limits	Targets or ideals
	Six Sigma	Infinite sigma
	Achievable metrics	Ideals, never ending, perfection, continuous, improvement
	Failure or defect, nonconformance	Transition of the system from one state to another
Prevention and proactive	Inspection/audit /detection	Prevention /proactive
	Burn-in	Reduce process, variation
Scientific approach	Follow or copy other's success stories	Scientific and not anecdotal
	Eliminate/minimize cause	Reduce the effect of the cause
	Accept time as a noise	Achieve robustness
Integration	Fragmented-jump from tool to tool	Integration based on values and beliefs
	Probability models	Utility, customer satisfaction, probability as a basis for action

13.3.2 Quality Function Deployment

A process may have many processes before it, which are typically called the suppliers, and has many processes after it, which are its customers. Therefore, anything that the present process affects is its customer, such as the next process, environment, the end user, *etc*. One of the most important tasks in a quality program is to understand and evaluate the needs or expectations of the customer, and then provide products and services that meet or exceed those expectations. Shewhart states this as follows [13]: "*The first step of the engineer in trying to satisfy these wants is, therefore, that of translating as nearly as possible these wants into the physical characteristics of the thing manufactured to satisfy these wants. In taking this step, intuition and judgment play an important role as well as the broad knowledge of human element involved in the wants of individuals. The second step of the engineer is to set up ways and means of obtaining a product which will differ from the arbitrary set standards for these quality characteristics by no more than may be left to chance.*"

Mizuno and Akao developed a technique called quality function deployment (QFD) that contains the necessary philosophy, system, and methodology to achieve the first step proposed by Shewhart [14]. As presented in Figure 13.5, QFD is a means to translate the "voice of the customer" into substitute quality characteristics, design

configurations, design parameters, and technological characteristics that can be deployed (horizontally) through the whole organization: marketing, product planning, design, engineering, purchasing, manufacturing, assembly, sales, and service [14, 15]. Products have several characteristics and an "ideal" state or value of these characteristics must be determined from the customer's viewpoint. This ideal state is called the target value. Using QFD methodology, target values can be developed for substitute quality characteristics, which satisfy the requirements of the customer. The second step mentioned by Shewhart is accomplished by statistical process control, which is given in his pioneering book [13].

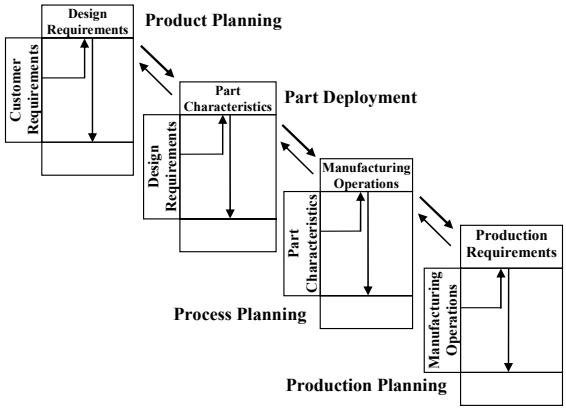


Figure 13.5. Phases for quality function deployment

13.3.3 Six Sigma Process Improvement

Based on the ideal or target value of the quality characteristic from the viewpoint of the customer, the traditional evaluation of quality is based on average measures of the process/product and their deviation from the target value. However, customers judge the quality of process/product not only based on the average, but also by the variance in each transaction with the process or use of the product. Customers want consistent, reliable and predictable processes that deliver or exceed the best-in-class level of quality. This is what the Six Sigma process strives to achieve. Six Sigma has been applied to many manufacturing companies and service industries such as healthcare systems, financial systems, *etc*.

Six Sigma is a customer-focused, data driven and robust methodology, which is well rooted in mathematics and statistics [16–18]. A typical process for Six Sigma process improvement has six phases: Define, Measure, Analyze, Improve, Control and Technology Transfer, denoted by (D)MAIC(T). Traditionally, a five-phase process, DMAIC is often referred in the literature [19]. We extend it to the six-phase process, (D)MAIC(T), because we want to emphasis the importance of the technology transfer (T) as the never-ending phase for continuous applications of the Six Sigma technology to other parts of the organization to maximize the rate of return on the investment in developing this technology [20, 21].

The process of (D)MAIC(T) stays on track by establishing deliverables at each phase, and by creating engineering models over time to reduce the process variation. In each phase, several steps need to be implemented. For each step, many quality improvement methods, tools and techniques are used. Interested readers are referred to Kapur and Feng for further details [20, 21].

The primary reason for the success of Six Sigma is that it provides an overall approach for quality and process improvement, and it is not just a collection of tools. During most quality training in academia, industry and government, students and professionals usually are taught a number of individual tools such as DOE, SPC, FMECA, FTA, QFD, *etc*., and leave the course without a mental big picture about how all these tools fit together. Six Sigma provides an overall process of improvement, (D)MAIC(T), that clearly shows how to link and sequence individual tools. With Six Sigma, students and professionals know what to do when faced to a real problem.

Six Sigma focuses on reducing process variation and thus on improving the process capability [22, 23]. The typical definition for process capability index, C_{pk}, is: $C_{pk} = \min\left\{\frac{USL-\hat{\mu}}{3\hat{\sigma}}, \frac{\hat{\mu}-LSL}{3\hat{\sigma}}\right\}$, where USL is the upper specification limit, LSL is the lower specification limit, $\hat{\mu}$ is the point estimator of the mean, and $\hat{\sigma}$ is the point estimator of the standard deviation. If the process is centered at the middle

of the specifications, which is also interpreted as the target value, i.e. $\hat{\mu} = \frac{USL + LSL}{2} = y_0$, then the Six Sigma process means that C_{pk} =2. In literature, it is typically mentioned that the Six Sigma process results in 3.4 defects per million opportunities (DPMO). For this statement, it is assumed that the process shifts by 1.5σ over time from the target (which is assumed to be the middle point of the specifications). It implies that the realized C_{pk} is 1.5 for the Six Sigma process over time. It is obvious that 6σ requirements or C_{pk} of 1.5 is not the goal; the ideal objective is to continuously improve the process based on some economic or other higher-level objectives for the system.

13.3.4 Design for Six Sigma (DFSS)

While Six Sigma process improvement approach leaves the fundamental structure of a process unchanged, Design for Six Sigma (DFSS) involves changing or redesigning the process at the early stage of product/process life cycle. DFSS becomes necessary when [18]

- An organization or designer chooses to replace, rather than repair, the current process;
- Improving an existing process cannot achieve the required quality level; or
- An opportunity is identified to offer a new process.

Although DFSS takes more effort at the beginning, it will benefit the system in the long run by designing Six Sigma quality into product/process. There are several methodologies for DFSS, such as DMADV, IDOV or ICOV. DMADV is a popular methodology since it has the same number of letters as the DMAIC acronym. The five phases of DMADV are defined as: Define, Measure, Analyze, Design and Verify. IDOV or ICOV is a well-known design methodology, especially in the manufacturing world. The IDOV (or ICOV) acronym is defined as Identify, Design (Characterize the design), Optimize and Validate. Interested readers are referred to the details in an article by Simon [24].

13.4 Off-line Quality Engineering

13.4.1 Engineering Design Activities

The engineering activity of designing and optimizing a product or process is complex. Off-line quality engineering methods are conducted at the product development cycle with the overall aim to improve product manufacturability and reliability, and reduce product development and lifetime costs [25]. As part of the delivery of these activities, three essential elements have to be specified: (1) system architecture including design of the overall system, subsystems and components, (2) nominal values of parameters in the system, and (3) tolerances of parameters. These three elements are accomplished through three steps of engineering design: system design, parameter design, and tolerance design [9].

1. *System design:* During this step, a variety of system architectures and technologies are examined, and the most suitable one is selected for achieving the desired function of the product or process. This step requires the experience, skills, and creativity of the design team. Quality function deployment (QFD) discussed in Section 3 can be used to translate the "voice of the customer" into design configurations, design parameters, and technological characteristics. After system design, it is often that the theoretical model is not available to describe the functional relationship between output variables and input variables. Statistical design of experiments, orthogonal polynomials, and regression analysis are important tools to derive the empirical model for the system transfer function.
2. *Parameter design*: In this step, the optimal settings of input variables are selected to optimize output variables by reducing the influence and effect of noise factors. The best settings should improve the quality level without increasing manufacturing cost. This is achieved by using low-grade components and materials with wide tolerances on noise factors, while the best settings of input variables are insensitive or robust to the variability. This step makes effective use of experimental design and response surface methods. Parameter design is the central focus of robust

design that is to improve the quality of a product or process by minimizing the effect of the causes of variation without eliminating the causes. Robust design is introduced in the next section of this chapter.

3. *Tolerance design*: In practice, when parameter design cannot achieve the desired results from the viewpoint of the customer, the quality of a product can be further improved using tolerance design. In this step, tolerances or variances of input variables are set to minimize the variance of output response by directly removing causes of variation. Usually, a narrower tolerance corresponds to a higher grade of material or component that leads to higher manufacturing costs. Therefore, design and manufacturing costs and quality losses due to variability to the customer have to be carefully evaluated and balanced (optimized) to determine the variances of input variables.

13.4.2 Robust Design and Quality Engineering

Robust design is a systematic approach that uses statistical experimental design to improve the performance of products and processes. It was originally developed by Taguchi and introduced to several major American companies in the 1980s, which resulted in significant quality improvements. Bendal *et al*. provided a collection of case studies covering the applications in automotive, electronics, plastics, and process industries [26].

The fundamental principle of robust design is to improve the quality of a product by minimizing the effect of variation without eliminating the causes [9, 10, 27, 28]. Robust design improves product quality while working on product design and manufacturing processes simultaneously by making product and process performance insensitive (robust) to hard-to-control noises [29]. Parameter design and tolerance design are very important to achieve this objective. Robust design and its associated methodology typically focus on the parameter design phase. The following are the two important tasks in robust design [27]:

1. *Performance measures* are used as an indicator to evaluate the effect of design on the product's performance in order to achieve the desired optimization goal. Taguchi introduced a family of performance measures called *signal-to-noise (S/N)* ratios.

2. *Effective experimental design* is used to determine the dependable information about control factors and their values to achieve robustness. Taguchi popularized orthogonal arrays (which have been known since the 1940s) to study many control factors simultaneously. Further information on statistical design of experiments can be found in [30–34].

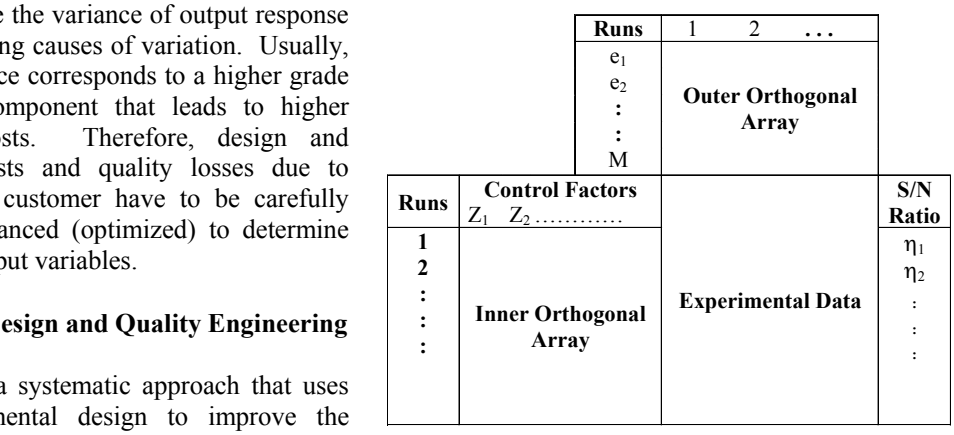


Figure 13.6. The inner and the outer orthogonal arrays

13.4.2.1 Experimentation

The goal of robust design is to reduce performance variation of a system by choosing the setting of its control factors to make it less sensitive to noise factors. Here, control factors and noise factors are two broad categories of input variables. A cross array or an inner-outer array design is often used as an experimental layout for robust design as shown in Figure 13.6. A cross array consists of a control array (or inner array) and a noise array (or outer array). For many dynamic characteristics, the inner array also has indicative factors and the outer array has signal factors (M) [10]. Each level combination in the control array is crossed with all the level combinations in the noise array. Usually, orthogonal arrays are chosen for the control array and the noise array. If some of the noise factors have more than three levels, the run size of the orthogonal array for the noise factors may be too large. Alternative plans include Latin hypercube sampling [35] and "uniform" designs based on number-theoretic methods [36].

When the run size of a cross array is too large, an alternative is to use a single array for both control and noise factors, which requires a much smaller run size. Wu and Hamada discussed the selection of cross arrays and single arrays, as well as the approaches for modeling and analyzing the data from experiments [32].

13.4.2.2 Quality Loss Function

Quality loss relates to cost or "loss" in dollars (or other measures), not just to the manufacturer at the time of production, but also to the next consumer. The intangible losses (customer dissatisfaction, loss of customer loyalty, and eventual loss of market share), along with other tangible losses (rework, defects, down time, *etc*.), make up some of the components of the quality loss. The quality loss function is a way to measure losses due to variability from the target values and transform them to economic values. The greater the deviation from target is, the greater is the economic loss.

A good quality evaluation system should measure the quality of all the items within and outside specifications. The concept of quality loss function provides a quantitative evaluation of loss caused by variation for "smaller the better", "larger the better" and "target the best" quality characteristics.

"Smaller the better" quality characteristics

The objective is to reduce the value of the quality characteristic. Usually the smallest possible value for such characteristics is zero, which is the "ideal" or target value. Some examples are wear, degradation, deterioration, shrinkage, noise level, harmful effects, level of pollutants, *etc*. Such characteristics generally have an upper specification limit (*USL*). A good approximation of the quality loss function, $L(y)$, is $L(y) = ky^2$, $y \geq 0$. The constant k depends on the natural of quality loss function $L(y)$, which reflects requirements of the customer.

"Larger the better" quality characteristics

For such quality characteristics, we want to increase their values as much as possible (within a given frame of reference). Some examples are strength, life of a system (a measure of reliability), fuel efficiency, *etc*. An ideal value may be infinity, though impossible to achieve. Such characteristics generally have a lower specification limit (*LSL*). A good approximation of $L(y)$ is $L(y) = k/y^2$, $y \geq 0$.

"Target the best" quality characteristics

An ideal or target value is specified for such a quality characteristic. The performance of the product deteriorates as the characteristic moves away from either side of the target value. Some examples are dimensional characteristics, voltage, viscosity of a fluid, shift pressure, clearance, and so on. Such characteristics generally have both *LSL* and *USL*. An approximation of the quality loss function is $L(y) = k(y - y_0)^2$.

13.4.2.3 Performance Measure: S/N Ratio

Taguchi introduced a family of performance measures called signal-to-noise (S/N) ratios. Based on the concept of quality loss function, the S/N ratio is a measure of quality loss due to noise factors and thus is used to achieve robustness and high quality. The form of S/N ratio is closely related to the form of the quality loss function that depends on the characteristic of the output response.

"Smaller the better" quality characteristics

The expected quality loss of a "smaller the better" quality characteristic is $E[L(Y)] = kE[Y^2]$. The signal to noise (S/N) ratio is a measure of the quality loss due to the effect of noise factors. Taguchi recommended using the logarithmic transformation for $E[Y^2]$ to calculate the signal to noise ratio, η:

$$\eta = -10 \log E\left[Y^2\right].$$

In order to decrease quality losses, we must increase the value of η. Let $y_1, y_2, .., y_n$ be a random sample from the distribution of Y. Then, S/N ratio (a measure of performance) can be estimated by

$$\eta = -10 \log\left(\frac{1}{n}\sum {y_i}^2\right).$$

"Larger the better" quality characteristics

The quality characteristic is continuous and nonnegative, and the target value is infinity. The expected quality loss of the "larger the better" quality characteristic is $E[L(Y)]=kE[1/Y^2]$. Again, we can develop a performance measure or S/N ratio, which minimizes the expected quality loss:

$$\eta = -10\log E\left[\frac{1}{Y^2}\right],$$

which can be estimated by the statistic:

$$\eta = -10\log\left\{\frac{1}{n}\sum\frac{1}{y_i^2}\right\}.$$

"Target the best" quality characteristics

For a "target the best" quality characteristic with the target value of y_0, an approximation for the expected loss is $E[L(Y)] = k\left[(\mu - y_0)^2 + \sigma^2\right]$. If the variance is not linked to the mean, we can use a monotone function of σ^2 and the performance measure or S/N ratio is given by

$$\eta = -10\log\sigma^2,$$

and this can be estimated by the statistic

$$\eta = -10\log\left\{\frac{\sum(y_i - \bar{y})^2}{n-1}\right\}.$$

If variance changes linearly with mean, we can minimize the coefficient of variation σ/μ to reduce quality losses. Since S/N ratio is always defined so that we maximize it, Taguchi suggested the following measure:

$$\eta = 10\log\frac{\mu^2}{\sigma^2}.$$

This can be estimated by the statistic

$$\eta = 10\log\left\{\frac{n\bar{y}^2 - s^2}{ns^2}\right\} = 10\log\left\{\frac{\bar{y}^2}{s^2} - \frac{1}{n}\right\}.$$

This performance statistics (S/N ratio) minimizes the coefficient of variation.

For "target the best" quality characteristics, Taguchi recommended a two-step procedure: (1) select the levels of the control factors to maximize the S/N ratio, and (2) select the level of adjustment factors to bring the location on target.

A summary of opinions and research directions of robust design are given in [37]. For the performance measure or the S/N ratio, Wu and Hamada described that the S/N ratio requires the system be a linear input-output system, and it lacks a strong physical justification in most practical situations [32]. A two-step procedure for the "target the best" quality characteristics was developed based on the quadratic loss function. Usually, parameter design is followed by a tolerance design, and it is called a sequential two-stage design. An economical alternative is to perform parameter design and tolerance design simultaneously [38–40]. A comprehensive review of operating window experiments and the performance measure independent of adjustment (PerMIA) for operating window experiments were given in [41].

Although Taguchi's robust design has drawn some criticism, it is broadly applicable due to its inherently sound philosophy and easier-to-implement design of experiments methods. Taguchi's robust design has promoted the use of statistical experimental design for product design improvement, and stimulated a wider application of existing statistical methods.

13.5 On-line Quality Engineering

On-line quality engineering methods are used for monitoring process and inspecting products in order to further reduce variation and improve quality. Techniques aimed at on-line quality improvement should be implemented after actions have been taken for off-line quality engineering. Since no process is free of variation, on-line process control techniques are always required to prevent, detect and reduce variations. Such techniques include acceptance sampling, inspection strategies, statistical process control, and process adjustment using feedback control.

13.5.1 Acceptance Sampling and its Limitations

As one of the earliest methods of quality control, acceptance sampling is closely related to

inspection of output of a process, or testing of product. Acceptance sampling is defined as the inspection and classification of samples from a lot randomly and decision about disposition of the lot. At the beginning of the concept of quality conformance back to the 1930s, the acceptance sample was taking the whole of the quality improvement effort. The most widely used plans are given by the Military Standard tables (MIL STD 105A), which were developed during World War II. The last revision (MIL STD 105E) was issued in 1989, but canceled in 1991. The American Society adopted the standard for Quality as ANSI/ASQ A1.4.

Due to its less proactive nature in terms of quality improvement, acceptance sampling is less emphasized in current quality control systems. Usually, methods of lot sentencing include no inspection, 100% inspection, and acceptance sampling. Some of the problems with acceptance sampling were articulated by W. Edwards Deming [6], who pointed out that this procedure, while minimizing the inspection cost, does not minimize the total cost to the producer. In order to minimize the total cost to the producer, Deming indicated that inspection should be performed either 100% or not at all, which is called Deming's "all or none rule". In addition, acceptance sampling has several disadvantages compared to 100% inspection [8]:

- There are risks of accepting "bad" lots and rejecting "good" lots.
- Less information is usually generated about the product or process.
- Acceptance sampling requires planning and documentation of the sampling procedure.

13.5.2 Inspection and Decisions on Optimum Specifications

Recent development of automated inspection technologies, such as optical sensors, thermal detectors, gas sensors, and CT scanners, makes it possible to perform 100% inspection on all items with low operating cost. 100% inspection, or screening, plays an important role in many processes, such as automobile assembly, semi-conductor manufacturing, airport baggage screening or other decision-making processes where the consequences of excessive deviations from target values are very high.

Variability means some kind of waste, yet it is impossible to have zero variability even after off-line quality engineering. The common wisdom is to set, not only a target performance value, but also a tolerance or specification about the target, which represents "acceptable" performance. The quality characteristic is regarded as acceptable only if the measurement falls within the specifications. The specification limits have to be determined in order to decide if a quality characteristic is acceptable or not. Feng and Kapur considered the specifications from the whole-system viewpoint of both the customer and the producer [42, 43]. They proposed an inspection strategy that is used to decide when to do 100% inspection, as well as to determine specifications for the 100% inspection. Two questions are to be answered after off-line engineering actions have been taken:

Question 1: Should 100% inspection be performed before output products are shipped to the next or downstream customer?

Question 2: If 100% inspection is to be performed, how to determine the optimal specification limits that minimize the total cost to the system including both the producer and the consumer?

By answering the above two questions, the decision maker has to choose between the following two decisions:

Decision 1: No inspection is done, and thus all the output products are shipped to the next customer. One economic interpretation of cost to the downstream customers is the expected quality loss.

Decision 2: Do 100% inspection. It is clear that we will do the inspection and truncate the tails of the distribution only if it reduces total cost to both the producer and the consumer. When we truncate the distribution by using certain specification limits, some additional costs will incur, such as the measurement or inspection cost (to evaluate if units meet the specifications), the rework cost, and the scrap cost. The general optimization model is

$$\text{Minimize } ETC = EQL + ESC + IC$$

where ETC = Expected total cost per produced unit
EQL = Expected quality loss per unit
ESC = Expected scrap cost per unit
IC = Inspection cost per unit.

Based on this general optimization model, several models have been formulated under different assumptions for different quality characteristics, quality loss functions, and inspection errors [2, 42–44].

13.5.3 Statistical Process Control

As traditional approaches of on-line quality engineering, acceptance sampling and inspection strategies control the final product and screen out items that do not meet the requirements of the next customer. This detection strategy related to after-the-fact inspection is mostly uneconomical, as the wasteful production has already been produced. A better strategy is to avoid waste by not producing the unacceptable output at the first place and focus more on prevention. Statistical process control (SPC) is an effective prevention strategy for monitoring the manufacturing process or any other process with key quality characteristics of interests [8, 13, 45–47].

13.5.3.1 Benefits of Using Control Charts

Statistical process control plays a very important role during the effort for process improvement. When we try to control a process, analysis and improvement are naturally resulted in; and when we try to make an improvement, we naturally come to understand the importance of control. We can only make breakthrough when we have achieved control. Without process control, we do not know where to improve, and we cannot have standards to use control charts. Some of the important benefits that come from using control charts include:

- Control charts are simple and effective tools to achieve statistical control. They can be maintained at the job station by the operator, and give the operator reliable information on when action should/should not be taken.
- When a process is in statistical control, its performance to specification will be predictable. In this way, both the producer and the customer can rely on consistent quality levels and stable costs of achieving that quality level.
- After a process is in statistical control, its performance can be further improved to reduce variation. The expected effect of proposed improvements in the system can be anticipated, and the actual effect of even relatively subtle changes can be identified through the control chart data. Such process improvements will:
  - Increase the percentage of output that meets customer expectations (improve quality),
  - decrease the percentage of scrap or rework (reduce cost per good unit produced), and
  - increase the total yield of acceptable output through the process (improve effective capacity).
- Control charts provide a common language for communications about the performance of a process between
  - two or three shifts that operate a process;
  - line production (operator, supervisor) and support activities (maintenance, material control, process engineering, and quality control);
  - different stations in the process,
  - supplier and user, or
  - the manufacturing/assembly plant and the design engineering activity.
- Control charts, by distinguishing special causes from common causes of variation, give a good indication of whether any problems are likely to be correctable locally or will require management action. This minimizes the confusion, frustration, and excessive cost of misdirected problem-solving efforts.

13.5.3.2 Trends of SPC Applications

SPC has a broad application in the manufacturing industry, and it has recently expanded to non-manufacturing sectors such as health care, education, banking, and other industries. For instance, standard control charts are recommended for use in the monitoring and improvement of hospital performance [48]. Woodall *et al*. provided an excellent review of current uses of control charts and issues in healthcare monitoring, primarily focused on public-health surveillance, and cumulative sum and related methods [49].

Standard control charts originated by Shewhart in the 1930s have been improved in many ways due to the expansion of SPC applications recently. New methodologies are developed to provide tools that are more suitable for specific applications, such as short-run SPC, SPC with autocorrelated process data, multivariate process control, and process adjustment with feedback control.

13.5.3.3 Advanced Control Charts

Major disadvantage of standard control chart is that it uses the information in the last plotted point and ignores information given by the sequence of points. This makes it insensitive to small shifts. Two effective control charts to detect small process shifts are [8]

- Cumulative sum (CUSUM) control charts, and
- exponentially weighted moving average (EWMA) control charts.

The competitive global market expects lower defect rate and higher quality level that requires 100% inspection of output products. The recent advancement of sensing techniques and computer capacity makes 100% inspection more feasible. Due to the reduced intervals between sampling of the 100% inspection, the complete observations will be correlated over time. However, one of the assumptions for Shewhart control charts is the independence between observations over time. When the observations are autocorrelated, Shewhart control charts will give misleading results in the form of many false alarms. Time series models, such as an autoregressive integrated moving average (ARIMA) model, are used to remove autocorrelation from data and control charts are then applied to the residuals. Further discussion on SPC with autocorrelated process data can be found in [8, 50, 51].

It is often necessary to simultaneously monitor or control two or more related quality characteristics. Using individual control charts to monitor the independent variables separately can be very misleading. Hotelling developed multivariate SPC control charts based on multivariate normal distribution [52]. Multivariate methods are particularly important today, as automatic inspection systems make it relatively easy to measure many parameters simultaneously. The recent development of multivariate SPC can be found in [8, 53, 54].

The use of control charts requires the selection of sample size, sampling frequency or interval between samples, and control limits for the charts. The selection of these parameters has economic consequences in that the cost of sampling, the cost of false alarms, and the cost of removing assignable causes will affect the choice of parameters. Therefore, economic design of control charts has called attention in research and practice [8, 55–57]. Other research issues and ideas in SPC can be found in review papers [58, 59].

13.5.4 Process Adjustment with Feedback Control

Processes frequently need to be adjusted due to unavoidable disturbances. The SPC monitoring techniques such as Shewhart control charts are inappropriate and inefficient for this purpose. Engineering process control (EPC) or automatic process control (APC) can be readily used to adjust processes [60, 61]. The principle idea of EPC or APC is the feedback control technique, which has become an important resource for quality engineers [51]. A variety of techniques for process adjustment have been studied, such as run-to-run process control in the semiconductor industry [62], and a unified view of process adjustment procedures for setting up a machine based on a Kalman filter approach [63].

13.6 Conclusions

In this chapter, we reviewed the status and new trends in quality engineering for the control, design, and optimization of product and manufacturing processes as well as other systems. Quality management strategies and programs are overviewed including principle-centered quality improvement, quality function deployment, and Six Sigma methodology. The techniques for off-line quality engineering are presented with emphasis on robust design, followed by approaches for on-line quality engineering including

acceptance sampling, 100% inspection, statistical process control, and process adjustment with feedback control.

With the advancement of technology, quality practitioners need more advanced quality tools, techniques, and methodologies in order to meet new challenges. The following new trends in quality engineering have been identified:

- Principle-centered quality improvement is emphasized based on the constancy of purpose in order to develop consistent ideas for research and development that are useful for the 21st century and beyond. Comparison of traditional or old methods with new methods and trends as well as ideals is given in Table 13.1.
- Integrated or unified methods are becoming more prevalent, such as the unified method of parameter design and tolerance design, and the integration of SPC and EPC, *etc*. This also applies to integration of all quality characteristics including reliability, safety, security, life cycle cost as well as the total product development cycle [4].
- Application of quality engineering has been expanded to non-manufacturing sectors, such as healthcare systems, banking, and biomedical systems.

References

[1] Hassan A, Shariff M, Baksh N, Shaharoun AM. Issues in quality engineering research. International Journal of Quality & Reliability Management 2000; 17(8).

[2] Kapur KC. Quality loss function and inspection. Proceedings of TMI Conference on Innovation in Quality (available through Engineering Society of Detroit). Detroit, MI, 1987; Sept. 21–24.

[3] Kapur KC. Quality engineering and tolerance design. In: Kusiak K, editor. Concurrent engineering: automation, tools, and techniques. New York: Wiley, 1993; 287–306.

[4] Kapur KC. An integrated customer-focused approach for quality and reliability. International Journal of Reliability, Quality and Safety Engineering 1998; 5(2):101–13.

[5] Juran JM, Gryna FM. Quality planning and analysis. New York: McGraw-Hill, 1980.

[6] Deming WE. Quality, productivity, and competitive position. Cambridge, MA: Massachusetts Institute of Technology, Center for Advanced Engineering Study, 1982.

[7] American Society for Quality, Glossary and Tables for Statistical Quality Control, 4th ed. Milwaukee, 2004.

[8] Montgomery DC. Introduction to statistical quality control, 5th ed. New York: Wiley, 2005.

[9] Taguchi G. Introduction to quality engineering. Tokyo: Asia Productivity Organization, 1986.

[10] Taguchi G. System of experimental design, Volume I and II. New York: Quality Resources, and MI: American Supplier Institute, 1987.

[11] Kapur KC. Integrated and distributed enterprise quality management system. Singapore Quality Institute, Featured Article, 2000:93–97.

[12] Kapur KC. Principle-centered quality. Proceedings of the 7th ISSAT Conference on Reliability and Quality in Design, Washington DC 2001; August 8–10.

[13] Shewhart WA. Economic control of quality of a manufactured product. New York: D. Van Nostrand Company, 1931.

[14] Mizuno S, Akao Y. Quality function deployment - approach to total quality control. Oregon: Japanese Union of Science and Technology Publishing Company, 1978.

[15] Akao Y. Quality function deployment: integrating customer requirements in product design. Oregon: Productivity Press, 1989.

[16] Breyfogle FW. Implementing Six Sigma: smarter solutions using statistical methods, 2nd ed. New York: Wiley, 2003.

[17] Pyzdek T. The Six Sigma handbook revised and expanded: The complete guide for greenbelts, blackbelts, and managers at all levels, 2nd ed. New York: McGraw-Hill, 2003.

[18] Yang K., El-Haik B. Design for Six Sigma: A roadmap for product development. New York: McGraw-Hill, 2003.

[19] De Feo JA, Barnard WW. Juran institute's Six Sigma breakthrough and beyond: Quality performance breakthrough methods, New York: McGraw-Hill, 2004.

[20] Kapur KC, Feng Q. Integrated optimization models and strategies for the improvement of the Six Sigma process. International Journal of Six Sigma and Competitive Advantage 2005; 1(2).

[21] Kapur KC., Feng Q. Statistical methods for product and process improvement. In: Pham H, editor. Springer handbook of engineering statistics. London: Springer, 2006.

[22] Kane VE. Process capability indices. Journal of Quality Technology 1986; 18.
[23] Kotz S, Lovelace CR. Process capability indices in theory and practice. London: Arnold, 1998.
[24] Simon K. What is DFSS? [Online]. Available from: "https://www.isixsigma.com" [Accessed 10 December 2006].
[25] Kackar RN. Off-line quality control, parameter design and the Taguchi method. Journal of Quality Technology 1985; 17(4):176–90.
[26] Bendal A, Disney J, Pridmore WA. Taguchi methods: application in world industry. New York, NY: IFS Publications, Springer, 1989.
[27] Phadke MS. Quality engineering using robust design. Englewood Cliffs, NJ: Prentice-Hall, 1989.
[28] Wu Y, Wu A. Taguchi methods for robust design. New York: The American Society of Mechanical Engineers, 2000.
[29] Jiang W, Murphy TE, Tsui KL. Statistical methods for quality and productivity improvement. In: Pham H., editor. Springer handbook of engineering statistics. London: Springer, 2006.
[30] Kuehl RO. Statistical principles of research design and analysis. CA: Duxbury Press, 1994.
[31] Hicks CR, Turner KV. Fundamental concepts in the design of experiments, 5th ed. New York: Oxford University Press, 1999.
[32] Wu CFJ, Hamada M. Experiments: planning, analysis, and parameter design optimization. New York: Wiley, 2000.
[33] Montgomery DC. Design and analysis of experiments, 5th ed. New York: Wiley, 2001.
[34] Myers RH., Montgomery DC. Response surface methodology: process and product optimization using designed experiments. New York: Wiley, 2002.
[35] Koehler JR., Owen AB. Computer experiments. In: Ghosh S, Rao CR., editors. Handbook of statistics: Design and analysis of experiments. Amsterdam: Elsevier Science, 1996.
[36] Fang KT, Wang Y. Number-theoretic methods in statistics. London: Chapman and Hall, 1994.
[37] Nair VN. Taguchi's parameter design: A panel discussion. Technometrics 1992; 34:127–61.
[38] Chan LK., Xiao PH. Combined robust design. Quality Engineering 1995; 8:47–56.
[39] Li W, Wu CFJ. An integrated method of parameter design and tolerance design. Quality Engineering 1999; 11:417–25.
[40] Feng Q, Kapur KC. Tolerance design through variance transmission equations. International Journal of Reliability, Quality and Safety Engineering 2005; 12(5):413–38.
[41] Joseph VR, Wu CFJ. Operating window experiments: a novel approach to quality improvement. Journal of Quality Technology 2002; 34(4):345–54.
[42] Feng Q, Kapur KC. Economic development of specifications for 100% inspection based on asymmetric quality loss function. IIE Transactions 2006; 38(8):659–69.
[43] Feng Q, Kapur KC. Economic design of specifications for 100% inspection with imperfect measurement systems. Quality Technology and Quantitative Management 2006; 3(2):127–44.
[44] Kapur KC, Cho B. Economic design of the specification region for multiple quality characteristics. IIE Transactions 1996; 28:237–48.
[45] Western Electric, Statistical quality control handbook. Indianapolis, IN: Western Electric Corporation, 1956.
[46] ASTM Publication STP-15D, Manual on the presentation of data and control chart analysis. Philadelphia, PA, 1976.
[47] Chandra MJ. Statistical quality control. Boca Raton, FL: CRC Press LLC, 2001.
[48] Carey RG. Improving healthcare with control charts: basic and advanced SPC methods and case studies. Milwaukee, WI: ASQ Quality Press, 2003.
[49] Woodall WH, Mohammed MA, Lucas JM, Watkins R, *et al.* The use of control charts in health-care and public-health surveillance with discussions. Journal of Quality Technology 2006; 38(2):89–135.
[50] Box GEP, Jenkins GM, Reinsel GC. Time series analysis, forecasting, and control, 3rd ed. Englewood Cliffs, NJ: Prentice-Hall, 1994.
[51] Box GEP, Luceno A. Statistical control by monitoring and feedback adjustment. New York: Wiley, 1997.
[52] Hotelling H. Multivariate quality control. In: Eisenhart C, Hastay MW, and Wallis WA, editors. Techniques of statistical analysis. New York: McGraw Hill, 1947.
[53] Pignatiello JJ, Jr. Runger GC. Comparison of multivariate CUSUM charts. Journal of Quality Technology 1990; 22(3):173–186.
[54] Tracy ND, Young JC, Mason RL. Multivariate control charts for individual observations. Journal of Quality Technology 1992; 24(2):88–95.
[55] Duncan AJ. The economic design of charts used to maintain current control of a process. Journal of the American Statistical Association 1956; 51:228–42.
[56] Duncan AJ. Quality control and industrial statistics, 5th ed. Homewood, IL: Irwin, 1986.

[57] Montgomery DC. The economic design of control charts: a review and literature survey. Journal of Quality Technology 1980; 14:75–87.
[58] Stoumbos ZG, Reynolds MR, Ryan TP, Woodall WH. The state of statistical process control as we proceed into the 21st century. Journal of the American Statistical Association 2000; 95:992–98.
[59] Woodall, WH, Montgomery DC. Research issues and ideas in statistical process control. Journal of Quality Technology 1999; 31(4):376-86.
[60] Box GEP, Coleman DE, Baxley RV Jr. A comparison of statistical process control and engineering process control. Journal of Quality Technology 1997; 29(2):128–30.
[61] Montgomery DC, Keats JB, Runger GC, Messina WS. Integrating statistical process control and engineering process control. Journal of Quality Technology 1994; 26:79–87.
[62] Del Castillo E, Hurwitz AM. Run-to-run process control: literature review and extensions. Journal of Quality Technology 1997; 29(2):184–96.
[63] Del Castillo E, Pan R, Colosimo BM. A unifying view of some process adjustment methods. Journal of Quality Technology 2003; 35(3): 286–93.

14

Statistical Process Control

V.N.A. Naikan

Reliability Engineering Center, Indian Institute of Technology, Kharagpur – 721302, India

Abstract: Statistical process control (SPC) is a tool used for on-line quality control in mass production. Statistical sampling theory is effectively used for this purpose in the form of control charts. Various types of control charts have been developed in industry for controlling different types of quality characteristics. The basic principles of development, design and application of various types of control charts are discussed in this chapter. The state of the art and recent developments in SPC tools are included with references for further research. A separate section on process capability studies is also included.

14.1 Introduction

The concepts of quality are as old as human civilization. It has been a constant endeavor of any society or culture to design and develop finest pieces of quality in all walks of life. This is visible in many of the human made world wonders such as the Taj Mahal of India, the pyramids of Egypt, the high roads and sculptures of the Roman Empire, the finest paintings of Renaissance Europe, or the latest developments such as space shuttles, super computers, or atomic power generation. However, quality as a science or as a formal discipline has developed only during the 20th century. Quality has evolved through a number of stages such as inspection, quality control, quality assurance, and total quality control.

The concepts of specialization, standardization, and interchangeability resulted in mass production during the Second World War. This also changed the traditional concepts of inspection of individual products for quality control. It was found that applications of statistical principles are much more practical and beneficial in mass production. Statistical sampling theory, for instance, helped to minimize the need of resources for quality control with acceptable levels of accuracy and risk. The concept of statistical process control (SPC) has now been accepted as the most efficient tool for on-line quality control in mass production systems. SPC uses control charts as the main tool for process control. The control chart is one of the seven tools for quality control. Fishbone diagrams or Ishikawa diagrams check sheets, histograms, Pareto-diagrams, scatter diagrams, and stem and leaf plots are other tools. They are discussed in detail in [1]. This chapter focuses on SPC using control charts.

14.2 Control Charts

The control chart is a graphical tool for monitoring the activities of a manufacturing process. The

numerical value of a quality characteristic is plotted on the *Y*-axis against the sample number on the *X*-axis. There are two types of quality characteristics, namely variables and attributes. The diameter of shafts, the strength of steel structures, service times, and the capacitance value of capacitors are examples of variable characteristics. The number of deformities in a unit, and the number of nonconformities in a sample are examples of attribute quality characteristics. A typical control chart is shown in Figure 14.1.

As shown in this figure, there is a centerline to represent the average value of the quality characteristic. It shows where the process is cantered. The upper control limit (UCC) and the lower control limit (LCL) on the control chart are used to control the process. The process is said to be in statistical control if all sample points plot inside these limits. Apart from this, for a process to be in control the control chart should not have any trend or nonrandom pattern.

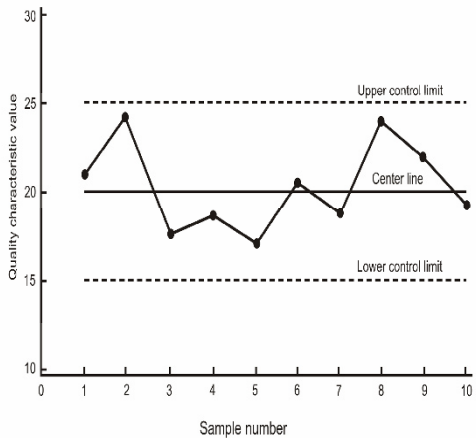


Figure 14.1. A typical control chart

14.2.1 Causes of Process Variation

Many factors influence the manufacturing process, resulting in variability. For example, variation in raw materials, skills of operators, capabilities of machines, methods, management policies, and many other factors including environmental variations affect the performance of a process. The causes of process variability can be broadly classified into two categories, *viz.*, assignable causes and chance causes.

Assignable Causes

If the basic reason for the occurrence of a cause of process variation can be found, then we list it under the category of assignable causes. Improper raw materials, usage of inappropriate cutting tools, carelessness of machine operators, *etc*., are examples of this. Such causes are also known as special causes. The basic purpose of using control charts is to identify the presence of assignable causes in the process and to eliminate these so as to bring back the process to statistical control.

Chance Causes

These are natural causes inherent in any process. The basic reasons for the occurrence of such causes cannot be correctly established. Elimination of such causes is also not possible in actual practice. A process is said to be out of control if any assignable cause is present in the process. Inherent material variations, operator skills, environmental conditions, and machine vibration are examples of chance causes. These are also known as common or random causes.

It is found that the assignable causes result in large variations in the process parameters whereas chance causes bring only small variations. It is reported that about 15% of the causes of variation are due to assignable causes and the remainder are due to chance causes for which only the management is accountable [2]. It is very important to remember that a process under statistical control will have some variations due to chance causes. In fact, the control limits are designed based on this principle.

Statistical Basis

Control charts are formulated based on the properties of the normal distribution [3]. The central limit theorem [1] states that if we plot the sample average of a process parameter, it will tend to have a normal distribution. The normal distribution is described by its parameters mean

(μ) and standard deviations (σ). For a normal distribution it can be shown that 99.74% of all points fall within the 3σ limits on either side of the mean. The upper and lower control limits of the control chart are determined based on this principle. This means that almost all the data points will fall within 3σ control limits if the process is free from assignable causes.

Errors in Control Charts

Two types of errors are associated with using the control charts. These are type I error and type II error. Type I error is the result of concluding that a process is out of control (based on actual data plotted on the chart) when it is actually in control. For a 3σ control chart this chance (α) is very small (about 0.0026). Type II error is the result of concluding that a process is in control (based on actual data plotted on the chart) when it is actually out of control. This may happen under many situations, such as the process mean changes from its initial setup, but all sample points fall within the control limits. The probability of type II error is generally represented by β and it is evaluated based on the amount of process change and the control limits. A plot of β *versus* the shifting process parameter is known as the operating characteristic (OC) curve of a control chart. The OC curve is a measure of the ability of a control chart to detect the changes in process parameters. A good control chart should have an OC curve as shown in Figure 14.2. For small changes in the process parameter, the probability of nondetection (β) by the control charts is high. For large changes in the process parameter, β should be small so that it is detected and corrected by the control chart.

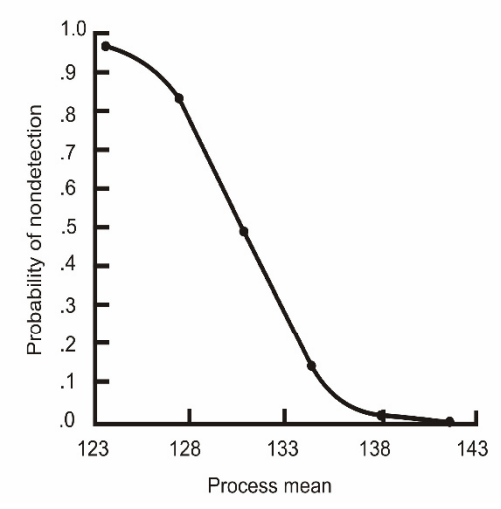


Figure 14.2. Typical OC curve for control charts

Average Run Length (ARL)

The average run length (ARL) is another measure of the performance of a control chart. It is the number of samples required to detect an out-of-control by a control chart. It is measured as reciprocal of type I error α.

$$ARL = \frac{1}{\alpha}.$$

For a 3σ control chart, $ARL = \left(\frac{1}{0.0026}\right) = 385$.

This shows that on an average one sample point is expected to fall out of 385 sample points outside the control limits. A large ARL is preferred since it produces fewer false alarms in a control chart.

Other Considerations

As mentioned earlier, control charts are plotted by taking small samples from the manufacturing process on a regular basis. Therefore, selection of sample size is very important in using the control charts.

Sample Size

It can be shown that a larger sample size results in narrow control limits. Decreasing the sample size makes the control limits wider. A larger sample size is needed if the small shift in the process parameter needs to be detected early. Apart from these factors the selection of sample size is influenced by the availability of resources, the types of tests used for sample evaluation, production rate, *etc*.

14.2.1.8 Frequency of Sampling

Theoretically it is most beneficial if we have more frequent large sample sizes. The type of inspection and the resource constraints are the main factors influencing the selection of these. In most practical situations a small sample size at frequent intervals is preferred.

Decision Rules for Control Charts

Five rules are used to detect when a process is going out of statistical control. These are briefly discussed below:

Rule 1: A process is going out of control if a single point plots outside the control limits.

Rule 2: A process is going out of control if two out of three consecutive points fall outside the 2σ warning limits on the same side of the centerline.

Rule 3: A process is going out of control if four out of five consecutive sample points fall outside the 1σ limits on the same side of the centerline.

Rule 4: A process is going out of control if nine or more consecutive points fall to one side of the centerline.

Rule 5: A process is going out of control if six or more consecutive sample points run up or down.

Applications of Control Charts

Control charts have several applications. This helps us in the following decision making:

1. To decide when to take corrective actions and when to leave the process as it is.
2. They give indications of type of remedial actions necessary to bring the process to control.
3. They help us to estimate the capability of our process to meet certain customer demands or orders.
4. They help us to improve quality.
5. They help us to take decisions such as the need for machine or technology replacement to meet quality standards.

Quality control and improvement are ongoing activities and, therefore, control charts must be maintained or revised as and when changes occur in the process. Installation of a new machine or application of a new technology necessitates the development of new control charts.

As mentioned earlier, the quality characteristics are broadly of two types. These are variables and attributes. Variable characteristics are continuous in their range where as attributes are discrete. Therefore, control charts are broadly classified into two categories, *viz.*, control charts for variables and for attributes.

14.3 Control Charts for Variables

Quality characteristics that can be measured on a numerical scale such as diameter of a shaft, length of a component, strength of a material and weight of a part are known as variables. Process control means controlling the mean as well as the variability of the characteristic. The mean of the variable indicates the central tendency and variability indicates the dispersion of the process. Variability is measured in terms of the range or standard deviation. Various types of control charts are discussed in the following sections.

14.3.1 Control Charts for Mean and Range

These charts are used to control the process mean and its variations. This is because the process control is ensured only if its mean is located correctly and its spread is kept within its natural limits. Therefore, these charts are used in pairs. The following steps are generally used for designing these control charts:

Step I: Decide the sampling scheme (sample size, number of samples, and frequency of sampling) and the quality characteristic to be controlled.

Step II: Collect the samples randomly from the process, measure the quality characteristic, and enter it into a data sheet. Let n be the sample size and X_i be the i-th observation, $i = 1...n$.

Step III: For each sample (j) calculate mean and range using the following equations ($j = 1...g$).

$$\overline{X}_j = \frac{\sum_{i=1}^{n} X_i}{n} \quad , \tag{14.1}$$

$$R_j = X_{j\max} - X_{j\min} \quad . \tag{14.2}$$

Step IV: Estimate the centerline (CL) and trial control limits for both mean and range charts using the following equations:

$$CL_{\overline{X}} = \overline{\overline{X}} = \frac{\sum_{j=1}^{g} \overline{X}_j}{g} \quad , \tag{14.3}$$

$$CL_R = \overline{R} = \frac{\sum_{j=1}^{g} R_j}{g} \quad , \tag{14.4}$$

$$\left(UCL_{\overline{X}}, LCL_{\overline{X}}\right) = \overline{\overline{X}} \pm A_2 \overline{R} \quad , \tag{14.5}$$

$$\left(UCL_R\right) = D_4 \overline{R} \quad , \tag{14.6}$$

$$LCL_R = D_3 \overline{R} \quad . \tag{14.7}$$

The values of A_2, D_3, D_4 depend on the sample size and can be taken from Appendix A-7 of [1].

Step V: Plot $\overline{X}_j$ and R_j on the control charts developed as per Step III. Check whether the process is in control as per the decision rules discussed earlier. If so, the control limits in Step III are final. Else revision of control limits by elimination of the out of control points is required. Repeat these steps for revision of control limits until final charts are obtained. The principle of development of other control charts is similar to the above methodology.

If the sample size is not constant from sample to sample, a standardized control chart can be used. The reader is referred to [4] and [5] for more details. Sometimes control charts are to be developed for specified standard or target values of mean and standard deviation. The reader is referred to [1] for the complete procedure for this. If a process is out of control assignable causes are present, which can be identified from the pattern of the control chart. AT & T [6] explains different types of control chart patterns that can be compared with the actual pattern to get an idea about "what" action is to be taken "when".

The effect of measurement error on the performance of $\overline{X}$ and S^2 charts is frequently quantified using gage capability studies [7], which are further investigated using a linear covariate [8]. Their study also identifies conditions under which multiple measurements are desirable and suggests a cost model for selection of an optimal mean. They also suggest taking multiple measurements per item to increase the statistical power of control charts in such cases.

14.3.2 Control Charts for Mean and Standard Deviation $\left(\overline{X}, S\right)$

Both range and standard deviation is used for measuring the variability. Standard deviation is preferred if the sample size is large (say $n > 10$). The procedure for construction of $\overline{X}$ and S charts is similar to that for $\overline{X}$ and R chart. The following formulas are used:

$$CL_s = \overline{S} = \frac{\sum_{j=1}^{g} S_j}{g} \quad , \tag{14.8}$$

$$UCL_s = B_4 \overline{S} \quad , \tag{14.9}$$

$$LCL_s = B_3 \overline{S} \quad . \tag{14.10}$$

The reader is referred to Appendix A-7 of [1] for the values of B_3 and B_4. $\overline{X}$ and S charts are sometimes also developed for given standard values [1].

14.3.3 Control Charts for Single Units (X chart)

In many practical situations we are required to limit the sample size to as low as unity. In such cases we use an X chart in association with a moving range (MR) chart. The moving range is the absolute value of the difference between successive observations. The assumption of normal distribution may not hold well in many cases of X and MR charts. The following formulas shown in Table 14.1 are used for developing the charts.

Table 14.1. Control limits for X and MR charts

Chart	CL	UCL	LCL
X	$\overline{X}$	$\overline{X} + 3\overline{MR}/d_2$	$\overline{X} - 3\overline{MR}/d_2$
MR	$\overline{MR}$	$D_4\overline{MR}$	$D_3\overline{MR}$

The values of d_2 depend on the sample size and can be taken from Appendix A-7 of [1]. These charts can also be developed for given standard values.

The control charts discussed so far are initially developed by Walter A Shewhart. Therefore, these charts are also known as Shewhart control charts [9]. Shewhart control charts are very easy to use and are very effective for detecting magnitudes of shifts from 1.5σ to 2σ or larger. However, a major limitation of these charts is their insensitivity to small shifts in process parameters, say about 1.5σ or less. To alleviate this problem a number of special charts have been developed. These are discussed in the following sections.

14.3.4 Cumulative Sum Control Chart (CUSUM)

These control charts are used when information from all previous samples need to be used for controlling the process. CUSUM charts are more effective in detecting small changes in the process mean compared to other charts discussed earlier.

The cumulative sum for a sample m is calculated by

$$S_m = \sum_{j=1}^{m} \left(\overline{X}_i - \mu_o\right) , \tag{14.11}$$

where μ_o is the target mean of the process. In this case CUSUM is plotted on the y-axis. The details of development and implementation of CUSUM charts are discussed in [10]. A V-mark is designed and developed for taking the decision on the process control while using these charts. A methodology to use CUSUM charts for detecting larger changes in process parameters is also available in this reference.

A comparative study of the performance based on the ARL of a moving range chart, a cumulative sum (CUSUM) chart based on moving ranges, a CUSUM chart based on an approximate normalizing transformation, a self-starting CUSUM chart, and an exponentially weighted moving chart based on subgroup variance is discussed in [11, 12]. The CUSUM chart is again compared with several of its alternatives that are based on the likelihood ratio test and on transformations of standardized recursive residual [13]. The authors conclude that the CUSUM chart is not only superior in the detection of linear trend out-of-control conditions, but also in the detection of other out-of-control situations. For an excellent overview of the CUSUM chart techniques the reader is referred to [14].

The adaptive CUSUM (ACUSUM) chart was proposed to detect a broader range of shifts on process mean [15]. A two-dimensional Markov chain model has also been developed to analyze the performance of ACUSUM charts [16]. This improves on the theoretical understanding of the ACUSUM schemes and also allows the analysis without running exclusive simulations. Moreover, a simplified operating function is derived based on an ARL approximation of CUSUM charts [16].

14.3.5 Moving Average Control Charts

These charts are also developed to detect small changes in process parameters. The moving average of width w for a sample number r is defined as:

$$M_r = \frac{\overline{X}_r + \overline{X}_{r-1} + \cdots\cdots + \overline{X}_{r-w+1}}{w} . \tag{14.12}$$

That means M_r is an average of latest w samples starting from the r-th sample. The control limits for this chart will be wider during the initial period and stabilize to the following limits after the first (w-1) samples:

$$CL = \overline{\overline{X}} , \tag{14.13}$$

$$\left(UCL, LCL\right) = \overline{\overline{X}} \pm \frac{3\sigma}{\sqrt{nw}} . \tag{14.14}$$

The initial control limits can be calculated by substituting r in place of w in these equations. Larger values of w should be chosen to detect shifts of small magnitudes. These charts can also be used when the sample size is unity.

14.3.6 EWMA Control Charts

The exponentially weighed moving average (EWMA) control chart was introduced in 1959 [17]. EWMA charts are also used for detecting shifts of small magnitudes in the process characteristics. These are very effective when the sample size is unity. Therefore, these are very useful for controlling chemical and process industries, in discrete part manufacturing with automatic measurement of each part, and in automatic on-line control using micro computers. EWMA is similar to MA, except that it gives higher weighting to the most recent observations. Therefore, the chances of detecting small shifts in process are better compared to the MA chart. These charts are discussed in details in [18–20], and [1]. The control limits of the EWMA chart are

$$CL = \overline{\overline{X}}\ , \tag{14.15}$$

$$(UCL, LCL) = \overline{\overline{X}} \pm 3\sigma \sqrt{\frac{p}{n(2-p)}\left[1-(1-p)^{2r}\right.} \tag{14.16}$$

where p is the weighing constant $(0 < p \le 1)$, and r is the sample number.

It may be noted that if p = 1, EWMA chart reduces to Shewhart chart and for $p = 2/(w+1)$, it reduces to MA chart. Selecting a small value of p (say 0.05) ensures faster detection of small shifts in process. These charts are also known as geometric moving average control charts.

As discussed earlier, violation of the assumption of independent data results in increased number of false alarms and trends on both sides on the centerline. A typical approach followed in the literature to study this phenomenon is to model the autocorrelated structure of the data and use a traditional control chart method to monitor the residuals. See [21–25], for more details. An alternative approach is the exponentially weighted moving average (MCEWMA) chart proposed in [26]. The literature also explores the shift detection capability of the moving centerline exponentially weighted moving average (MCEWMA) chart and recommends enhancements for quicker detection of small process upsets [27].

14.3.7 Trend Charts

In many processes the process average may continuously run either upward or downward after production of every unit of product. This is a natural phenomenon and therefore, it is an acceptable trend. Examples are effects of wearing of the punch, die, cutting tools or drill bits. However, such a trend in the process mean is acceptable only within some upper and lower limits (in most cases the specification limits). The trend charts are developed to monitor and control these types of processes. The centerline of the trend chart will have an upward or downward trend, and the upper and lower control limits will be parallel to the centerline. The intersection of centerline a and the slope b can be evaluated from the observations collected from the process [1]. The equations for the control limits are

$$CL = a + b_i\ , \tag{14.17}$$

$$UCL = (a + b_i) + A_2 \overline{R}\ , \tag{14.18}$$

$$LCL = (a + b_i) - A_2 \overline{R}\ . \tag{14.19}$$

These charts are useful for detecting changes in the process and also to decide whether or not a tool change is required. These charts are also known as regression control charts and are very helpful in controlling processes in machine shops and other production machines.

14.3.8 Specification Limits on Control Charts

If we want to include specification limits on the control charts, we require modification of the control limits. This is because the specification limits are defined on individual units where as most control charts are developed for sample average values. A simple methodology for finding the modified control limits is discussed in [1].

14.3.9 Multivariate Control Charts

The quality of a product is a function of many characteristics. For example, the length, diameter, strength, and surface finish among others contribute to the quality of a shaft. Therefore

controlling of all these variables is required to control the quality of the product. Multivariate control charts are developed to simultaneously control several quality characteristics. The procedure for development and application of multivariate control charts are discussed in detail in [1]. The T^2 distribution is used to develop the control chart and the F-distribution is used for finding the upper control limit [28]. The lower control limit is zero. The probability of type I error for this type of chart is very difficult to establish if the variables are dependent. If all the variables are independent then we can calculate this probability by the equation:

$$\alpha^* = 1-(1-\alpha)^p \quad , \tag{14.20}$$

where p is the number of independent variables.

Two phases in constructing multivariate control charts are defined, with phase I divided into two stages [29]. In stage I of phase I, historical observations are studied for determining whether the process was in control and to estimate the in-control parameters of the process. The T^2 chart of Hotelling is used in this stage as proposed in [30], and [31]. Control charts are used in stage II with future observations for detecting possible departures from the parameters estimated in the first stage. In the phase II charts are used for detecting any departures from the parameter estimates, which are considered the true in-control process parameters. A T^2 control chart based on robust estimators of location and dispersion is proposed in [32]. Using simulation studies the author shows that the T^2 control chart using the minimum volume ellipsoid (MVE) estimators is effective in detecting any reasonable number of outliers (multiple outliers).

Multiway principal components analysis (MPCA), a multivariate projection method, has been widely used for monitoring the batch process. A new method is proposed in [33] for predicting the future observation of the batch that is currently being operated (called the new batch). The proposed method, unlike the existing prediction methods, makes extensive use of the past batch trajectories.

The effect of measurement error on the performance of the T^2 chart is studied in [34]. For some multivariate nonnormal distributions, the T^2 chart based on known in-control parameters has an excessive false alarm rate as well as a reduced probability of detecting shifts in the mean vector [35]. The process conditions that lead to the occurrence of certain nonrandom patterns in a T^2 control chart are discussed in [36]. Examples resulting from cycles, mixtures, trends, process shifts, and auto correlated data are identified and presented. Results are applicable to a phase I operation or phase II operation where the T^2 statistics is based on the most common covariance matrix estimator. The authors also discuss the cyclic and trend patterns, effects of mixture of populations, process shifts and autocorrelated data on the performance of the T^2 chart.

A strategy for performing phase I analysis (of the multivariate control charts) for high-dimensional nonlinear profiles is proposed in [37]. This consists of two major components: a data reduction component that projects the original data into a lower dimension subspaces while preserving the data-clustering structure and a data-separation technique that can detect single and multiple shifts as well as outliers in the data. Simulated data sets as well as nonlinear profile signals from a forging process are used to illustrate the effectiveness of the proposed strategy.

Excellent reviews on the T^2 chart are presented in [38, 39]. Several useful properties of the T^2 statistics based on the successive difference estimator which give a more accurate approximate distribution for calculating the upper control limit individual observation in a phase I analysis are demonstrated in [40].The author discusses how to accurately determine the upper control limit for a T^2 control chart based on successive difference of multivariate individual observations.

A multivariate extension of the EWMA chart was proposed in [41]. This chart, known as MEWMA chart, is based on sample means and on the sum of squared deviations from the target. The performance of many of these control charts depends on the direction of the shifts in the mean vector or covariance matrix [42].

14.4 Control Charts for Attributes

Attribute characteristics resemble binary data, which can take only one of two given alternatives. In quality control, the most common attribute characteristics used are "conforming" or "not conforming", "good" or "bad". Attribute data need to be transformed into discrete data to be meaningful.

The types of charts used for attribute data are:

- Control chart for proportion nonconforming items (*p* chart)
- Control chart for number of nonconforming items (*np* chart)
- Control chart for nonconformities (*c* chart)
- Control chart for nonconformities per unit (*u* chart)
- Control chart for demerits per unit (*U* chart)

A comprehensive review of the attribute control charts is presented in [43]. The relative merits of the *c* chart compared to the X chart for the Katz family covering equi-, under-, and over-dispersed distributions relative to the Poisson distribution are investigated in [44]. The Katz family of distributions is discussed in [45]. The need to use an X chart rather than a *c* chart depends upon whether or not the ratio of the in control mean is close to unity. The X chart, which incorporates the information on this ratio, can lead to significant improvements under certain circumstances. The c chart has proven to be useful for monitoring count data in a wide range of application. The idea of using the Katz family of distribution in the robustness study of control charts for count data can be extended to the cumulative sum (CUSUM) and exponentially weighted moving average (EWMA) chart.

The *p* and *np* charts are developed based on binomial distribution, the *c*, *u*, and *U* charts are based on Poisson distribution. These charts are briefly discussed in this section.

14.4.1 The *p* chart

The *p* chart is used when dealing with ratios, proportions or percentages of nonconforming parts in a sample. Inspection of products from a production line is a good example for application of this chart. This fulfils all the properties of binomial distribution. The first step for developing a *p* chart is to calculate the proportion of nonconformity for each sample. If *n* and *m* represent the sample size and number of nonconforming items in the sample, then the fraction of nonconforming items *p* is given by:

$$p = \frac{m}{n}. \tag{14.21}$$

If we take g such samples, then the mean proportion nonconforming $\overline{p}$ is given by:

$$\overline{p} = \frac{p_1 + p_2 + ... + p_g}{g}. \tag{14.22}$$

The centerline and the 3σ limits of this chart are as follows:

$$CL = \overline{p}\ , \tag{14.23}$$

$$UCL = \overline{p} + 3\sqrt{\frac{\overline{p}(1-\overline{p})}{n}}\ , \tag{14.24}$$

$$LCL = \overline{p} - 3\sqrt{\frac{\overline{p}(1-\overline{p})}{n}}\ . \tag{14.25}$$

In many situations we may require to develop p-charts with variable sample size. In such situations control charts can be developed either for individual samples or for a few representative sample sizes. A more practical approach is to develop a standardized chart. For this a standardized value z of p for each sample is calculated as follows:

$$z_i = \frac{p_i - \overline{p}}{\sqrt{\overline{p}(1-\overline{p})/n_i}}\ . \tag{14.26}$$

z_i is then plotted on the chart. This chart will have its centerline at zero and the control limits of 3 on either side. A number of rules are developed for decision making on the out-of-control situations. Different types of p-charts and the decision rules are discussed in more detail in [1] and [5]. A p chart has the capability to combine information from many departments, product lines, and work centers and provide an overall rate of product nonconformance.

14.4.2 The *np* chart

The *np* chart is similar to the *p* chart. It plots the number of nonconforming items per sample. Therefore it is easier to develop and use compared to the *p* chart. While the *p* chart tracks the proportion of nonconformities per sample, the *np* chart counts the number of defectives in a sample. The binomial distribution can be used to develop this chart. The mean number of nonconformities in a sample is *np*.

The centerline and the control limits for an *np*-chart are as follows:

$$CL = n\bar{p}, \tag{14.27}$$

$$UCL = n\bar{p} + 3\sqrt{n\bar{p}(1-\bar{p})}, \tag{14.28}$$

$$LCL = n\bar{p} - 3\sqrt{n\bar{p}(1-\bar{p})}. \tag{14.29}$$

np charts are not used when the sample size changes from sample to sample. This is because the centerline as well as the control limits are affected by the sample size. Using and making inferences in such cases are very difficult.

14.4.3 The *c* chart

The *c* chart monitors the total number of nonconformities (or defects) in samples of constant size taken from the process. Here, nonconformance must be distinguished from defective items since there can be several nonconformances on a single defective item. For example a casting may have many defects such as foreign material inclusion, blow holes, hairline cracks, *etc*. Other examples are the number of defects in a given length of cable, or in a given area of fabric. Poisson distribution is used to develop this chart. If the sample size does not change and the defects on the items are fairly easy to count, the *c* chart becomes an effective tool to monitor the quality of the production process.

If $\bar{c}$ is the average number of nonconformities per sample, then the centerline and the 3σ control limits of the *c* chart are:

$$CL = \bar{c}, \tag{14.30}$$

$$UCL = \bar{c} + 3\sqrt{\bar{c}}, \tag{14.31}$$

$$LCL = \bar{c} - 3\sqrt{\bar{c}}, \tag{14.32}$$

14.4.4 The *u* chart

One of the limitations of the *c* chart is that it can be used only when the sample size remains constant. The *u* chart can be used in other cases. It can be effectively used for constant as well as for variable sample size. The first step in creating a *u* chart is to calculate the number of defects per unit for each sample,

$$u_i = \frac{c_i}{n_i}, \tag{14.33}$$

where *u* represents the average defect per sample, *c* is the total number of defects, *n* is the sample size and *i* is the index for sample number. Once all the averages are determined, a distribution of the means is created and the next step will be to find the mean of the distribution, in other words, the grand mean.

$$\bar{u} = \frac{\sum_{i=1}^{g} c_i}{\sum_{i=1}^{g} n_i}, \tag{14.34}$$

where *g* is the number of samples. The control limits are determined based on $\bar{u}$ and the mean of the samples *n,*

$$UCL = \bar{u} + 3\sqrt{\bar{u}/n_i}, \tag{14.35}$$

$$LCL = \bar{u} - 3\sqrt{\bar{u}/n_i}. \tag{14.36}$$

Furthermore, for a *p* chart or an *np* chart the number of nonconformances cannot exceed the number of items on a sample, but for a *u* chart, it is conceivable since what is being addressed is not the number of defective items but the number of defects in the sample.

14.4.5 Control Chart for Demerits *per* Unit (*U* chart)

One of the deficiencies of the *c* and *u* charts is that all types of nonconformities are treated equally. In actual practice there are different types of nonconformities with varying degrees of severity. ANSI/ASQC Standard A3 classifies the nonconformities into four classes, *viz.*, very serious, serious, major, and minor, and proposes a

weighing system of 100, 50, 10, and 1, respectively. The total number of demerits (D) for a sample is therefore calculated as the weighed sum of nonconformities of all types as follows:

$$D = w_1 c_1 + w_2 c_2 + w_3 c_3 + w_4 c_4 \ . \qquad (14.37)$$

The demerits per sample (U) is defined as $U = D/n$ where n is the sample size. The center line of the control chart is given by:

$$CL = \overline{U} = w_1 \overline{u_1} + w_2 \overline{u_2} + w_3 \overline{u_3} + w_4 \overline{u_4} \ , \qquad (14.38)$$

where $\overline{u_i}$ represent the average number of nonconformities per unit in the i-th class. The control limits of the chart are:

$$UCL = \overline{U} + 3\sigma_U \ , \qquad (14.39)$$

$$LCL = \overline{U} - 3\sigma_U \ , \qquad (14.40)$$

where

$$\sigma_U = \sqrt{\left(w_1^2 \overline{u_1} + w_2^2 \overline{u_2} + w_3^2 \overline{u_3} + w_4^2 \overline{u_4}\right)/n} \ . \qquad (14.41)$$

For a detailed discussion on the U hart the reader is referred to [1].

As mentioned earlier, the success of using control charts for process control depends to a great extent on the observed data. Data must be independent of one another to ensure the random phenomenon. If this is not strictly ensured, the data will be autocorrelated and the inferences on process control based on the control charts will be misleading. In actual practice there is a chance of some level of autocorrelation of the data. Therefore, dealing with autocorrelated data has been a research problem in SPC. Many useful ideas have been developed and published on this topic.

A model for correlated quality variables with measurement error is presented in [46]. It is shown that the performance of multivariate control charting methods based on measured covariates is not directionally invariant to shifts in the mean vector of the underlying process variables, even though it may be directionally invariant when no measurement error exists. For further information on the directional invariance of multivariate control charts the reader is referred to [41, 47, 48], and [49].

The traditional control charts become unreliable when the data are autocorrelated [50]. In the literature the reverse moving average control chart is proposed as a new forecast-based monitoring scheme, compare the new control chart to traditional methods applied to various ARMA(1,1), AR(1), MA(1) processes, and make recommendations concerning the most appropriate control chart to use in a variety of situations when charting autocorrected processes [51].

Many new types of control charts have been proposed in the recent literature to handle different types of data. The proportional integral derivative (PID) chart for monitoring autocorrelated processes based on PID predictors and corresponding residuals is introduced in [52]. The PID charting parameter design, the mean shift pattern analysis, and the relationship between the average run length performance and PID parameter selection are also discussed extensively in the literature. Improved design schemes are suggested for different scenarios of autocorrelated processes and verified with Monte Carlo simulation. This study provides useful information for practitioners to effectively apply PID charts. See [53–56] for further discussions on autocorrelation of data in control charts.

The cumulative conformance count (CCC) chart was introduced as a Six Sigma tool to deal with controlling high-yield processes (see [57]). CCC chart was first introduced in [58] and became popular through [59]. It is primarily designed for processes with sequential inspection carried out automatically one at a time. A control scheme that is effective in detecting changes in nonconforming fractions for high yield processes with correlation within each inspection group is followed in [60]. A Markov model is used to analyze the characteristics of the proposed schemes in terms of which the average run length (ARL) and average time signal (ATS) are obtained. The performance of the proposed schemes in terms of ATS is presented along with the comparison with the traditional cumulative conformance count (CCC) chart. Moreover, the effects of correlation and group size are also investigated by the authors. The authors also have proposed a control scheme, the C^4-chart for monitoring high-yield high volume

production/process under group inspection with consideration of correlation within each group. Circumstances that lead to group inspection include a slower inspection rate than the production rate, economy of scale in group inspection, and strong correlation in the output characteristics.

Many applications and research opportunities available in the use of control charts for health-care related monitoring are reported in [61]. The advantage and disadvantage of the charting methods proposed in health care and public health areas are considered. Some additional contribution in the industrial statistical process control literature relevant to this area are given. Several useful references in the related areas are listed in this paper. This shows that the application of SPC for health care systems has become increasingly popular in recent times.

14.5 Engineering Process Control (EPC)

In recent times EPC has been used to control the continuous processes manufacturing discrete parts. It is also known as automatic process control (APC) in which an appropriate feedback or feedforward control is used to decide when and by how much the process should be adjusted to achieve the quality target. It is an integrated approach in which the concepts of design of experiments and robust design are also effectively used for designing control charts. EPC has been developed to provide an instantaneous response, counteracting changes in the balance of a process and to apply corrective action to bring the output close to the desired target. The approach is to forecast the output deviation from target that would occur if no control action were taken and then to act so as to cancel out this deviation [62].

14.6 Process Capability Analysis

Process capability represents the performance of a process when it is in a state of statistical control. It is measured as the total process variability when only common causes are present in the system. The process spread 6σ is generally taken as a measure of the process capability. 99.74% of all products will be within this spread if the normality assumption is valid. In many situations we are required to check if our existing process is capable of meeting certain product specifications. Such decisions are taken based on the process capability indices (PCI). The following PCI are generally used.

14.6.1 Process Capability Indices

This relates the process spread to the specification spread as follows:

$$C_p = \frac{USL - LSL}{6\sigma}. \qquad (14.42)$$

where *USL* and *LSL* are the upper and lower specification limits. From the above equation it can be seen that the process is capable when $C_p > 1$. However, C_p is not a good measure since it does not take care of the location of the center of the process. C_p represents only the process potential. Therefore other PCI such as upper capability index (*CPU*), lower capability index (*CPL*), C_{pk} and C_{pm} are also developed for such studies. They are defined as follows:

$$CPU = \frac{USL - \mu}{3\sigma}, \quad CPL = \frac{\mu - LSL}{3\sigma}, \quad \text{and}$$

$$C_{pk} = Min\{CPU, CPL\}. \qquad (14.43)$$

Since C_{pk} also takes into account the position of the centerline of the process (μ), it represents the actual process capability of the process with the present parameter values. Taguchi proposed and used another index, *viz.*, C_{pm} [63, 64]. The author emphasizes the need to reduce the process variability around a target value *T*. C_{pm} is defined as follows.

$$C_{pm} = \frac{USL - LSL}{6\tau}, \qquad (14.44)$$

where τ is the standard deviation from the target value and is calculated by

$$\tau^2 = E\left[(X - T)^2\right] . \quad (14.45)$$

Combining the merits of these indices, a more advanced index, C_{pmk}, is proposed that takes into account process variation, process centering, and the proximity to the target value, and has been shown to be a very useful index for manufacturing processes with two-sided specification limits. The behavior of C_{pmk} as a function of process mean and variation is discussed in [65]. If the variation of the process increases, the maximum value of C_{pmk} moves from near the target value to the midpoint of the specification. If the process mean varies inside the specification, C_{pmk} decreases as the variation increases. It is argued that these properties may constitute a sensible behavior of the process capability index. For an extensive study on process capability the reader is referred to [66–68].

In many situations we may require to compare several processes based on process capability. If there are two processes, the classical hypothesis testing theory can be applied as suggested in [69, 70]. A bootstrap method for similar studies is proposed in [71]. When there are more than two processes, the best subset selection method proposed in [72–76] can be effectively used. A solutions to this problem based on permutation testing methodology is proposed in [77]. In the case of two processes, the methodology is based on a simple permutation test of the null hypothesis that the two processes have equal capability. In the case of more than two processes, multiple-comparison techniques are used in conjunction with the proposed permutation test. The advantage of using the permutation methods is that the significance levels of the permutation tests are exact regardless of the distribution of the process data. The methodology is demonstrated using several examples, and the potential performance of the methods are investigated empirically.

References

[1] Mitra A. In: Fundamentals of quality control and improvement. Pearson Education Asia, 2001.

[2] Deming W Edwards. In: Quality, productivity, and competitive position. Cambridge, Mass: Center for Advanced Engineering Study, MIT, 1982.

[3] Duncan AJ. In: Quality control and industrial statistics. 5th Edition, Homewood, III: Richard D Irvin, 1986.

[4] Nelson LS. Standardization of control charts. Journal of Quality Technology 1989; 21(4):287–289.

[5] Nelson LS. Shewart control charts with unequal subgroup sizes. Journal of Quality Technology 1994; 26(1): 64–67.

[6] AT&T, Statistical Quality Control Handbook, 10th printing, 1984.

[7] Montgomery DC, Runger GC. Gauge capability and designed experiments. Part 1: Basic methods. Quality Engineering 1994; 6:115–135.

[8] Linna KW, Woodall WH, Busby KL. The performance of multivariate control charts in the presence of measurement errors. Journal of Quality Technology 2001; 33:349–355.

[9] Nelson LS. The Shewart control chart tests for special causes. Journal of Quality Technology 1984; 16 (4): 237–239.

[10] Lucas JM. The design and use of V-mask control schemes. Journal of Quality Technology 1976; 8(1):1–12.

[11] Cesar A Acosta-Mejia, Joseph J Pignatiello Jr. Monitoring process dispersion without subgrouping. Journal of Quality Technology 2000; 32 (2):89–102.

[12] Klein Moton. Two alternatives to the Shewhart X-bar control chart. Journal of Quality Technology 2000; 32(4):427–431.

[13] Koning Alex J, Does Ronald JMM. CUSUM chart for preliminary analysis of individual observation. Journal of Quality Technology 2000; 32(2):122–132.

[14] Hawkins DM, Olwell DH, Cumulative sum charts and charting for quality improvement. Springer, New York, NY, 1998.

[15] Sparks RS. CUSUM charts for signaling varying location shifts. Journal of Quality Technology 2000;32:157–171.

[16] Shu Lianjie, Wei Jiang. A Markov chain model for the adaptive CUSUM control chart. Journal of Quality Technology 2006; 38(2): 135–147.

[17] Roberts SW. Control chart tests based on geo-metric moving averages. Technometrics 1959; 1.

[18] Crowder SV. Design of exponentially weighed moving average schemes. Technometrics 1987; 21.
[19] Crowder SV. A simple method for studying run length distributions of exponentially weighed moving average charts. Technometrics 1989;29.
[20] Lucas JM, Saccussi MS. Exponentially weighed moving average control schemes: Properties and enhancements. Technometrics 1990;32.
[21] Alwan LC, Roberts HV. Time series modeling for statistical process control. Journal of Business and Economic Statistics 1988;6 (1):87–95.
[22] Alwan LC. Radson D. Time series investigation of sub sample mean charts. IIE Transactions 1992; 24(5): 66–80.
[23] Montgomery DC, Friedman DJ. Statistical process control in a computer- integrated manufacturing environment. In: Keats JB, Hubele NF, editors. Statistical process control in automated manufacturing. Marcel Dekker, New York, 1989.
[24] Yourstone SA, Montgomery DC. Development of a real time statistical process control algorithm. Quality and Reliability Engineering International 1989; 5:309–317.
[25] Notohardjono BD, Ermer DS. Time Series control charts for correlated and contaminated data. Journal of Engineering for Industry 1996; 108: 219–225.
[26] Montgomery DC, Mastrangelo CM. Some statistical process control methods for autocorrelated data. Journal of Quality Technology 1991; 23: 179–193.
[27] Mastrangelo Christrina M, Brown Evelyn C. Shift detection properties of moving centerline control chart schemes. Journal of Quality Technology 2000; 32 (1):67–74.
[28] Hoteling H. Multivariate quality control. In: Eisenhart C, Hastny MW, Wallis WA, editors. Techniques of statistical analysis. McGraw Hill, New York, 1947.
[29] Alt FB. Multivariate quality control. In: Katz S, .Johnson NL, editors. Encyclopedia of statistical sciences. Wiley, New York, 1985; 6.
[30] Alt FB, Smith ND. Multivariate process control. In: Krishnaiah PR, Rao CR, editors. Handbook of statistics. North-Holland, Amsterdam, 1988; 7: 333–351.
[31] Tracy ND, Young JC, Mason RL. Multivariate control charts for individual observations. Journal of Quality Technology 1992; 24: 88–95.
[32] Vargas Jose Alberto N. Robust estimation in multivariate control charts for individual observations. Journal of Quality Technology 2003; 35(4): 367–376.
[33] Cho Hyun-Woo, Kim Kwang-Jae. A method for predicting future observations in the monitoring of a batch process. Journal of Quality Technology 2003; 35(1): 59–69.
[34] Linna Kenneth W, Woodall William H, Busby Kevin L. The performance of multivariate control charts in the presence of measurement error. Journal of Quality Technology, 2001; 33(3):349–355.
[35] Stoumbos ZG, Sullivan JH. Robustness to nonnormality of the multivariate EWMA control chart. Journal of Quality Technology 2002; 34: 260–276.
[36] Mason Robert L, Chou Youn-Min, Sullivan Joe H, Stoumbos Zachary G, Young John C. Systematic pattern in T^2 chart. Journal of Quality Technology 2003; 35(1):47–58.
[37] Ding Yu, Zeng Li, Zhou Shiyu. Phase I analysis for monitoring nonlinear profiles in manufacturing processes. Journal of Quality Technology 2006; 38(3):199–216.
[38] Fuchs C, Kenett RS. Multivariate quality control: theory and applications. Marcel Dekker, New York, 1998.
[39] Mason RL, Young JC. Multivariate statistical process control with industrial applications. SIAM, Philadelphia, PA, 2002.
[40] Woodall William H. Rejoinder. Journal of Quality Technology 2006; 38(2):133–134.
[41] Lowry CA, Woodall WH, Champ CW, Rigdon SE. A multivariate exponentially weighted moving average control chart. Technometrics 1992; 34: 46–53.
[42] Reynolds Jr. Marion R, Cho Gyo-Young. Multivariate control chart for monitoring the mean vector and covariance matrix. Journal of Quality Technology 2006; 38 (3):230–253.
[43] Woodall WH. Control charting based on attribute data: Bibliography and review. Journal of Quality Technology 1997; 29:172–183.
[44] Fang Yue. C-chart, X-chart, and the Katz family of distributions. Journal of Quality Technology 2003; 35(1):104–114.
[45] Katz L. Unified treatment of a broad class of discrete probability distributions. Proceedings of the International Symposium on Discrete Distributions, Montreal, Canada 1963.
[46] Linna Kenneth W, Woodall William H. Effect of measurement error on Shewhart control charts. Journal of Quality Technology 2001; 33(2):213–222.
[47] Mason, RL, Champ CW, Tracy ND, Wierda SJ, Young, JC. Assessment of multivariate process

control techniques. Journal of quality technology 1997; 29:140–143.

[48] Pignatiello JJ Jr., Runger GC. Comparisons of multivariate CUSUM charts. Journal of Quality Technology 1990; 22:173–186.

[49] Lowry CA, Montgomery DC. A review of multivariate control charts. IIE Transactions 1995; 27:800–810.

[50] Maragah HD, Woodall WH. The effect of autocorrelation on the retrospective X-chart. Journal of Statistical Computation and Simulation, 1992; 40:29–42.

[51] Dyer John N, Benjamin M Adams, Michael D Conerly. The reverse moving average control chart for monitoring autocorrelated processes. Journal of Quality Technology 2003; 35(2):139–152.

[52] Jiang W, Wu H, Tsung F, Nair VN, Tsui KL. Proportional integral derivative charts for process monitoring. Technometrics 2002; 44:205–214.

[53] Shu L, Apley DW, Tsung F. Autocorrelated process monitoring using triggered cuscore charts. Quality and Reliability Engineering International 2002; 18:411–421.

[54] Apley DW, Tsung F. The autoregressive T^2 chart for monitoring univariate autocorrelated processes. Journal of Quality Technology 2002; 34:80–96.

[55] Castagliola P, Tsung, F. Autocorrelated statistical process control for non normal situations. Quality and Reliability Engineering International 2005; 21:131–161.

[56] Tsung Fugee, Zhao Yi, Xiang Liming, Jiang Wei. Improved design of proportional integral derivative charts. Journal of Quality Technology 2006; 38(1):31–44.

[57] Goh TN. Xie M. Statistical control of a Six Sigma process. Quality Engineering 2003; 15:587–592.

[58] Calvin TW. Quality control techniques for 'Zero defects. IEEE Transactions on Components, Hybrids, and Manufacturing Technology CHMT 1983; 6:323–328.

[59] Goh, T.N., A Control Chart for Very High Yield Processes. Quality Assurance, 1987, 13: 18–22.

[60] Tang Loon-Ching, Cheong Wee-Tat. A control scheme for high-yield correlated production under group inspection. Journal of Quality Technology 2006; 38(1):45–55.

[61] Woodball Wiiliam H. The use of control chart in health-care and public-health surveillance. Journal of Quality Technology 2006; 38(2):89–104.

[62] Jin J, Ding Y. Online automatic process control using observable noise factors for discrete-part manufacturing. IIE Transactions 2004; 36:899–911.

[63] Taguchi G. A tutorial on quality control and assurance–the Taguchi methods. ASA Annual meeting, Las Vegas, 1985.

[64] Taguchi G. Introduction to quality engineering. Asian productivity organization, Tokyo, 1986.

[65] Jessenberger Jutta, Weihs Claus. A note on the Behavior of C_{pmk} with asymmetric specification limit. Journal of Quality Technology 2000; 32(4):440–443.

[66] Pignatiello JJ. Process capability indices: Just say 'no!' Annual Quality Congress Transactions 1993; 92–104.

[67] Gunter BH. The use and abuse of Cpk: Parts 1–4. Quality Progress 1989; 22(1):72–73; 22(2):108–109; 22(5):79–80; 86–87.

[68] Polansky AM. Supplier selection based on bootstrap confidence regions of process capability indices. International Journal of Reliability, Quality and Safety Engineering 2003; 10:1–14.

[69] Chou YM, Owen DB. A likelihood ratio test for the equality of proportions of two normal populations. Communications in Statistics Theory and Methods 1991; 20:2357–2374.

[70] Chou YM. Selecting a better supplier by testing process capability indices. Quality Engineering 1994; 6:427–438.

[71] Chen JP, Chen KS. Comparing the capability of two processes using Cpm. Journal of Quality Technology 2004; 36:329–335.

[72] Tseng ST, Wu TY. Selecting the best manufacturing process. Journal of Quality Technology 1991; 23: 53–62.

[73] Huang DY, Lee RF. Selecting the largest capability index from several quality control processes. Journal of Statistical Planning and Inference 1995; 46:335–346.

[74] Polansky AM, Kirmani SNUA. Quantifying the capability of industrial processes. In: Khattree B, Rao CR, editors. Handbook of Statistics. Elsevier Science, Amsterdam, 2003; 22: 625–656.

[75] Daniels L, Edgar B, Burdick RK, Hubele NF. Using confidence intervals to compare process capability indices. Quality Engineering 2005; 17:23–32.

[76] Hubele NF, Bernado A, Gel ES. A Wald test for comparing multiple capability indices. Journal of Quality Technology 2005; 37:304–307.

[77] Polansky Alan M. Permutation method for comparing process capabilities. Journal of Quality Technology 2006; 38(3):254–266.

15

Engineering Process Control: A Review

V.K. Butte and L.C. Tang

Department of Industrial & Systems Engineering
National University of Singapore
1, Engineering Drive 2, Singapore 117576

Abstract: The chapter provides an overview of engineering process control (EPC). The need for EPC and earlier misconceptions about process adjustments are discussed. A brief overview of time series is provided to model process disturbances. Optimal feedback controllers considering the various costs involved such as off-target costs, adjustment costs and sampling costs are discussed. Further, optimal control strategies in the case of short production runs and adjustment errors are also discussed. This is followed by an overview of run-to-run control in the semiconductor industry. First the most widely used single-EWMA controllers are detailed and then their weakness and the need for double EWMA controllers are discussed. Double-EWMA is detailed and its transient and steady state performances are also discussed. Further, the need for variable EWMA and initial intercept iteratively adjusted (IIIA) controllers are pointed out and elaborated on. The chapter then addresses some criticism of EPC and responses to it. Finally the integration of SPC and EPC for greater benefits is discussed.

15.1 Introduction

15.1.1 Process Control in Product and Process Industries

In product based industries the objective is to keep the quality characteristics as close as possible to the desired target. The exact conformance to the target value is not achievable since there are many factors affecting the manufacturing process and causing deviation from target. The objective is achieved by statistical process control (SPC), which involves the plotting and interpretation of control charts. The quality characteristics of the process such as the mean of a continuous process, nonconformities or percent nonconformities are monitored on a chart sampling of the process over time. A centerline and control limits are established using the process measurements. As long as the measurement falls within the control limits, no action is taken. Whenever the process measurement exceeds the control limits, a search for the assignable causes begins. SPC takes a binary view of the condition of a process; the process is either running satisfactorily or not. The purpose is to differentiate between inevitable random causes and assignable causes in the process. If random causes alone are at work, the process is continued. If assignable causes are present, the process is stopped to detect and eliminate them. SPC tools such as Shewhart

control charts, exponential weighted moving average (EWMA) charts and cumulative sum (CUSUM) charts are employed for this purpose.

EPC is used in process control of continuous production processes. EPC is a collection of techniques to manipulate the adjustable variables of the process to keep the output of the process as close to the target as possible. The aim of engineering process control is to provide an instantaneous response, counteracting changes in the balance of a process and to apply corrective action to bring the output close to the desired target. The approach is to forecast the output deviation from target, which would occur if no control action were taken and then to act so as to cancel out this deviation. The control is achieved in EPC by an appropriate feedback or feedforward control that indicates when and by how much the process should be adjusted to achieve the objective.

In this chapter we shall study EPC for product industries. The quality objective of the process is met by systematic application of the feedback process adjustment. The first step in feedback adjustment is to build a predictive model for the process determining how process output and input are related. This is an important task as it provides the basis for a good adjustment policy. Design of experiment (DOE) and response surface methedology are initially used offline to construct the process predictive model. In this chapter control variables are assumed to be available and responsive processes are considered, in which the dynamic behavior of the output is only due to disturbance dynamics and the control excercised comes into full effect immediately. In such descrete part manufacturing problems, the control factor will typically be the machine set point. The change in steady state output that will be obtained by unit change in input is called gain. The value of the gain is obtained offline after conducting designed experiments and regression techniques before proceeding to process adjustment. The literature available on process adjustment can be broadly classified according to the problems addressed:

- Feedback adjustment for machine tool problems
- Setup adjustment problems
- Run-to-run process control in application to the semiconductor industry

Machine tool problems address the processes that are affected by disturbances, the setup problems address processes that are offset during initial setting up, while run-to-run problems address the processes affected by process disturbance and are also offset.

15.1.2 The Need for Complementing EPC-SPC

Though SPC and EPC have been developed in different fields for respective objectives, they can be a good compliment to each other as both share the objective of reduction of variability. The following points highlight the need for process adjustment in the product manufacturing industry:

1. Practical production environments are nonstationary and the process is subject to occasional shifts. Though the causes of the shifts are known, it may be either impossible or uneconomical to remove them. A few examples are raw material variability, change of process behavior due to maintenance, variation in ambient temperature and humidity, *etc*. Such sources of variability are unavoidable and cannot be eliminated from process monitoring alone. Process adjustment can be applied to minimize process variability in such circumstances.
2. A process may undergo slow drift. The drift might be due to known causes such as build up of deposition inside a reactor, ageing of components, *etc.*, which cannot be precisely identified. SPC alone is not well suited to control a process with slow drift. With no interference in control process, the process must drift a certain distance before a control action is taken in response to an alarm. If the product's off-target cost is high or the adjustments are inexpensive, there is no need to wait for a long time to observe out of limit points and take control action.

3. In few processes the state of statistical control may be an ideal case and difficult to achieve or it is difficult to tell if the process is in statistical control. In these cases it is beneficial to have mild control with process adjustment.
4. Process adjustment alone is not suited to eliminate special causes that may affect the process. When special causes occur, such as a sudden change in environment conditions or mistakes in readings, *etc.*, process adjustment alone will not handle such situations. It will result in off-target bias and increase variability of output. Process monitoring may be utilized to detect assignable causes.

Hence the objective on quality requirement can be better realized by integrating SPC and EPC. This is especially true in these contemporary times where the hitherto border line between product and process based industries have faded. There are several industries where a combination of product and process manufacturing techniques are employed. The semiconductor manufacturing industry is one such industry. High quality products are required for technical and market reasons. Process monitoring coupled with process adjustment will form a better tool to achieve process control and high quality.

The control steps are as follows:

1. Detect the process performance from a stable process.
2. Identify the assignable cause of variation with the help of control charts and remove them.
3. If all the assignable causes cannot be removed economically, find a variable to adjust the process so as to maintain quality characteristics as close to the target as possible.

15.1.3 Early Arguments Against Process Adjustments and Contradictions

In the past statisticians and process engineers adhered to the notions of "do not interfere with the process that is in statistical control". They shunned the idea of process adjustment. Such a notion was also advocated by Deming through what is popularly known as Deming's funnel experiment [1]. The experiment was conducted by monitoring a funnel over a target bull's eye placed on a flat surface. The marbles were continuously dropped through a funnel and their position with respect to the target was measured. The aim was to keep the balls on target with minimum variance. The position of the funnel relative to target can be adjusted from drop to drop. Deming studied the effect of no adjustments to adjustments on the variance of the process. He found that the strategy of no adjustment produced minimum variance and the process remained on target. Deeper insights on the experiment can be obtained by understanding the assumptions made in the experiment, which were as follows:

1. The process producing deviation from target is in statistical control.
2. The process is initially on target.
3. It is possible to aim the funnel at the target.

The same experiment was further analyzed and useful information was obtained [2]. The process on target and statistical control should not be adjusted. However, if the uncontrolled process exhibits autocorrelation the feedback control rules would prove beneficial. For a nonstationary process the mean itself is moving, if left uncontrolled the mean will move away from the target, hence feedback control is needed. This case is analogous to the moving bull's eye in the funnel experiment, keeping the funnel fixed is not the best alternative.

The process variance would double if we apply full adjustment equal to deviation on a process that is in statistical control. Policy of adjustment would be better if the process is slightly nonstationary. Introduction of mild control would greatly reduce the variance of output. Implementing mild control on process under statistical control would increase the variance slightly [3].

EPC uses the feedback controller for process control; deviations from the target are usually autocorrelated and this information is used to forecast the future deviation from target. The time

series model is fitted to the autocorrelated output and model is identified and then the model parameters are estimated. This model is used to get the minimum mean square error forecast of future disturbance and the controller is set in such a way that the deviation from the target is cancelled out. However, an efficient process adjustment strategy has to take into account the economical aspects of process adjustment. In the following sections, we shall review the above mentioned steps.

15.2 Notation

The notation with terms used in this chapter is given below.

T : Process target
y_t : Process quality characteristics at period t
z_t : Deviation of quality characteristic from target T
x_t : Control variable (input)
G : Damping factor
a_t : White noise $N(0,\sigma_a^2)$
ϕ : Autoregressive parameter
θ : Moving average parameter
λ : Discount factor
(V_m) : Variance of values m steps apart
β : Process gain.
m: Sampling interval
C_T : Cost of being off- target by an amount σ_a
C_M : Fixed cost incurred each time the process is observed
C_A : Fixed cost incurred each time the process is adjusted
AAI: Average interval between adjustments-measured in terms of unit interval
MSD: Mean squared deviation
ISD: Increase in standard deviation
L : Bound length
σ_e^2 : Variance of scheme
η_t : Process disturbance
α : Intercept or offset of the process.
p_t : Estimate of intercept
b: Estimate of gain
w : Discount factor
δ : Deterministic drift rate
w_1 : Discount factor to estimate mean
w_2 : Discount factor to estimate trend
ξ : Gain estimate bias

15.3 Stochastic Models

The important need for process adjustment is to model the stochastic disturbances accurately. It is necessary to understand the behavior of disturbances and their effect on the quality characteristics of interest. The most valuable contributions to model dynamic behavior of process are due to from Box and Jenkins [4–7]. In their contributions stochastic time series modeling was adopted. The disturbances were envisaged as the result of a sequence of independent random shocks entering the system.

15.3.1 Time Series Modeling for Process Disturbances

Stochastic disturbances are most conveniently modeled as a time series. We shall briefly revise time series analysis; an in-depth analysis can be obtained from references [4–13].

The simplest time series is a sequence of values of $a_t, a_{t-1} \ldots a_1$, which are normally independently distributed with mean zero and standard deviation σ_a. Such a series is called white noise. Let us define disturbance as $z_t = y_t - T$, where y_t is the quality characteristics to be maintained on target *T*. The time series model is an equation that relates the sequence of disturbance values z_t to white noise a_t.

Time series models are broadly classified into two classes (see Figure 15.1):

1. Stationary time series models
2. Nonstationary time series models

Stationary time series are the time series that oscillate around a fixed mean while nonstationary time series do not stay around a fixed mean but gradually move away from the mean.

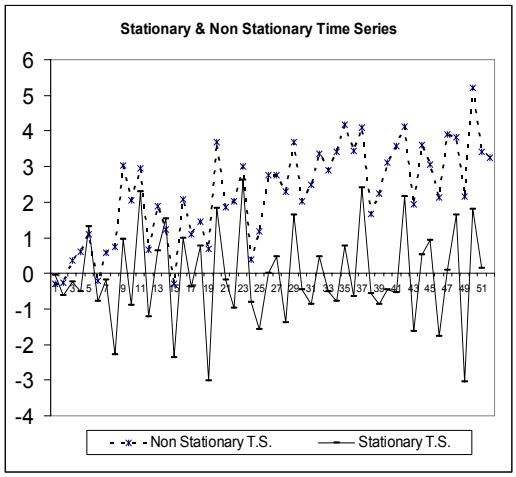


Figure 15.1. Stationary and nonstationary time series

Stationary Time Series Models

Stationary time series models assume that the process is in equilibrium and oscillates about a constant mean. The three stationary models are autoregressive models, moving average models and autoregressive moving average models.

In autoregressive AR(p) models the current value of the process is expressed as function of p previous values of the process. The AR(p) model is represented as

$$\begin{aligned} &\phi(B)z_t = a_t \\ &where \\ &\phi(B) = 1 - \phi_1 B - \phi_2 B^2 ... \phi_p B^p \\ &B^m z_t = z_{t-m} \end{aligned} \tag{15.1}$$

In moving average MA(q) models z_t is a linear function of finite number (q) of previous a_t's. The MA(q) model is represented as

$$\begin{aligned} &z_t = \theta(B)a_t \\ &\theta(B) = 1 - \theta_1 B - \theta_2 B^2 ... \theta_q B^q \end{aligned} \tag{15.2}$$

In autoregressive moving average ARMA(p, q) models include both AR and MA terms in the model. It is represented as

$$\phi(B)z_t = \theta(B)a_t \tag{15.3}$$

Nonstationary Time Series Models

Many series come across in practice in various fields exhibit nonstationarity, *i.e.*, they do not oscillate around a fixed mean but drift. Stock prices, bacterial growth, and process disturbance are few of such series. So most commonly assumed disturbances are of the nonstationary time series family, where once the time series makes the excursion from the mean it does not return unless control action is taken.

Autoregressive integrated moving average ARIMA(p, d, q) models are nonstationary time series models and are of great help in representing nonstationary time series. ARIMA has AR, MA and an integrating operator.

It is represented as

$$\begin{aligned} &\phi(B)\nabla^d z_t = \theta(B)a_t \\ &\nabla = 1 - B \\ &\varphi(B)z_t = \theta(B)a_t \\ &\varphi(B) = \phi(B)\nabla^d \end{aligned} \tag{15.4}$$

ARIMA can be regarded as a device transforming the highly dependent and possibly nonstationary process z_t to a sequence white noise a_t.

15.3.2 Stochastic Model Building

Box and Jenkins proposed three-stage iterative procedures to build model to data. The three steps are identification, estimation, and diagnostic checking of model

1. Use the data efficiently to *identify* the promising subclass of parsimonious models.
2. Use the data effectively to *estimate* the parameters of the identified model
3. Carry out a *diagnostic check* on the fitted model and its relation with the data to find the model inadequacies and analyze the need for model improvement.

Model Identification

The task at the model identification is to estimate parameters p d q. It is most convenient to estimate model parameters based on autocorrelation

functions and partial autocorrelation function graphs.

The first step is to check for the time series stationarity. If the time series is not stationary, reduce it to a stationary time series by differencing to appropriate degree. The stationarity of the time series can be inferred by looking at the time series plot. However, a statistical way may also be adopted. If the estimated autocorrelation function of the time series does not die out rapidly, this suggests that the underlying stochastic process is nonstationary. If the time series is found to be nonstationary the differencing is done *d* times until the estimated autocorrelation of differenced series dies out quickly. The reduced time series is of the form

$$\varphi(B)z_t = \theta(B)a_t \,.$$

The next step is to identify the resultant stationary ARMA process. The various subclasses of the time series model have the following autocorrelation and partial autocorrelation properties:

- For an AR(*p*) process,

The autocorrelation function of an AR(*p*) process tails off and the partial autocorrelation function of an AR(*p*) process cuts off after lag *p*.

- For an MA(*q*) process,

The autocorrelation function of an MA(*q*) process cuts off after lag *q,* and the partial autocorrelation function of an MA (*p*) process tails off.

- For an ARMA(*p q*) process,

both the autocorrelation function and the partial autocorrelation function tail off.

As can be noted, AR(*p*) parameter *p* and MA*(q)* parameters *q* are easier to identify than ARMA(*p q*) parameters *p* and *q*. In practice the ARMA model is fixed after trying with the pure AR and MA processes. Most time series encountered in practice have parameters *p, d, q* less than or equal to 2.

Model Parameter Estimation

The parameters of the identified model are to be estimated. If the estimation is carried out using an historical data set it is called offline estimation. The parameters are estimated by maximum likelihood estimates.

Diagnostic Checking

If the model fitted is appropriate, the residuals should not have any information concealed in them. If the autocorrelation is completely captured, the residuals should be white noise. In diagnostic checking the autocorrelation function of residuals is checked. The Ljung–Box–Pierce statistic is used to test the null hypothesis of no autocorrelation for any lag. If the residuals show significant autocorrelation then the model must be refit and all the three steps should be repeated until a satisfactory model is fit.

15.3.3 ARIMA (0 1 1): Integrated Moving Average

IMA (0 1 1) is a special class of the ARIMA(*p d q*) model. It is capable of representing a wide range of time series encountered in practice, such as, stock prices and chemical process characteristics (temperature, viscosity, concentration). It is also most suitable for modeling disturbances occurring in a process. With the AR parameter 0 and I and MA parameters 1 each, the ARIMA becomes

$$\nabla z_t = a_t - \theta a_{t-1} \tag{15.5}$$

The model has two parameters θ and σ_a^2. It may be convenient to represent IMA (0 1 1) in following forms:

$$\begin{aligned} \nabla z_t &= (1-\theta B)a_t \\ z_t &= z_{t-1} + a_t - \theta a_{t-1} \\ z_t &= \text{constant} + a_t + \lambda \sum_{i=1}^{t-1} a_i \end{aligned} \tag{15.6}$$

Intuitively z_t is a mixture of current random shocks and sum of previous shocks

The obtained model is used to forecast the disturbances and characterize the transfer function of the dynamic process. It is easy to show that EWMA provides the minimum mean square error forecast for IMA (0 1 1). They are used in feedback control in engineering process control.

Justification for IMA (0 1 1) Model

The nonstationary time series model IMA (0 1 1) is most commonly used to model industrial disturbances. As can be noted, most of the literature assumes that the disturbances are IMA (0 1 1). Here we shall justify the use of IMA (0 1 1) disturbance assumptions in deriving control actions to be used in practical cases.

A good way to explain the nonstationary model and to justify its adoption is by a variogram. The variogram tells us how much bigger the variance is for values *m* steps apart (V_m) than for values one step apart (V_1). The plot of (V_m / V_1) against *m* is called a variogram [14]. For a white noise the (V_m / V_1) ratio is equal to unity for any value of *m* as data are uncorrelated. For a stationary series the ratio (V_m / V_1) increases rapidly initially and then flattens out. This implies that the variance for initial *m* values differs but for further values, the ratio reaches a steady value. This is practically not justifiable because once the process goes out of control the variance keeps on increasing. For example, if a crack appears on a shaft the crack goes on increasing until the shaft breaks down. For nonstationary models the (V_m / V_1) ratio keeps on increasing as *m* increases and this represents a more practical case [15]. Stationarity implies that once a process goes out of control, it just wanders about the mean value. A nonstationary model implies that once the process goes out of control, it keeps on drifting away from the mean unless a control action is taken.

Study on ARMA and IMA models for a discrete adjustment scheme has shown that a) the IMA model leads to a much easier analysis, b) almost exactly the same average adjustment interval (AAI) and mean square deviation (MSD) are obtained under both disturbance models in the region of interest of the action limits, c) for wider action limits the ARMA disturbances overestimate the AAI and MSD with respect to the results provided by IMA disturbances, and d) the IMA model is robust against model misspecification but the ARMA is not [16]. Hence the IMA (0, 1, 1) model is adopted to represent the process disturbance.

15.4 Optimal Feedback Controllers

The objective of EPC is to minimize the variance of quality characteristics around the target. It is assumed that a control variable that can be adjusted to compensate for the disturbances is available. In this chapter no process dynamics is considered. The effect of a change in control variables is observed fully in the next period on quality characteristics. Such responsive systems are common in discrete parts manufacturing. The expected deviation from the target for the next period is forecasted at the end of every period and the control variable is set so as to cancel out the deviation. Similar to any intuitive controllers, the adjustment is made proportional to the deviation. A typical adjustment equation may be represented as

$$\beta x_t = \hat{z}_{t+1} \tag{15.7}$$

β is called the process gain. It is similar to the regression coefficient showing the relative effect of change in input on output. The value of β may be determined from classical design of experiments and response surface methodology [17]. In the machine tool setting gain is usually assumed to be unity.

$\hat{z}_{t+1}$ is the minimum mean square error forecast of next deviation from target. The controller is known as the minimum mean square error controller.

Example 1

Consider the hypothetical industrial process shown in Figure 15.2 (Table 15.3), whose quality characteristics have to be maintained on target = 0. The process is affected by disturbances from various sources and the quality characteristics drift away from the target. The graph shown in figure depicts the process. We shall demonstrate EPC methodologies in industrial scenarios through the data set in this chapter.

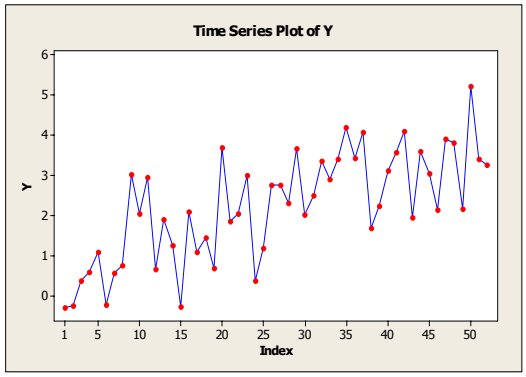


Figure 15.2. Uncontrolled process

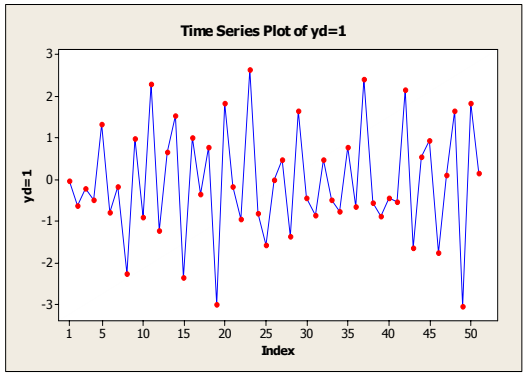


Figure 15.3. Differenced time series

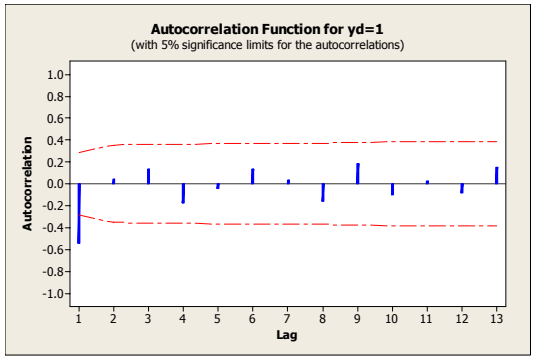


Figure 15.4. Autocorrelation function (5% significance limits)

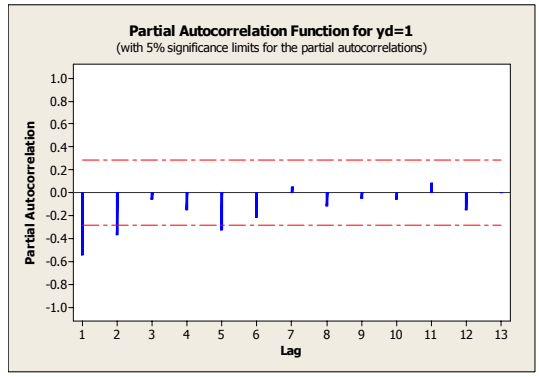


Figure 15.5. Partial autocorrelation function (5% significance limits)

Model Identification

The first step is to identify and estimate the time series model for the process disturbances.

From the graph in Figure 15.2 it can be seen that the process is nonstationary, as the process drifts away from target. The first differencing operation is carried out on the data. The graph of the differenced series shows that the series is reduced to a stationary time series (Figure 15.3). To identify the time series model further, the autocorrelation and partial autocorrelation graphs are plotted as shown in Figures 15.4 and 15.5. The following observations are made

1. The autocorrelation function cuts off after lag 1.
2. The partial autocorrelation function tails off.

These are the characteristics of the MA (q) model and the order of the MA series is 1 ($q = 1$).
The parameter of this MA(1) series is $\theta = 0.75$.

Minimum Mean Squares Error Control

In minimum mean squares error control (MMSE), at the end of each period the next period disturbance (deviation from target) is forecasted and the control is applied against the forecasted disturbance. Figure 15.6 shows the MMSE controlled process. The deviations from the target in an MMSE controlled process are forecast errors.

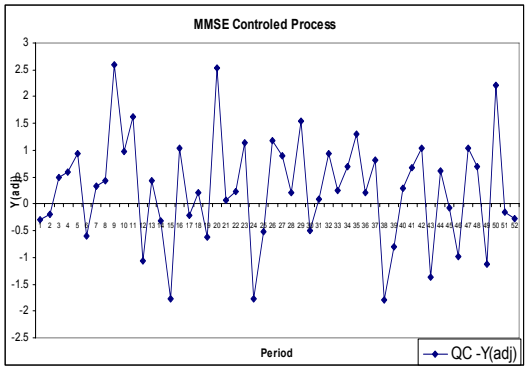


Figure 15.6. MMSE controlled process

Robustness Against Suboptimal Model Parameter Estimation

Most industrial disturbances follow IMA (0 1 1). The optimal value of smoothing constant, which produces minimum mean square error at the output is $G = \lambda = 1 - \theta$.

In industrial settings estimates from the available data set may not be accurate due to a lack of data set. Minimum mean square error control is robust against the use of inaccuracy of the damping factor [18]. The sum of the square curve tends to be flat in the neighborhood of the theoretical minimum. So a moderate departure from the theoretical optimal damping factor would produce a relatively lower increase in the mean square error. The control applied using these estimates will produce an output variance very close to the theoretical minimum.

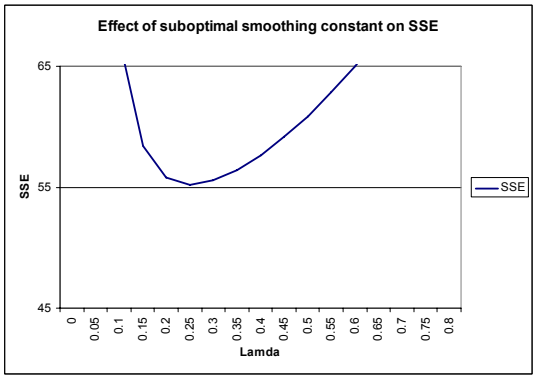


Figure 15.7. MMSE robustness against a suboptimal smoothing constant

The graph in Figure 15.7 illustrates the sum of squared errors (SSE) forecast for the assumed process data; it should be noted that the minimum is not a sharp point but a smooth flat curve near the optimal value of $\lambda = 0.25$. Even if we would have chosen any value in the most general interval of industrial disturbance $\lambda \sim [0.2, 0.4]$ the increase in SSE from the minimum possible SSE would have been just 4.47%.

Further the robustness is well explained as follows [3]. Consider an IMA (0 1 1) disturbance model with the true value of smoothing constant θ_T . Let the value of G used in the control scheme be a suboptimal value different from $\lambda_T = 1 - \theta_T$. The variance of the control scheme is inflated by the following factor

$$\frac{\sigma_e^2}{\sigma_a^2} = 1 + \frac{(G - \lambda_T)^2}{G(2 - G)} \tag{15.8}$$

The equation depicts the inflation in the process variance as a consequence of using a suboptimal smoothing constant. Two important points can be noted from the analysis:

1. If the process in the state of statistical control $\lambda_T = 0$ is adjusted equal to the deviation G = 1. The variance of the process is inflated by a factor of 2. This point is a reaffirmation of Deming's funnel experiment. The process already in a state of statistical control should not be tampered with.
2. If the process is slightly nonstationary $\lambda_T > 0$ the use of mild control (*G = 02~0.4)* greatly reduces the process variance when compared with the no control strategy. In fact, several times in practice a state of statistical control is difficult to maintain. Manufacturing environments are not static and the quality engineer cannot be sure if the process is under a state of statistical control. In these cases process adjustment is a better strategy.

15.4.1 Economic Aspects of EPC

The aim of EPC is to adjust the process to keep the quality characteristics on target. In practice, there

are various costs incurred. These costs have to be taken into account to make a rational decision. The major cost parameters involved in engineering process control are as follows

Off-target Costs

Off-target costs are costs incurred when quality characteristics deviate from the target. These costs are proportional to the deviation from the target; they are linear functions. Off-target costs are usually assumed to be quadratic. The cost function is symmetric. The costs of deviation above and below target by same amount are the same. However, it is not rare to come across cases where the loss function is not symmetric about the target.

Adjustment Costs

Adjusting a process may incur significant costs in real-life processes. The adjustments may require the process to be stopped and some costly manipulations to be made. This consumes monitory resources as well as valuable time. Frequent adjustments are hence not encouraged. It may be noted that adjustment is also shunned because it may induce additional variability in the process. The adjustment costs in EPC are assumed to be fixed and independent of the magnitude of adjustment.

Sampling Costs

Sampling costs are those costs incurred in obtaining the final numerical value of the quality characteristics. They include the costs incurred in sampling the process and making physical and chemical analyses to obtain accurate readings from high precision measurements. When the sampling costs are significant it may be desirable to reduce the sampling rate.

These costs are highly situation and case dependent. While producing a costly product the off-target costs may dominate the adjustment and sampling costs. In some processes the sampling costs may be high, while in others the required output data may be easily available from digital display. Similarly, some process adjustment costs may be high, requiring the process to be stopped or some costly repairs to be done, while in others the adjustment may only involve turning a knob, making the adjustment costs insignificant. The rational decision, whether to adjust the process and how often to sample the process should be based on the off-target costs, adjustment costs, and sampling costs.

15.4.2 Bounded Feedback Adjustment

If there are no adjustment costs and sampling costs, and the adjustment is accurate, it is advisable to adjust the process at every period. In such cases, the minimum variance controllers will be appropriate and effective in keeping the process on target. In several practical cases it is undesirable to adjust and sample the process often due to the respective costs. A controller operating on the sole objective of minimizing the variability of quality characteristics around the target while neglecting other costs may not be of significant practical value.

To accommodate cost parameters into feedback adjustment, bounded feedback adjustment is proposed. In bounded feedback adjustment a deadband is placed around the target. The process is adjusted only if the forecasted deviation from the target exceeds the bound length. This bound length is a function of off-target costs, adjustment costs, and sampling costs.

Example 2

The bounded feedback control is applied to the process (Figure 15.8). Let the bound length of 1

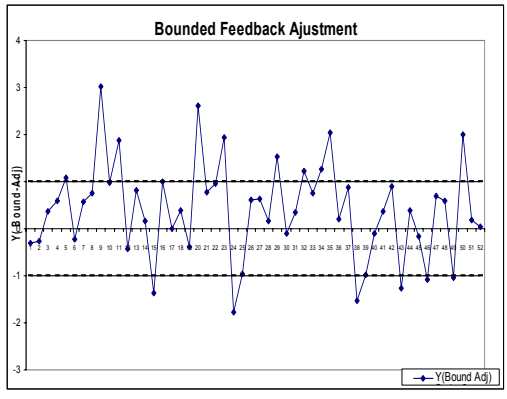


Figure 15.8. Bounded feedback adjusted process

Table 15.1. Comparison of **r**esults

		MSD about Target	No. of adjust-ments	Out-put std dev
Feed-back Adjust-ed	Un-bounded	1.06	51	1
	Bounded $L = 1$	1.86	3	1.02
Unadjusted		6.8		1.8

unit be placed around the target. The process is not adjusted if the forecasted deviation from the target falls within this deadband. If forecasted deviation from the target falls beyond the deadband, the process is stopped and the control is applied to nullify the forecasted deviation from the process. The process is carried out further in the same way.

Table 15.1 gives the relative comparison on performance of the bounded and unbounded feedback control.

It can be seen that though mean squared deviation (MSD) about the target for bounded adjusted process has increased, the number of adjustment has decreased in greater proportion.

Decision on Deadband Limits

Under the assumption of the responsive adjustment system the uncontrolled disturbance is adequately modeled by the IMA (0 1 1) model with parameters λ and σ_a. The average adjustment interval (AAI) and increase in standard deviation (ISD) considering quadratic off-target cost, fixed adjustment costs, and fixed sampling costs for various values of λ and σ_a are determined as follows [19, 20]:

The following assumptions are made regarding the process:

1. Process disturbance is adequately modeled by IMA (*0 1 1*)
2. Quadratic off-target costs
3. Fixed adjustment costs
4. Fixed sampling costs
5. Infinite production length

A process that was initially sampled at unit intervals, considering the possibility of sampling at interval *m* units apart where *m* is an integer, the sampled process is still an IMA (0, 1, 1) time series but with parameters λ_m and σ_m [9].

Here,

$\lambda^2{}_m\sigma^2{}_m = m\lambda^2\sigma^2{}_a$ and $\theta\ {}_m\sigma^2{}_m = \theta\ \ \sigma^2{}_a$

The overall expected cost *C* per unit interval is

$$C = \frac{C_A}{AAI} + \frac{C_M}{m} + \frac{C_T(MSD)}{\sigma_a{}^2} \tag{15.9}$$

where

C_T: cost of being off target by an amount σ_a

C_M: observed fixed cost incurred each time process is sampled

C_A: Fixed cost incurred each time process is adjusted

AAI: Average interval between adjustments measured in terms of unit interval

MSD: Mean squared deviation

MSD is defined by

$$MSD = \frac{1}{AAI} E\left[\sum_{J=0}^{n-1}\sum_{K=1}^{m} \varepsilon_{mj+k}{}^2\right] \tag{15.10}$$

Finally the overall cost function arrived at is

$$C = \frac{C_A}{mh[L/(\lambda_m\sigma_m)]} + \frac{C_M}{m} + C_T\left\{\frac{\theta}{\theta_m} + m\lambda^2 g[L/(\lambda_m\sigma_m)] - \frac{(m-1)\lambda^2}{2}\right\} \tag{15.11}$$

where *h(.)* and *g(.)* are both solely functions of $L/(\lambda_m\sigma_m)$ that relate *AAI* and *MSD*. These functions are exactly characterized by integral equations. These equations can be approximated by the following functions, which have been checked by extensive simulations [21]:

$$h(B) = (1 + 1.1B + B^2) \times \{1 - 0.115 \exp[-9.2(B^{.3} - .88)^2]\} \quad (15.12)$$

and

$$g(B) = \frac{1 + .06B^2}{1 - .647\Phi\{1.35[\ln(B) - .67]\}} - 1 \quad (15.13)$$

Where $\Phi(.)$ is the standard normal *cdf*. The optimal bound length is obtained by minimizing the above overall cost C with respect to bound length L.

15.4.3 Bounded Feedback Adjustment Short Production Runs

The current market life of several products is short. Products become outdated with the entry of better quality products at reasonable costs. In such cases, it is not reasonable to assume infinite production length. The rapid development of technology, product innovation, use of just-in-time manufacturing, *etc*., have made production run lengths short. To control such processes, applying the bound lengths obtained based on infinite production run length may prove to be suboptimal. There is a need to solve this under finite production length assumption. It is shown that the length of production significantly influences adjustment strategy. The use of control limits based on the assumption of an infinite run process can significantly inflate the expected costs. The short run limits were computed using dynamic programming and an algorithm was developed. It has been shown that the optimal deadband limits funnel out as the end of production run approaches. It is less attractive to adjust if the end of run is close [22]. Owing to the lack of data available on the short production run model, the parameters are estimated adaptively and recursively.

The same cost function [22] was further studied with inclusion of adjustment errors [23]. The effects of adjustment costs, adjustment variance, and drift rate on the obtained optimal policy have been studied. The following two important results were given in the study. Firstly, in the case of nonzero adjustment error there will be a deadband in the optimal policy even when there is no fixed adjustment cost. It is advantageous not to make adjustments if the adjustment is imprecise even if there is no fixed adjustment cost. Secondly, for relatively small nonzero deterministic drifts the optimal policy calls for a certain amount of over compensation with each ordered process adjustment to anticipate drift that will occur in future time periods.

15.5 Setup Adjustment Problem

In manufacturing process it is crucial to accurately set up the machine at the beginning of production run. An incorrect setup can result in sever consequences on the part produced in the run. The effect of set-up error is to induce a mean shift in the output. It is necessary to adjust and correct the process that has set-up error induced at the beginning of the run.

Consider a process where a machine is set up before the production run and this set-up is subject to set-up errors. The so induced set-up error will induce step deviation in the output quality characteristics (y_t) and deviates it from the desired target T. The objective is to adjust the process to eliminate the offset induced in output. Suppose that a control variable x is available that has a direct effect on the output and control exercised comes into effect immediately without delay. In set-up adjustment the objective is to bring the process on target quickly by estimating the offset accurately. The magnitude of offset is estimated from the observed data. The observations are subject to inherent process variation and measurement errors. The accuracy of the offset estimate can be improved with increase in the available observation. Waiting for a long time to collect data, conflicts with the objective of bringing the process on target as soon as possible. An optimal strategy for this situation is to sequentially estimate the offset and adjust the process accordingly. Grubbs proposed an elegant sequential adjustment rule to solve the set-up error adjustment problem;

this is popularly known as Grubb's harmonic rule [24]. The proposed adjustment strategy is to adjust the process according to following equation,

$$x_{t+1} - x_t = \frac{-(y_t - T)}{t} \qquad t = 1, 2, 3, \ldots$$

The expected value of the process quality characteristics of every next period will have the mean as target value and the variance is minimum around the target.

The adjustment rule implies that, after producing the first part, the machine is adjusted against the full observed deviation. After the second part is produced, the machine is adjusted against half the observed deviation and so on. The adjustment follows a harmonic series $\left[1, \frac{1}{2}, \frac{1}{3}, \ldots\right]$, thus called as Grubb's harmonic rule.

The following assumptions were made:

1. The process is stable with no autocorrelation or drift in the mean.
2. Adjustments modify the process mean
3. Adjustments are exact and implemented on every part.

Sullo and Vandevan [25] studied optimal adjustment strategies for a process with run-to-run variation and 0-1 quality loss function for a short run manufacturing process. They considered a set-up error induced at the beginning of each run and remaining fixed through the run. They developed a single adjustment strategy based on taking a sample of fixed size from the process. The strategy depends on the actual process parameters such as adjustment error, run size, and adjustment and sampling costs. They specified both the time and magnitude of adjustment for 0-1 quality loss function and a short run manufacturing environment.

Pan and Del Castillo [26] studied the set-up adjustment problem and presented scheduling methods to determine the optimal time instants for adjusting a process. They compared the three scheduling methods in terms of the expected manufacturing cost and computational effort of each method. The adjustment methods were based on estimates of process variance and size of the offset. The robustness of these methods with respect to biased estimates of process variance and of the set-up error was discussed. They recommended the silver-meal heuristic used in inventory control based on performance analysis.

15.6 Run-to-run Process Control

Run-to-run control is also a discrete form of feedback control in which control action is exercised between runs or batches to minimize deviation from target and process variability. It is mostly referred to in the context of semiconductor manufacturing. Run-to-run control has some characteristic differences from the machine tool control problem discussed in the preceding sections. Reviews on run-to-run control can be found in [27, 28].

The main difference between machine tool problems and the run-to-run (R2R) control problem lies in adjustment costs. In the machine tool problem the adjustment costs are assumed to be significant and adjustments are performed manually. In R2R problems the adjustment costs are insignificant because adjustment may involve simply turning a knob. Machine tool problems often assume long production runs. The parameters of disturbance are assumed to be determined to a satisfactory degree of accuracy offline. In R2R problems production runs are short. There is no luxury of large historical data set to accurately estimate the model parameters. The parameters are roughly estimated offline with a limited data set and are updated online. The differences between the R2R and machine tool problems are summarized in Table 15.2. The differences are not a strict demarcation between the two but a rough classification is provided.

R2R control has found several successful applications in semiconductor manufacturing, such as photolithography, reactive ion etching and chemical mechanical polishing.

Table 15.2. Machine tool and R2R problem comparison

	Machine tool problem	Run-to-run problem
1	Adjustment costs are significant	Adjustment costs are not significant
2	Production length is large	Production length is small
3	Trend in the process is assumed to be stochastic	Trend in the process is assumed to be deterministic

15.6.1 EWMA Controllers

Single EWMA controllers are the most widely used controllers in the semiconductor manufacturing industry. These controllers are simple and yet highly effective in keeping the process on target and reducing variability. The procedure of adjusting the process by using EWMA controllers is as follows [29].

Consider a process that is offset and interfered with by process disturbance. Let the process be described by following equation:

$$y_t = \alpha + \beta x_{t-1} + \eta_t \tag{15.14}$$

where

y_t: Value of process quality characteristics (output) for batch number *t*

x_{t-1}: Control variable (input) chosen at the end of the run

η_t: Process disturbance

α: Intercept or offset of the process

β: Slope or gain.

α and β are assumed to be constant over time. They are unknown and are to be estimated from available data.

Process gain is similar to a regression coefficient depicting the amount of change in output for the corresponding change in input. Process gain is estimated through design of experiments, regression analysis and response surface methodology [17].

Let p_0 and b denote initial estimates of α and β. p_0 and b are typically chosen to be least square estimates of α and β based on historical data. Like in any other controller, in run-to-run control the control variable is set to nullify the deviation from target. Thus,

$$x_0 = \frac{T - p_0}{b} \tag{15.15}$$

where T is the desired target value of output.

In the proposed EWMA controller, the unknown parameter α (intercept or offset) is recursively estimated and updated and the input variable is determined at the end of each run. The equation for estimation is as follows:

$$p_t = w(y_t - bx_{t-1}) + (1-w)p_{t-1} \tag{15.16}$$

where $0 \le w \le 1$ is called the discount factor.

The estimated intercept is substituted into the following equation to determine the value of control variable:

$$x_t = \frac{T - p_t}{b}$$

As it can be noted, the key idea in the EWMA controller is that for a predetermined process gain, the intercept and input variables are updated recursively. The expected value will then asymptotically converge to the desired target.

If the process disturbances follow the nonstationary IMA (0 1 1) model

$$\eta_t = \eta_{t-1} + a_t - \theta_1 a_{t-1}$$
$$a_t \sim N(0, \sigma_a^2) \quad t = 1, 2, \ldots$$

and the gain estimate bias be represented as $\xi = \frac{\beta}{b}$ under the condition that $0 < \frac{\beta}{b} < 2$, *i.e.*, the gain estimation is biased not more than twice the original value, the optimal discount factor is given by

$$w_0 = \frac{b(1-\theta_1)}{\beta}$$

However, an inaccurate estimation of unknown parameters α and β leads to a large value of the initial bias

$$\frac{\alpha + \beta(T - p_0)}{b}$$

and it will take several runs for the EWMA controller to bring the process back to target.

Example 3

Consider the process given in Table 15.3. In addition to being interfered with by IMA (0,1 1) process disturbance let the process be offset $\alpha = 2$. Suppose that the gain estimate is determined and found to be unity $\beta = 1$. The objective is to bring the process on target by process adjustment. A single-EWMA controller with $w = 0.25$ is employed to control the process and keep it near target. The control is started with the initial estimate of offset $p_0 = 0$ and is recursively updated in subsequent steps. Figure 15.9 shows the uncontrolled and single EWMA controlled process.

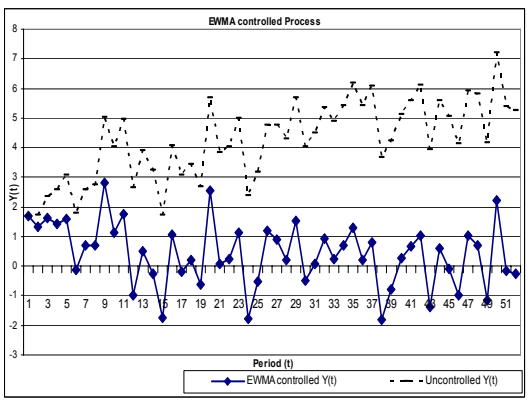


Figure 15.9. Uncontrolled and EWMA controlled process

15.6.2 Double EWMA Controllers

The manufacturing process may experience deterministic drifts with time and trend away from the target. Such a phenomenon may be due to ageing machines or deterioration of ideal manufacturing conditions with time. The goal of feedback control is to adjust control variables so that the output will be as close to the target as possible. Use of single-EWMA in this case would not be optimal because it cannot compensate for a deterministic trend. Hence, such processes are not efficiently controlled using single-EWMA controllers.

Consider a process that is offset and interfered with by process disturbance and is drifting with runs. Let the process be described by the following equation:

$$y_t = \alpha + \beta x_{t-1} + \delta t + \eta_t \qquad (15.17)$$

as defined earlier $y_t, \alpha, \beta, \eta_t, x_{t-1}$ denote output, intercept, slope, process disturbance and the input recipe determined at the end of *(t-1)*th run, respectively. δ denotes the deterministic drift rate. The following double-EWMA controllers are applied for such linear drifting manufacturing processes [30]:

$$x_t = \frac{T - p_t - D_t}{b} \qquad (15.18)$$

$$p_t = w_1(y_t - bx_{t-1}) + (1 - w_1)p_{t-1} \qquad 0<w_1 \le 1$$
$$D_t = w_2(y_t - bx_{t-1} - p_{t-1}) + (1 - w_2)p_{t-1} \qquad 0<w_2 \le 1$$

(15.19)

A double-EWMA controller consists of a filter to estimate the true output mean as well as a filter to estimate the trend. The forecast is equal to the smoothed value plus the smoothed trend.

It may also be represented in following way:

Current smoothed value =

$(1-\alpha)$data at time t+(α)best previous estimate

Current smoothed trend= (1-β)Estimated trend value at time t

+ (β)previous trend estimate

Forecast=Current smoothed value+Current smoothed trend

Example 4

Consider the process given in Table 15.3. In addition to being interfered with by IMA (0,1,1) process disturbance, let the process be offset by $\alpha = 3$ and also be experiencing a deterministic trend of $\delta = 0.5$ per period, Suppose that the gain estimate is determined and found to be unity $\beta = 1$. The objective is to bring the process on target by process adjustment. First, a single-EWMA controller with $w = 0.25$ is employed to control the process and keep it near target. The control is started with an initial estimate of offset $p_0 = 0$ and is recursively updated in subsequent steps. It can be observed in Figure 15.10 that single-EWMA control leaves the process with considerable offset. This is because unlike double-EWMA controllers, single-EWMA is not equipped to control processes with high deterministic drift. A double-EWMA controller with $w_1 = 0.25$ and $w_2 = 0.05$ is employed to control the process. The control is started with the initial estimate of $p_0 = 0$ and $D_t = 0$. They are recursively updated in subsequent steps. The graph in Figure 15.10 shows the single-EWMA controlled and double-EWMA controlled process.

Weights in the double-EWMA controller are selected considering transient and long term stability conditions [31, 32]. The process given by $y_t = \alpha + \beta x_{t-1} + \delta t + a_t$ and regulated by double-EWMA will be asymptotically stable if and only if,

$$|1 - 0.5\xi(w_1 + w_2) + 0.5\kappa| < 1$$

and

$$|1 - 0.5\xi(w_1 + w_2) - 0.5\kappa| < 1$$

where

$$\kappa = \sqrt{\xi(\xi((w_1 + w_2)^2 - 4w_1 w_2}$$

The no oscillation and stability conditions for different ranges of values of ξ are given as follows [31]:

$$\xi \in \begin{cases} (-\infty, 0] & \text{System is unstable} \\ \left(0, \dfrac{4w_1 w_2}{(w_1 + w_2)^2}\right) & \text{System is stable but oscilates} \\ \left[\dfrac{4w_1 w_2}{(w_1 + w_2)^2}, \dfrac{1}{(w_1 + w_2 - w_1 w_2)}\right] & \text{System is stable and does not oscilate} \\ \left(\dfrac{1}{(w_1 + w_2 - w_1 w_2)}, \dfrac{2}{(w_1 + w_2)}\right] & \text{System is stable and oscilates} \\ \left(\dfrac{2}{(w_1 + w_2)}, +\infty\right) & \text{System oscilates and is unstable} \end{cases}$$

For the general class of ARIMA (*p,d,q*) process disturbances, the exact expression for process output under double-EWMA control, stability conditions and feasibility region have been obtained by Tseng *et al*. [33]. They derived the optimal discount factor by minimizing the rework rate of the process output instead of minimizing the mean square error criteria used in [32].

In the case of the double-EWMA control scheme, the predicted model is constructed by a random sample to input-output variables, the strength of the linear relationship between input output plays an important role in determining the validation of the stability conditions. Tseng and Hsu [34] derived a formula for an adequate sample size required to construct the predicted model in the case of single input single output, and multiple input single output systems. They demonstrated the effectiveness of the covariance structure of input output variables in determining the sample size. The stability conditions of single and double-EWMA feedback controllers are invariant with

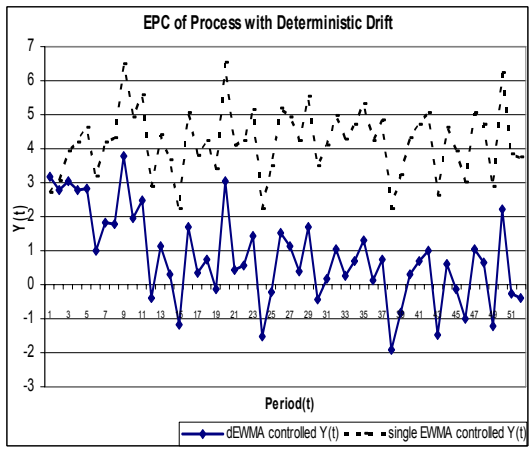


Figure 15.10. Single-EWMA and double-EWMA controlled process with deterministic drift

respect to the large class of process disturbances that model the drift. However, the use of double-EWMA in place of single-EWMA is justified only if the drift rate is severe [35].

15.6.3 Run-to-run Control for Short Production Runs

Single-EWMA controllers and double-EWMA controllers presented above long term stability under suitable discount factors but it may take a large number of runs to bring the process output to meet its target. This will have severe consequences in short production runs, frequently encountered in the semiconductor industry. In this section internal intercept iteratively adjusted (IIIA) controllers and variable EWMA controllers, which overcome this shortcoming and reduce the high rework rate during initial runs, are briefly discussed..

Internal Intercept Iteratively Adjusted (IIIA) Controllers

Double-EWMA guarantees long term stability under suitable fixed discount factors but it takes a large number of runs to bring the process output to meet its target. The quality characteristics may be out of specification limit in the first few runs. This makes double-EWMA controllers inefficient for short production runs. This weakness is overcome by adopting internal intercept iteratively adjusted (IIIA) controllers [36]. IIIA controllers further reduce the off-target or nonrandom bias of the process output. The equation is similar to double-EWMA controllers. The IIIA controller updates the double-EWMA filter to remove initial nonrandom bias for short production runs. It is found that the mean square error of IIIA controllers is less than the mean square error of double-EWMA controllers.

Variable EWMA Controllers

The EWMA controller with a small discount factor can guarantee long term stability under fairly regular conditions but it usually requires a large number of runs to bring the process output to its target. Variable EWMA controllers overcome this weakness [37]. In variable EWMA instead of using a fixed discount factor, a variable discount factor is used. To accelerate convergence, a larger discount factor is used in first few runs of R2R control. An optimal variable discount factor is obtained by minimizing the total mean square error within the first few runs.

15.6.4 Related Research

Paterson *et al*. [38] addressed the challenge of selecting the variable to feedback for applying feedback control to the semiconductor manufacturing process. They proposed an empirical methodology for selecting the best process variable for feedback in order to minimize variation in product variables. Paterson *et al.* [39] illustrated the practical aspects of utilizing the Paterson *et al.* [38] methodology to the self-aligned gate etch process.

Firth *et al.* [40] presented just-in-time adaptive disturbance estimation, which uses recursive least square parameter estimation to identify the contributions to variation that depend on the manufacturing context.

Chen and Guo [41] analyzed that controllers based on the EWMA statistic are not sufficient for controlling a wearing out process. They proposed a predictor corrector controller (PCC) to enhance the run-to-run control capability.

The topic of run-to-run control for multiple inputs and multiple output process has not received the deserved attention. Some notable work is listed here. Del Castillo [32] showed that double-EWMA controllers for single output and single input can be extended to multiple input single output models. Tseng *et al.* [42] proposed multivariate EWMA for linear MIMO models. They obtained the stability conditions and feasible region of its discount factor.

15.7 SPC and EPC as Complementary Tools

Greater benefits are obtained when SPC and EPC are used as complementary tools. This combination helps to verify adequacy of adjustment and also to identify assignable causes of change in performance.

It is criticized that EPC implementation deprives us of the opportunity of improving a process by identifying the assignable cause and removing it. EPC has even been described as a bandage to cover the wound not to cure it. The implementation of EPC and feedback control may conceal the true nature of the disturbance affecting the process. This may be avoided by monitoring the control variable and the deviation from the target. Any out of control points in the controller variable corresponding to an unusual large compensation for a disturbance may alarm the engineer that there is a special cause in the system. Similarly, any unusual errors will be seen through the charts monitoring deviation from the target. Another criticism is that the implementation of EPC may result in suboptimal compensation. This may happen if the disturbance models are wrongly chosen or parameter estimate is inaccurate. In most cases the disturbance is assumed to be the integrated moving average, and EWMA is used to forecast the next disturbance to apply control to. The EWMA smoothing constant used for industrial disturbances is often less than 0.3. Hence the inflation of process variance due to a wrong model and inaccurate parameter estimates is not severe. In addition, EWMA provides a good estimate even if the process model is not precise IMA.

Suitability of EPC and SPC for a process depends on following factors [43]:

1. When adjustment costs and/or adjustment errors are high it is better not to implement EPC.
2. When the measurement errors are high it is not advisable to implement EPC.
3. Finally, when the sampling is slow relative to the process dynamics (the rate at which quality characteristics react to a change in controllable factor), the process observed will be uncorrelated and SPC alone will be sufficient.

It should be noted that reducing sampling frequency for SPC purposes may be useful only if the original process is stationary. Reducing sampling frequency of a nonstationary process still produces nonstationary processes; an adjustment strategy of EPC based on prediction is advisable in such cases [44].

SPC charts can be effective in reducing process variation when assignable causes exist in EPC controlled processes. Algorithmic statistical process control (ASPC) is a framework that unifies EPC and SPC. Its is a control system that employs EPC to regulate the processes and then uses SPC methods to monitor the EPC controlled processes to detect any departure from the assumed system model and revise it if necessary [45, 46, 47]. There are two methods used to integrate SPC and EPC: the first one is to monitor the output of the EPC controlled process. The second one is to monitor the EPC control action. One of the issues with monitoring output of EPC controlled process is that, when assignable causes exist, outputs are contaminated by control action and are autocorrelated. This results in a small window of opportunity for detection of assignable causes. However, monitoring control action can be more efficient in some autocorrelated processes, while monitoring output can be more efficient in others [48]. The performance of monitoring an EPC controlled process depends on:

1. Monitoring data stream-controlled output or control action.
2. EPC control scheme employed-MMSE control of PID control.
3. Underlying autocorrelation structure.

Standard schemes such as Shewhart control charts, CUSUM charts, EWMA charts, proportional-integral feedback control and various feedforward schemes are appropriate or inappropriate, depending on the choice of parameters in the model, the objective about assignable cause, the nature of noise, process dynamics, off-target costs, adjustment costs and observation costs of the process [49].

Joint monitoring schemes using either Hotelling's approach or Bonferroni's approach can overcome the shortcomings of conventional SPC for controlled processes and both are quite efficient over a wide region of parameter space [50]. Among the various multivariate procedures for joint monitoring of process output and control actions combined $U_o - U_\infty$ charts [51, 52] show good performance followed by T^2 [50] and M [53] charts [52].

Table 15.3. A nonstationary process

Period (t)	y (t)
1	–0.30515
2	–0.26328
3	0.365147
4	0.592477
5	1.093311
6	–0.22287
7	0.566752
8	0.749081
9	3.021413
10	2.051145
11	2.952504
12	0.657239
13	1.888777
14	1.245216
15	–0.28757
16	2.081887
17	1.086115
18	1.452894
19	0.678882
20	3.688226
21	1.854147
22	2.034564
23	2.999517
24	0.373992
25	1.187501
26	2.76128
27	2.769371
28	2.299462
29	3.680006
30	2.028539
31	2.488729
32	3.363288
33	2.901176
34	3.410425
35	4.187757
36	3.429498
37	4.083043
38	1.676501
39	2.232224
40	3.11156
41	3.574948
42	4.109802
43	1.951855
44	3.592194
45	3.055566
46	2.128624
47	3.903199
48	3.813223
49	2.165239
50	5.220853
51	3.405461
52	3.256172

References

[1] Deming WE..Out of the crisis. Cambridge, MA: Center for Advanced Engineering Study MIT, 1986

[2] MacGregor JF. A different view of funnel experiment. Journal of Quality Technology 1990; 22:255–259.

[3] Box GEP, Luceno A. Statistical control by monitoring and feedback adjustment. New York: Wiley, 1997.

[4] Box GEP, Jenkins GM. Some statistical aspects of adaptive optimization and control. Royal Statistical Society Journal 1962; 24(B): 297–343.

[5] Box GEP, Jenkins GM. Mathematical models for adaptive control and optimization. AI Chem. E Symposium series 1965; (4): 61–68.

[6] Box GEP, Jenkins GM. Time series analysis: forecasting and control. Holden-Day, San Fransisco, 1970.
[7] Box GEP, Jenkins GM, MacGregor JF. Some recent advances in forecasting and control, Part II. Applied Statistics 1974; 23(2):128–179.
[8] Chartfield C. The analysis of time series: An introduction. London: Chapman and Hall, 1989.
[9] Box GEP, Jenkins GM, Reinsel GC. Time series analysis, forecasting and control. Upper Saddle River, NJ: Prentice-Hall, 1994.
[10] Montogmery DC, Johnson LA, Gardiner JS. Forecasting and time series analysis. New York: McGraw Hill, 1990.
[11] Ljung L System identification: Theory for users 2nd edition. Upper Saddle River, NJ.: Prentice Hall, 1999.
[12] Ljung L, Soderstrom T. Theory and practice of recursive identification. Cambridge, MA: MIT Press, 1983,
[13] Richard A Davies, Peter J Brockwell. Time series: Theory and methods. Berlin: Springer, 1996.
[14] Cressie. A graphical procedure for determining non stationary in time series. J Of American Statistical Association 1998; 83:1108–1116.
[15] Box GEP, Kramer T. Statistical process monitoring and feedback adjustment: A discussion. Technometrics 1992;34:251–275.
[16] Luceno A. Performance of discrete feedback adjustment scheme with dead band under stationary v/s nonstationary stochastic disturbance. Technometrics 1998; 40(3):223–233.
[17] Box GEP, Hunter WG, Hunter JS. Statistics for experimenters, an introduction to design, analysis and model building. New York: Wiley, 1978.
[18] Box GEP. Feedback control by manual adjustment. Quality Engineering 1991a; 4:143–151.
[19] Box GEP, Jenkins GM. Further contributions to adaptive optimization and control: Simultaneous estimation of dynamics: Non-zero costs. Bulletin of International Statistical Institute 1963; 34:943–974.
[20] Box GEP, Luceno A. Sampling interval and action limit for discrete feedback adjustment. Technometrics 1994; 36(4): 369–378.
[21] Kramer T Process control from economic point of view. University of Wisconsin- Madison, 1989.
[22] Crowder SV. An SPC model for short production runs: Minimizing expected costs. Technometrics 1992; 34: 64–73.
[23] Jensen KL, Vardeman SB. Optimal adjustment in the presence of deterministic process drift and random adjustment error. Technometrics 1993; 35:376–389.
[24] Grubbs FE. An optimal procedure for setting machines or adjusting processes. Journal of Quality technology 1954 /1983; 15(4):186–189.
[25] Sullo P, Vandevan M. Optimal adjustment strategies for a process with run to run variation and 0-1 quality loss. IIE Trans. 1999; 31:1135–1145.
[26] Pan R., Del Castillo E. Scheduling methods for the statistical setup adjustment problem. International Journal of Productions Research 2003; (41): 1467–1481
[27] Del Castillo, Hurwitz A. Run to run process control: A review and some extensions. Journal of Quality Technology 1997; 33(2):153–166.
[28] Moyne J, Del Castillo E, Hurwitz A. Run to run control in semiconductor manufacturing. CRC Boca Rotan Washington D.C, 2001.
[29] Ingolfsson A, Sachs E. Stability and sensitivity of a EWMA controller. Journal of Quality Technology 1993; 25: 271–287.
[30] Butler SW, Stephani JA. Supervisory run to run control of a polysilicon gate etche using in situ ellipsometry. IEEE Trans. Semiconductor Manufact. 1994; 7(2):193–201.
[31] Del Castillo E. Statistical process adjustment for quality control. New York : Wiley, 2002.
[32] Del Castillo E. Long run and transient analysis of a double EWMA feedback controller. IIE Transactions 1999; 31(12):1157–1169.
[33] Tseng ST, Chou RJ, Lee SP. Statistical design of double EWMA controller. Applied Stochastic Models in Business and Industry 2002b; 18(3):313–322.
[34] Tseng ST, Hsu NJ. Sample size determination for achieving asymptotic stability of a double EWMA control scheme. IEEE Trans. Semiconductor Manufact. 2005; 18 (1):104–111.
[35] Del Castillo E. Some properties of EWMA feedback quality adjustment scheme for drifting disturbances. Journal of Quality Technology 2001a; 29(2):184–196.
[36] Tseng ST, Song W, Chang Y. An initial intercept iteratively adjusted controller: An enhanced double EWMA feedback control. IEEE Trans. Semiconductor Manufact. 2005; 18(3):448–457.
[37] Tseng ST, Yeh AB, Tsung. FG, Chan Y. A study of variable EWMA controller. IEEE Trans. Semiconductor Manufact. 2003; 16(4):633–643.
[38] Patterson OD, Dong X, Pramod P, Nair VN. Methodology for feedback variable selection for control of semiconductor manufacturing processes–Part 1: Analytical and simulation

resutsl. IEEE Trans. Semiconductor Manufact. 2003; Nov,16(4):575–587.

[39] Patterson OD, Dong X, Pramod P, Nair VN. Methodology for feedback variable selection for control of semiconductor manufacturing processes–Part 2: Application to reactive ion etching. IEEE Trans. Semiconductor Manufact. 2003; Nov.,16(4):588–597.

[40] Firth SK, Campbell WJ, Toprac A, Edgar TF. Just-in-time adaptive disturbance estimation for run to run control of semiconductor processes. IEEE Trans. Semiconductor Manufact. 2006; Aug., 19(3):298–315.

[41] Chen A, Guo R. Age based double EWMA controllers and its application to CMP processes. IEEE Trans. Semiconductor Manufact. 2001; Feb.,14(1):11–19.

[42] Tseng ST, Chou.R, Lee S. A study on a multivariate EWMA controller. IIE Trans. 2002; 34: 541–549.

[43] Hunter JS. Beyond the Shewhart SPC paradigm. Dept of Statistics Southern Methodist University Dallas, 1994.

[44] MacGregor JF. Optimal choice of the sampling interval for discrete process control. Technometrics 1976; 18(2):151–160.

[45] Vander WSA, Tucker WT, Faltin FW, Doganaksoy N. Algorithmic statistical process control: Concepts and applications. Technometrics 1992; 34(3):286–297.

[46] Vander WSA, Vaderman SB. Discussion: integrating SPC and APC. Technometrics 1992; 34(3):278–281.

[47] Tucker WT, Faltin FW, Vander WSA. ASPC: an elaboration. Technometrics 1993;35(4):363–375.

[48] Jing W. SPC monitoring of MMSE- and PI-controlled processes. Journal of Quality Technology 2002; 34 (4):.384–398.

[49] Box GEP, Kramer T. Statistical process control and automatic process control- a discussion. report 41. Center for Quality and Productivity Improvement. Uni. of Wisconsin Madison, 1990.

[50] Tsung F, Shi J, Wu CFJ., Joint monitoring of PID controlled processes. Journal of Quality Technology 1999; 31:275–285.

[51] Jiang W. A joint SPC monitoring scheme for APC controlled processes. IIE Transactions 2004;36: 1201–1210.

[52] Jiang W, Shu L, Tsung F. A comparative study of joint monitoring schemes for APC processes. Quality and Reliability Engineering International 2006; 22:939–952.

[53] Hayter AJ, Tsui KL. Identification and quantification in multivariate quality control problems. Journal of Quality Technology 1994; 26:197–208.

16

Six Sigma – Status and Trends

U. Dinesh Kumar

QMIS Group, Indian Institute of Management, Bannerghatta Road, Bangalore 560076, India

Abstract: Six Sigma originated from Motorola as a simple statistical technique to reduce defects in manufacturing in the 1980s with an objective to improve quality by improving manufacturing processes. Today, Six Sigma is an important corporate strategy used by many companies to improve their business processes, create a competitive advantage, and to increase market share and profitability. A recent study conducted by DynCorp, USA, has revealed that the effectiveness of Six Sigma as a tool for process improvement is the highest compared to other process improvement tools such as total quality management (TQM) and ISO 9000. The main objective of this chapter is to provide an overview of Six Sigma and discuss emerging trends in Six Sigma such as Design for Six Sigma (DFSS) and Lean Six Sigma (LSS).

16.1 Introduction

Quality has been an important discriminating factor for many centuries now. Many strategies have evolved over the last several decades to improve the quality of manufacturing and service organizations. Six Sigma as a method to reduce manufacturing defects was introduced more than 20 years ago by William Smith of Motorola. Motorola was the first company to win the Malcom Baldridge National Quality Award in 1988 for developing what later became to known as the Six Sigma methodology. The Six Sigma methodology tries to achieve a process capability index value of 2, whereas in the past a process capability index value of 1 was an acceptable quality standard. In the past (prior to Six Sigma), the upper and lower specification limits for a process were set at the three sigma level ($\mu + 3\sigma$ and $\mu - 3\sigma$), whereas the corresponding limits in a Six Sigma processes are set at $\mu + 6\sigma$ and $\mu - 6\sigma$, respectively, where μ is the process mean and σ is the standard deviation of the process.

Six Sigma is an extension of other quality initiatives such as Deming's statistical quality control and total quality management (TQM). Most management strategies on quality improvement are customer focused and Six Sigma is also focused around meeting the customer expectations as the main objective. It is difficult to define a methodology like Six Sigma, since it is a combination of several tools and techniques. Kwak and Anbari [1] define Six Sigma as a combination of TQM with strong customer focused additional data analysis plus financial results and project management. That is:

Six Sigma = TQM + stronger customer focus + additional data analysis tools + financial results + project management

Six Sigma evolved by synergizing most of the earlier quality improvement tools and created very few tools of its own. While Six Sigma was being developed as a technique to reduce defects in manufacturing, the world of business was witnessing the rise of the service industry. Currently, the growth of the service industry is much higher than that of the manufacturing industry in most developed nations. Service quality plays a crucial role in the profitability of a business, since customer defections can significantly reduce the profit of the service industry [2]. From an operational strategy Six Sigma has evolved as a competitive corporate strategy and a new mantra of the corporate world. Even traditional companies that adhere to conventional management methods have started embracing Six Sigma and believe that Six Sigma is a method of substance that will increase market share and profitability [3].

Although Six Sigma originated within the manufacturing industry to reduce the wastes due to manufacturing process deficiencies, it is now used by almost all industries including service industries such as healthcare management, banking, *etc.* [4–8] None of the previous quality improvement initiatives has received such wide applications outside the manufacturing industry.

The term Six Sigma was coined by William Smith, a reliability engineer at Motorola, and is a registered trade mark of Motorola. Smith pioneered the concept of Six Sigma to deal with the failure rate experienced by systems developed by Motorola. Smith proposed the Six Sigma process as a goal to improve the reliability and quality of the product. The initial days of Six Sigma were focused at reducing defects by improving manufacturing processes. Six Sigma uses five macro phases for process improvement called the DMAIC (define, measure, analyze, improve and control) procedure. DMAIC cycle is a standardized methodology used by Six Sigma to achieve process improvement iteratively. However, the DMAIC cycle itself has many similarities with Deming's "plan-do-check-act" (PDCA) cycle. A differentiating factor between TQM and Six Sigma is that Six Sigma provides a well defined target for quality that the process defect rate should not be more than 3.4 defects per million opportunities. This focused target along with the well defined DMAIC procedure probably resulted in a higher success rate for Six Sigma compared to TQM. Another important difference between Six Sigma and TQM is that Six Sigma is mostly a business results oriented model compared to the return on investment orientation of TQM [9].

Six Sigma can be used as an operational strategy to reduce the number of defects or as a business strategy to improve business processes and evolve new business models. Many proponents of Six Sigma stress that its power lies in the fact that it can be used as a business strategy to improve market share and profitability. The Design for Six Sigma (DFSS) concept uses Six Sigma to as a strategy to design and develop new products compared to the traditional Six Sigma, which aims to reduce the defects. A survey conducted by DynCorp revealed that the concept of Six Sigma is rated highly compared to many other process improvement techniques [10]. Table 16.1 shows the ratings of Six Sigma and other process improvement techniques based on the survey conducted by the DynCorp to determine the most successful process improvement tool.

For manufacturing companies the benefit of Six Sigma results from reduction in the number of

Table 16.1. Rating of Six Sigma and other process improvement techniques [10]

Process improvement tool	Impact
Six Sigma	53.6 %
Process mapping	35.3 %
Root cause analysis	33.5 %
Cause and effect analysis	31.3 %
Lean thinking and manufacturing	26.3 %
ISO 9001	21.0 %
Statistical process control	20.1 %
Design of experiments	17.4 %
Total quality management	10.3 %
Malcolm Baldridge criteria	9.8 %
Knowledge management	5.8 %

defects due to improved manufacturing processes. However, the direct benefit of Six Sigma decreases as the sigma quality level increases. The sigma quality level is a measure of process defect rate. A higher sigma level indicates that the process results in fewer defects, whereas a lower sigma means higher defect rate. The sigma quality level can be used for benchmarking purposes and helps to measure quality of the process. The sigma quality level also helps to set a realistic target for improvement of process quality during the DMAIC cycle of process improvement. Improving a process from sigma level 3 to sigma level 4 reduces the number of defects per million opportunities (DPMO) from 66,811 to 6,210, whereas improving the sigma level from 5 sigma to 6 sigma reduces the DPMO from 233 to 3.4. However, more effort may be required to improve a process from sigma level 5 to 6 compared to improving a process from sigma level 3 to 4. Thus, any process improvement using Six Sigma requires careful analysis. That is, Six Sigma implementation may not always result in financial benefit. Dinesh Kumar *et al.* [11] developed a mathematical programming model to select various improvement opportunities in an optimal way.

Any improvement in the sigma level is likely to reduce the cost of poor quality (COPQ). The cost of poor quality as a result of manufacturing defects is a function of rework cost, excessive use of material, warranty related costs, and excessive use of resources. Assuming that COPQ is linearly related to the number of defects produced by the process, the benefit of a relative increase in the sigma level decreases [11]. The improving process may involve replacing the existing process with a new technology. Gowen and Tallon [12] point out that Six Sigma programs must take into consideration the level of technological intensity of the organization to determine the impact of Six Sigma. Replacing existing process with a new technology can be costly and if the resulting new process does not improve the sigma level significantly, the investment required to improve the process may not result in significant returns. Like any other process improvement technique, Six Sigma would also fail to deliver if the management fails to understand the cost of implementing Six Sigma and its effectiveness.

The objective of this chapter is to review the current status of Six Sigma and recent trends. In Section 16.2, the metrics used by Six Sigma is presented. Selection of projects for implementation of Six Sigma plays a crucial role in the success of Six Sigma implementation. Section 16.3 discusses issues in Six Sigma project selection. Section 16.4 deals with DMAIC methodology and an example is used to illustrate the DMAIC cycle. The trends in Six Sigma such as Design for Six Sigma and Lean Six Sigma are discussed in Section 16.5. Conclusions are presented in Section 16.6.

16.2 Management by Metrics

Six Sigma is without any doubt an important strategies used by companies irrespective of their business. Six Sigma is very popular among manufacturing companies and is equally, if not more, popular among service organizations. One of the reasons for the success of Six Sigma can be attributed to its metrics. Other than sigma level quality, all other measures in Six Sigma can be traced to concepts such as statistical process control and total quality management. In this section we will define and establish the relationship between the following fundamental Six Sigma metrics:

1. yield
2. defects per million opportunities (DPMO)
3. sigma quality level

16.2.1 Yield

Yield, Y, is an important measure of process capability and is defined as the ratio of the total number of defect free units to the total number of units produced (or opportunities):

$$Yield = Y = \frac{\text{Number of defect free units}}{\text{Number of opportunites}} \times 100\% \tag{16.1}$$

At Six Sigma quality, the yield is 99.99966%. This value of course assumes that the process mean may

shift up to 1.5σ, where σ denotes the process standard deviation. In the absence of any shift in the process mean, the yield at Six Sigma quality will be 99.9999998%. That is, two defects per billion opportunities.

16.2.2 Defects *per* Million Opportunities (DPMO)

Defects per million opportunities (DPMO) measures the number of defects in a process in terms of million opportunities. It is also known as ppm (defects counted in parts per million). However, it is very difficult to get the complete data of defects in one million opportunities for most processes. Usually DPMO is estimated from a sample of units produced. DPMO is calculated from estimating the defects per unit (DPU) using the following expression:

$$DPMO = DPU \times \mathbf{10^6}. \qquad (16.2)$$

The above equation can be written as:

$$DPMO = \frac{\text{Number of defects}}{\text{Number of opportunities}} \times \mathbf{10^6}. \qquad (16.3)$$

16.2.3 The Sigma Quality Level

The sigma quality level is a measure of quality of the output produced by an organization. The higher the sigma level, the better the quality. In other words, a process with a high sigma level will result in fewer defects. The sigma level or sigma quality level can be understood as the Z value of the standard normal distribution under the assumption that there is no shift in the process mean. Several polynomial approximations [13] are available to calculate the value of Z. Similarly, when there is a shift in the process mean (say as much as Λσ), then the following mathematical relationship [14] can be used to approximate the value of Z (sigma level):

$$Z = \Lambda + \left(Q - \frac{C_0 + C_1 Q + C_2 Q^2}{\mathbf{1} + d_1 Q + d_2 Q^2 + d_3 Q^3} \right), \qquad (16.4)$$

where C_0 = 2.515517, C_1 = 0.802853, C_2 = 0.010328, d_1 = 1.432788, d_2 = 0.189269, d_3 = 0.001308 and,

$$Q = \sqrt{\ln\left(\left(\mathbf{1} - \frac{Y}{\mathbf{100}}\right)^{-2}\right)}, \qquad (16.5)$$

where Y is the process yield. In Excel® spreadsheet, the Sigma quality level can be calculated using the function NORMINV(Y, Λ, 1). Here, Λσ is the shift in the process mean over a long period of time. Six Sigma uses several context specific measures and a few of them are listed below:

1. Time to market.
2. Percentage of sales from new product.
3. Ratio of units returned over units sold.

16.3 Six Sigma Project Selection

Six Sigma is a project based problem solving methodology. In Six Sigma, each process improvement opportunity is treated as a project. Thus it is important to choose a project that would result in maximum benefit. Several Six Sigma project selection methodologies have been reported in the literature [14]. The chosen project should align with the strategic objectives of the organization. Pande *et al.* [15] classify Six Sigma project selection criteria into three categories: 1) business benefits criteria, 2) feasibility criteria, and 3) organization impact criteria. Business benefits criteria include issues such as the *impact on customers*, the *impact on business strategy*, and the *impact on core competencies*, *financial impact* and *urgency*. Feasibility criteria for Six Sigma project selection include criteria such as *resources needed, expertise available, complexity* and *probability of success*. Learning benefits and cross-functional benefits are listed under organizational impact criteria. Harry and Schroeder [16] propose the following criteria for Six Sigma project selection: 1) DPMO, 2) net cost savings, 3) cost of poor quality, 4) cycle time, 5) customer satisfaction, 6) capacity, and 7) internal performance. Banuelas *et al.* [17] list the following six criteria as critical for Six Sigma project selection.

1. Customer impact.
2. Financial impact.
3. Top management commitment.
4. Measurable and feasible.
5. Learning and growth.
6. Connected to business strategy and core competence.

The most frequently used methodology for project selection is the analytic hierarchy process (AHP). AHP is a multi-criteria decision making tool, which selects a best solution to a problem from a set of alternatives by assigning weights to multiple criteria. For Six Sigma projects, the following criteria are considered in AHP:

1. Duration (time required to complete the Six Sigma project).
2. Project cost.
3. Probability of success.
4. Strategic fit of the project.
5. Increase in customer satisfaction.
6. Increase in Sigma quality level.
7. Reduction in cost of poor quality (CoPQ)
8. Manpower requirement (Six Sigma green belts and Six Sigma black belts).

The above list of criteria is only representative and not exhaustive. AHP identifies the strength with which one alternative (alternative Six Sigma project) dominates the other and comes out with an overall priority list. This task is achieved by normalizing the pair-wise comparison matrices. For more details about Six Sigma project selection using AHP the reader may refer to Dinesh Kumar *et al.* [14]. Once a project is chosen for Six Sigma implementation, it goes through the DMAIC methodology, which implements Six Sigma solution systematically.

16.4 DMAIC Methodology

DMAIC (pronounced De-MAY-ick) is at the center of every Six Sigma project. DMAIC stands for five stages of Six Sigma methodology, namely, define, measure, analyze, improve and control. The tasks performed during these five stages of DMAIC are described in the following paragraphs:

Define

The main focus of the *define* stage is to identify the problem in terms of critical to quality (CTQ) parameters. The problem is defined in terms of some deficiency in CTQ parameters. In other words, in the define stage the problem with respect to one or more CTQ parameters is identified.

Measure

During the m*easure* stage an appropriate metric is used to measure the current process capability. The main objective during this stage is to establish the current performance of the process and measure the gap in the process performance and set target for improvement.

Analyze

In this stage, the cause and effect relationship between process performance and the process inputs are identified. The causes for performance gap measured in terms of CTQs are identified and solutions to the problems are generated. The best solution is then chosen to improve the process performance.

Improve

The main focus during this stage is to implement the solution to the problem identified during the define stage and target set during the Measure stage. Several optimization techniques are used to solve the problem in an optimal way.

Control

Sustaining the improvement obtained is equally important as achieving the improvement itself. In the control stage of the DMAIC cycle several statistical tools are used to sustain the quality improvement achieved using the previous four stages. The strength of DMAIC lies in its tool box. The methodology uses several mathematical and statistical tools and techniques to identify and solve the problem. A few of the tools and techniques used during various stages of DMAIC cycle is shown in Table 16.2. It should be noted that a particular tool may be used in more than one stage of the DMAIC cycle, since the most tools are context specific.

Table 16.2. DMAIC tool box

Define	Measure	Analyze	Improve	Control
Quality function deployment (QFD) Pareto diagram cause and effect diagram Analytic hierarchy process Kano model	Balanced scorecard Defects per million opportunities (DPMO) Sigma quality level Pareto diagram	Failure modes effects and criticality analysis Design of experiments Data mining Regression analysis 5 whys	Concept selection Pugh matrix QFD Mathematical programming Analytic hierarchy process Regression Pugh matrix	Statistical process control Process capability analysis Control charts

16.4.1 DMAIC Case: Engineer Tank

In this section we demonstrate the DAMIC procedure using an engineer tank case. The data used in this case example are for demonstration purposes only. Engineer tanks are used on the battlefield to undertake engineering tasks. This vehicle's primary task on the battlefield is to open routes. Its tasks include providing a route across short gaps, countering mines by clearing routes across mine fields and obstacle breaching and clearance (by digging and bulldozing). The functional elements for the armored vehicle are: mobility, surveillance, and communications, Lethality and survivability. During the development of the engineer tank engine, reliability targets were set and these targets are shown in Table 16.3.

The failure data collected from 70 engines are shown in Table 16.4. These failures have resulted in unscheduled maintenance of the engine. The time to failure data given in Table 16.4 is analyzed using a statistical software package MINITAB to find the best fit probability distribution. The best fit in this case is a Weibull distribution with scale parameter $\eta = 246.361$ and shape parameter $\beta = 1.286$. The corresponding mean time between failures, MTBF, value is 228.05 hours.

The analysis of in-service data shows that the achieved MTBF is much less than the target value of 420 hours. Improvement of reliability in this case is a good candidate for Six Sigma project and the DMAIC methodology. The DMAIC procedure for the reliability improvement in this case is discussed in the following example.

Table 16.3. Target reliability measures for engineer tank engine

Metric	Target: engine hours
Mean time between failure (MTBF)	420
Mean time between mission critical failures (MTBMCF)	3500
Mean time between routine overhaul	13500

Table 16.4. Failure data (failures resulting in unscheduled maintenance)

215	114	247	122	91	291	194	315	241	9
95	378	425	252	22	153	195	165	130	451
456	350	105	275	294	232	441	94	360	202
18	50	68	244	126	557	168	64	99	323
42	560	232	198	27	947	239	89	325	273
178	33	997	75	126	23	416	247	292	216
210	36	46	223	284	52	223	454	151	88

The define stage, as mentioned earlier, basically identifies the problem.

Poor reliability of the engineer tank engine is a major concern and thus reliability improvement forms the basis for remaining four stages of DMAIC cycle. The measure stage of the DMAIC cycle identifies the gap in the target and achieved reliability of the tank engine. The reliability of the engine is measured using the engine hours and based on the analysis of the in-service data it is found that the actual reliability of the engine is 228.05 hours against the target of 420 hours. To achieve the target MTBF of 420 hours, an almost 85% increase in reliability is required from the current level of 228.05 hours MTBF.

During the analyze stage the actual causes of reliability problems are analyzed. Figure 16.1 shows failure cause Pareto for engine failures. It is evident from Figure 16.1 that dust ingestion is a major cause of failure followed by mechanical failures and overheat. Since armored vehicles work in an environment hostile to air filters, it is expected that dust ingestion is a major cause for failure of engines.

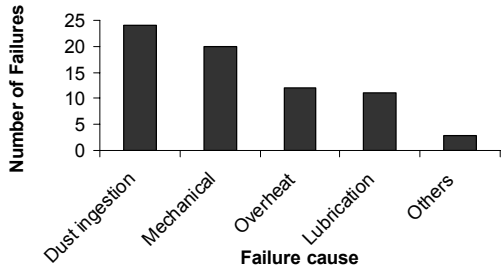


Figure 16.1. Failure cause Pareto

During the improve stage, the objective is to generate solutions to solve the reliability problem; in this case, it would be to design an air-filter that can reduce the engine failures due to dust ingestion. However, one should also look at alternative ways of improving the reliability since re-designing the air-filter may not be the optimal solution to the problem (that is, either it may not be feasible or cost effective). It may easier to eliminate other failure causes than dust ingestion, such as providing a better cooling system to reduce failures due to overheat. Once the optimal solution has been identified, one should go ahead and implement the solution. Strategies to sustain the reliability improvement would be objective of the control stage. Control charts and online health monitoring systems can be used to meet the objective of the control stage.

16.5 Trends in Six Sigma

Six Sigma has gone through a dramatic change over the last decade. Although it started as a tool to reduce waste it is now used as a strategy to run businesses. In this section, we shall discuss Design for Six Sigma (DFSS) and Lean Six Sigma (LSS), two of the most powerful tools used by industries to improve profitability.

16.5.1 Design for Six Sigma

Six Sigma is not just a technique to reduce defects. It has evolved into a successful strategy deployed by many companies to improve the design of products and services. For many companies, an important business objective is to improve profitability and Six Sigma is successfully applied to achieve this by using the Design for Six Sigma (DFSS) approach [18, 19].

In DFSS, design engineers interpret and design the functionality of customer requirements by optimizing both customer needs and organizational objectives. DFSS consists of five stages, namely (i) define, (ii) measure, (iii) analyze, (iv) design, and (v) verify, and is popularly known as DMADV methodology. DMADV is appropriate for new product development where the product and processes do not exist. The activities during various stages in DMADV are given below:

- *Define*: Develop new product development (NPD) strategy, scope of the NPD project.
- *Measure:* Understand the customer requirements and critical to quality parameters.
- *Analyze:* Develop conceptual design after analyzing various design options.

- *Design:* Develop detailed design of the product and processes.
- *Verify:* Develop prototype to verify the effectiveness of the design and check whether the product has met all the goals set during the previous stages of product development.

It is believed that Six Sigma is more effective when it is used for designing new products and processes rather than improving existing processes, since in many cases replacing existing processes may not be an easy task. Thus, the maximum benefit of Six Sigma is realized when it is used for design and development of new products.

16.5.2 Lean Six Sigma

Lean Six Sigma (LSS) combines the lean concepts along with Six Sigma to achieve higher performance. Lean management originated from Toyoto production systems (TPS). TPS is also credited with creating just-in-time (JIT) methodology, a key method in lean management [20]. Lean concepts try to improve efficiency of a process by eliminating the waste in the process/system, whereas Six Sigma makes a process effective by reducing process variation and improving process capability. Combining lean and Six Sigma results in an efficient and effective process improvement tool. That is, lean Six Sigma synergies the speed of lean with accuracy of Six Sigma.

The principle of lean Six Sigma [21] is that the activities, which cause the customers' critical quality issues creating longest delays in any process, offer greatest opportunity for improvement. The current trend in Six Sigma is to apply lean concepts first and then apply Six Sigma. That is, first make the process efficient by eliminating process waste and then effective by eliminating process variation. Here process waste refers to overproduction, inventory lead time, process cycle time. *etc*. George [21] has reported several applications of LSS in various fields including manufacturing, finance, logistics and supply chain management.

16.6 Conclusions

Six Sigma has become a new corporate mantra. Since its beginning in late the 1980s, Six Sigma has evolved into the most powerful tool of the 21st century so far. Kwak and Anbari [1] compiled the benefits of Six Sigma across various industries. Table 16.5 shows the benefits of Six Sigma as reported by them. It should be noted that Six Sigma is not just a tool for quality improvement but an organizational culture to achieve excellence in business processes. However, like any other process improvement tool, Six Sigma should be used with caution. Six Sigma is not a one stop solution to all problems. Before any company wishes to embrace Six Sigma, it should realize that achieving Six Sigma quality is not possible with the existing knowledge in most cases. In fact, in most cases, achieving even five sigma quality itself is impossible. However, this does not in anyway reduce the power of the Six Sigma concept. It is probably the best methodology currently available for continuous process improvement. Any company that would like to embrace Six Sigma should set a realistic target for quality improvement measured in terms of the sigma quality level. For example, if a company at present is a 3 sigma company, then a realistic improvement target would be a 3.5 sigma level rather than a 5 or 6 sigma level.

Any tool comes with its own limitations. For small and medium size (SMEs) companies, a large scale Six Sigma implementation may not be financially feasible. SMEs should target small process improvement, which in many cases tends to improve the quality and profitability of the company. Six Sigma is without any doubt a champion tool among all the process improvement tools.

Table 16.5. Reported benefits of Six Sigma [1, 11, 22–26]

Company	Metrics/Measures	Benefits/Savings
Motorola (1992)	In-process defect levels	150 time reduction
Raytheon aircraft integration system	Depot maintenance inspection time	Reduced 88% as measured in days
GE (Railcar leasing business)	Turnaround time at repair shops	62% reduction
Allied Signal (Honeywell) – Lamination plant in South Carolina	Capacity, Cycle Time Inventory, and On time delivery	Up 50%, Down 50%, Down 50% and increased to near 100%
Huges aircraft's missile system group / wave soldering operations	Quality / productivity	Improved 1000% and Improved 500%
Continental Teves/ Brake and axle assemblies	Failure rate	More than 50% reduction in failure rate
Borg Warner Turbo Systems	Financial	$ 1.5 million annually since 2002
General Electric	Financial	$ 2 billion in 1999
Motorola	Financial	$15 billion over 11 years
Dow Chemical – Rail delivery project	Financial	Savings of $2.45 million in capital expenditures
DuPont/Yerkes plant in New York	Financial	Savings of more than $ 25 million
Telefonica de Espana (2001)	Financial	Savings and increase in revenue 30 million Euro in first 10 months
Texas Instruments	Financial	$ 600 Million
Johnson and Johnson	Financial	$ 150 Million
Honeywell	Financial	$ 1.2 Billion
Ford Motor Company / Exterior Surface defects	Financial	$500,000

References

[1] Kwak YH, Anbari FT. Benefits, obstacles and future of Six Sigma. Technovation: The International Journal of Technological Innovation, Entrepreneurship and Technology Management 2006; 26(5-6):708–715.

[2] Reichheld FF, Sasser WE. Zero Defections: Quality Comes to Services. Harvard Business Review 1990;105–111.

[3] Harry MJ. Six Sigma: A breakthrough strategy for profitability. Quality Progress 1998; 31(5): 60–64.

[4] Krupar J. Yes, Six Sigma can work for financial institutions. ABA Banking Journal 2003; 95(9):93–94.

[5] Antony J. Six Sigma in the UK service organizations: Results from a pilot survey, Managerial Auditing Journal, 2004; 19(8):1006–1013.

[6] Chakrabarty A, Tan KC. The current state of Six Sigma application in services, Managing Service Quality, 2007; 17(2):194–208.

[7] Antony J, Fergusson C. Six Sigma in a software industry: Results from a pilot study. Managerial Auditing Journal 2004; 19:1025–1032.

[8] Moorman DW. On the quest for Six Sigma. The American Journal of Surgery 2005; 189:253–258.

[9] Bertels T (Editor). Rath and Strong's Six Sigma Leadership Handbook, Wiley, New York, 2003.

[10] Dusharme D. Six Sigma survey: Big success… but what about the other 98 percent? Quality Digest, accessed on 10th February 2006 at http://www.qualitydigest.com/feb03/articles/01_article.shtml.

[11] Dinesh Kumar U, Nowicki D, Ramírez-Márquez José Emmanuel, Verma D. Optimal selection of process improvements in a Six Sigma

implementation. Forthcoming International Journal of Production Economics 2007.

[12] Gowen RC, Tallon WJ. Effect of technological intensity on the relationship among Six Sigma design, electronic business, and competitive advantage: A dynamic capability model. Journal of High Technology Management Research 2005; 16, 59–87.

[13] Abramovitz M, Stegun IA. Handbook of Mathematical Functions. Dover, New York. 1972.

[14] Dinesh Kumar U, Crocker J, Chitra T, Saranga H. Reliability and Six Sigma, Springer, Berlin, 2006.

[15] Pande PS, Neuman RP, Cavanagh RR. The Six Sigma way – How GE, Motorola and other top companies are honing their performance. Tata McGraw Hill, New Delhi, 2003.

[16] Harry MJ, Schroeder R. Six Sigma: The breakthrough management strategy revolutionizing the world's top corporations. Currency Doubleday, New York, NY, 2000.

[17] Banuelas R, Tennant C, Tuersley I, Tang S. Selection of Six Sigma projects in UK. The TQM Magazine 2006; 18(5):514–527.

[18] Antony J, Banuelas R. Design for Six Sigma. IIE Manufacturing Engineering 2002; 81(1):119–121.

[19] Brue G, Launsby R. Design for Six Sigma. McGraw Hill, New York, 2003.

[20] Arnheiter ED, Maleyeff J. The integration of lean management and Six Sigma. The TQM Magazine 2005; 17(1): 5–18.

[21] George ML. Lean Six Sigma. Tata McGraw Hill, New Delhi, 2002.

[22] Antony J, Banuelas R. Key ingredients for the effective implementation of Six Sigma program. Measuring Business Excellence 2002; 6(2):20–27.

[23] Buss P, Ivey N. Dow chemical design for Six Sigma rail delivery project. IEEE Computer Society; Proceedings of the Simulation Conference 2001; winter; Dec.9–12, Arlington, VA, U.S.A.: 1248–1251.

[24] De Feo J, Bar-El Z, Creating strategic change more efficiently with a new design for Six Sigma process. Journal of Change Management 2002; 3(1): 60–80.

[25] McClusky R. The rise, fall and revival of Six Sigma. Measuring Business Excellence 2001; (4)2:6–17.

[26] Weiner M. Six Sigma. Communication World. 2004; 21(1):26–29.

17

Computer Based Robust Engineering

Rajesh Jugulum[1] and Jagmeet Singh[2]

[1]MIT and Bank of America, Boston, Massachusetts, USA
[2]GE Energy, Greenville, South Carolina, USA

Abstract: In this chapter, new trends in robust engineering (RE) are discussed. The chapter discusses use of robust engineering principles in simulation based experiments and in software testing with illustrative examples.

17.1 Introduction

Robustness can be defined as designing a product in such a way that the level of its performance in various customer usage conditions is same as that in the nominal conditions. Robust engineering methods (also known as Taguchi methods) are intended as cost-effective methods to improve the performance of a product by reducing its variability in the customer usage conditions. Because they are intended to improve companies' competitive positions in the market, these methods have attracted the attention of many industries and academic community across the globe. The methods of robust engineering are the result of research effort led by Genichi Taguchi.

Quality, in the context of robust engineering can be classified into two types:

1. customer driven quality
2. engineered quality

Customer quality leads to the size of the market segment. It includes product features such as color, size, appearance and function. The market size becomes bigger as the customer quality gets better. Customer quality is addressed during the product planning stage. Customer quality is extremely important to create the new market. On the other hand, engineered quality includes defects, failures, noise, vibrations, pollution, *etc*. While the customer quality defines the market size, the engineered quality helps in winning the market share within the segment.

All problems of engineered quality are caused by three types of uncontrollable factors (called noise factors).

I. Various usage conditions
   - environmental conditions

II. Deterioration and wear
   - degradation over time

III. Individual difference
   - manufacturing imperfection robust engineering (RE) methods or Taguchi methods (TM) aim at improving the engineered quality.

While designing a new product optimization for robustness can be achieved in the following three stages:

1. concept design
2. parameter design
3. toleranced design

Although there are three stages, most of the RE applications focus on parameter design optimization and tolerance design. It is widely acknowledged that the gains in terms of robustness will be much higher if a design process is started with a robust concept selected in the concept stage. Techniques like Pugh concept selection, the theory of inventive problem solving (TRIZ), and axiomatic design and P-diagram strategies developed for conceptual robustness through Ford-MIT collaboration by [1] can be used to achieve robustness at the concept level.

The methods of robust engineering are developed based on the following five principles:

1. Measurement of function using energy transformation.
2. Take advantage of interactions between control and noise factors.
3. Use of orthogonal arrays and signal-to-noise ratios.
4. Two-step optimization.
5. Tolerance design using quality loss functions and on-line quality engineering.

Taguchi [2] and Phadke [3] provide a detailed discussion on the principles of TM. These principles have been successfully applied in many engineering applications to improve the performance of the product/process. They are proved to be extremely useful and cost effective. A brief illustration of these principles is given below:

1. *Measurement of Function Using Energy Transformation*
   The most important aspect of Taguchi methods (TM) is to find a suitable function (called the ideal function) that governs the energy transformation in the system from input signal to output response. It is important to maximize the energy transformation by minimizing the effect of uncontrollable or noise factors. In the Taguchi approach measure the functionality of the system to improve the product performance (quality). The energy transformation is measured in terms of signal to noise (S/N) ratios. A higher S/N ratio means better energy transformation and hence functionality of the system.
2. *Take Advantage of Interactions Between Control and Noise Factors*
   In TM, we are not interested in measuring the interaction between the control factors, but rather in the interaction between the control and noise factors, since the objective is to make the design robust against the noise factors.
3. *Use of Orthogonal Arrays (OA's) and Signal-to-noise Ratios (S/N Ratios)*
   OAs are used to minimize the number of runs (or combinations) needed for the experiment. Usually, many people are of the opinion that the application of OA is TM. However, it should be noted that the application of OAs is only a part of TM. S/N ratios are used as a measure of the functionality of the system.
4. *Two-Step Optimization*
   After conducting the experiment, the factor-level combination for the optimal design is selected with the help of two-step optimization. In two-step optimization, the first step is to minimize the variability (maximize S/N ratios). In the second step, the sensitivity (mean) is adjusted to the desired level. It is easier to adjust the mean after minimizing the variability.
5. *Tolerance Design Using Quality Loss Function and On-line Quality Engineering*
   While the first four principles are related to parameter design, the fifth principle is related to the tolerance design and on-line quality engineering. Having determined the best settings using parameter design, the tolerancing is done with the help of quality loss function. If the performance deviates from the target there is a loss associated with the deviation. This loss is termed as the loss

to the society. It is proportional to the square of the deviation. It is recommended to design the safety factors using this approach. On-line QE is used to monitor the process performance and detect the changes in the process.

17.1.1 Concepts of Robust Engineering

17.1.1.1 Parameter Diagram (P-diagram)

This is a block diagram, which is often quite helpful to represent a product or process or a system. In Figure 17.1, the energy transformation takes place between input signal (**M**) and the output response (**y**). The goal is to maximize energy transformation by adjusting control factors (**C**) settings in the presence of noise factors (**N**).

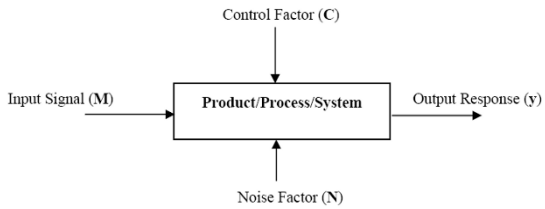


Figure 17.1. Parameter diagram or p-diagram

1. *Signal Factors (M)*
   These are the factors that are set by the user/operator to attain the target performance or to express the intended output. For example, the steering angle is a signal factor because the steering angle is a signal factor for the steering mechanism of an automobile. The signal factors are selected by the engineer based on the engineering knowledge. Sometimes even more than one signal factor is used in combination, for example, one signal factor may be used for coarse tuning and one for fine-tuning.
2. *Control Factors (C)*
   These are the product parameters specification whose values are the responsibility of the designer. Each of the control factors can take more than one value, which will be referred to as levels. It is the objective of the design activity to determine the best levels of these factors that will make product insensitive to noise factors or robust against noise factors. Robustness is the insensitivity to the noise factors.
3. *Noise Factors (N)*
   Noise factors are the uncontrollable factors. They influence the output **y** and their levels change from one unit of the product to another, from one environment to another and from time to time. As mentioned before noise factors can be one of or a combination of the following three types: 1) Various usage conditions, 2) deterioration and wear, and 3) individual difference.

17.1.1.2 Experimental Design

Experimental design is a subject with a set of techniques and a body of knowledge to help the investigator to conduct experiments in a better way, analyze results of experiments and find the optimal parameter combination for design to achieve intended objectives. In experimental design, various factors affecting the product/ process performance are varied (by changing their values called levels) in a systematic fashion to estimate their effects on product/ process variability to find the optimal factor combination for a robust design. There is an extensive literature on this subject. A typical experimental design cycle is shown in Figure 17.2.

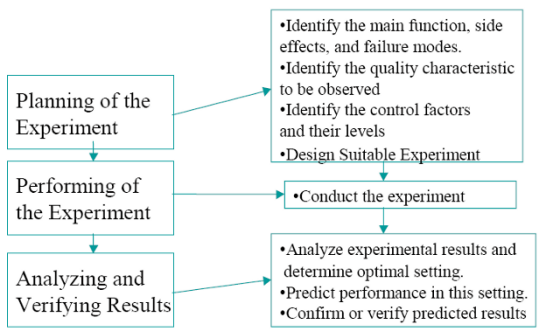


Figure 17.2. Experimental design cycle

Types of Experiments

There are typically two types of experiments, full factorial experiments and fractional factorial experiments. In full factorial experiments, all combinations of factors are studied. All main effects and interaction effects can be estimated with the results of such an experiment. In fractional factorial experiments, a fraction of the total number of experiments is studied. This is done to reduce cost, material and time. Main effects and selected interactions can be estimated with such experimental results. The orthogonal array is an example of this type. In robust engineering, the main role of OAs is to permit engineers to evaluate a product design with respect to robustness against noise, and cost involved by changing settings of control factors. OA is an inspection device to prevent a "poor design" from going "down stream".

17.1.1.3 Signal to noise (S/N) Ratios

The term S/N ratio means signal to noise ratio. S/N ratio tries to capture the magnitude of true information (*i.e.*, signals) after making some adjustment for uncontrollable variation (*i.e.*, noise). From Figure 17.1, we can say that a system consists of a set of activities or functions that are designed to perform a specific operation and produce an intended or desired result by minimizing functional variations due to noise factors. In engineering systems the input energy is converted into an intended output through laws of physics.

These engineered systems are designed to deliver specific results as required by customers. All engineered systems are governed by an ideal relationship between the input and the output. This relationship is referred to as the ideal function. The robust engineering approach uses this relation and brings the system closer to the ideal state (Figure 17.3).

If the all input energy is converted into output, then there will be no energy losses. As a result there would be no squeaks, rattles, noise, scrap, rework, quality control personnel, customer service agents, complaint departments, warranty claims, *etc*. Unfortunately it does not happen because reality is much different from ideal situations.

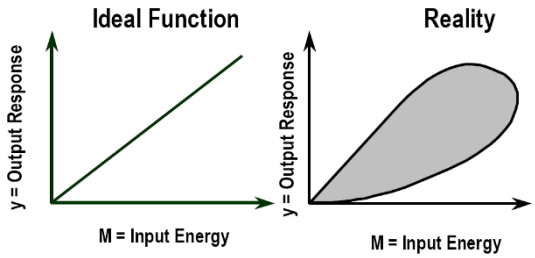


Figure 17.3. Ideal function and reality

In reality there is energy loss when input is transformed to output. This loss occurs because of variability and noise factors. This energy loss will create unintended functions. Further, the bigger the energy loss, the bigger the problems.

The S/N ratio is a measure of robustness as it measures energy transformation that occurs within a design. The S/N ratio is expressed as:

S/N ratio = ratio of energy (or power) that is transformed into intended output and energy (or power) that is transformed into unintended output;

= ratio of useful energy and harmful energy

= ratio of work done by signal and work done by the noise

A higher S/N ratio is more robust than the system's function.

17.1.2 Simulation Based Experiments

Earlier the experiments are performed as hardware experiments. However, the present day trend is towards simulated based experiments. Computer simulations are quite important in robust engineering because:

- Simulated experiments play a significant role in reducing product development time because there is no need to conduct all hardware experiments.
- Simulated based robust engineering can serve as a key strategy for research and development.
- They help to conduct functionality based analysis.

- Simulated experiments are typically inexpensive, less time consuming, more informative and many control factors can be studied.

Once a simulation method is available, it is extremely important to optimize the concept for its robustness. The results of simulated experiments are analyzed by calculating S/N ratios and sensitivities. However, the optimal combination is tried using hardware experimentation to confirm the results. This book focuses only on simulation based experiments. While using simulated based experiments, it is important to select suitable signals, noise factors and output response.

The example given Section 17.1.2.1 explains how to conduct simulation based experiments. This example also explains the differences between Taguchi methods of robust engineering with other methods of design of experiments.

17.1.2.1 Example

Consider a circuit stability design as a simple example with a theoretical equation.

The output current, **y** in amperes of an alternating-current circuit with resistance, *R*, and self-inductance, *L*, is given by Equation 17.1 below,

$$\mathbf{y} = \frac{V}{\sqrt{R^2 + (2\pi f L)^2}}, \qquad (17.1)$$

where:

V: input alternating–current voltage (V)
R: resistance (Ω)
f: frequency of input alternating current (Hz)
L: self-inductance (H) and, $\omega = 2\pi f$.

The target value of output current y is 10 amps. If there is a shift of at least 4 amps during use by the consumer, the circuit no longer functions. The target value of **y** is 10 amps and the tolerance is 10 $\pm$ 4 amps.

The purpose of parameter design is to determine the parameter levels (normal values and types) of a system of elements. For example, it determines whether the nominal value of resistance, *R*, in the circuit is to be 1 or 9. The purpose of tolerance design is to determine the tolerance around the nominal value of the parameter.

Classification of Factors: Control Factors and Noise Factor:

Those variables in the equation whose central values and levels the designer can select and control are the control factors.

The input voltage is 100 volts AC in the case of a household source, and because the designer cannot alter this, it is not a control factor. Neither is the frequency, *f*, a control factor.

Only *R* and *L* are control factors. The designer sets the resistance value at 1Ω, 3Ω, or 9Ω. The same is true with regard to self-inductance, *L*. It is obvious that since the target value of the output current is given as 10 amps, in this case, once one decides on the central value of the resistance, *R*, the central value of the inductance, *L*, will be determined by the equation.

When there are three or more control factors, it is best not to consider such limiting conditions. The reason for this is that it is more advantageous to adjust the output to the target value by changing the levels of those control factors that have little influence on stability after an optimum design for stability has been determined. Factors that are favorable for adjustment are factors that can be used to change the output to the target value. These factors are sometimes termed signal factors. We can perform parallel analyses for the S/N ratio, and for the mean, which are measures of stability and sensitivity, and adjusts the mean after variability has been reduced. In the present case, we choose three levels of *R* and L independently, as follows:

$R_1 = 0.5$ (Ω), $R_2 = 5.0$ (Ω), $R_3 = 9.5$ (Ω),
$L_1 = 0.010$ (H), $L_2 = 0.020$ (H), $L_3 = 0.030$ (H).

An orthogonal array is used if the control factors are more numerous, but since there are only two here, we can use a two-way layout with full factorial experiment. An orthogonal array to which control factors have been assigned is termed an inner orthogonal array or control orthogonal array.

One should use as many control factors as possible, take a wide range of levels and assign only the main effects.

Next, let us examine noise factors. As described earlier, noise factor is a general term for a cause that disperses the target characteristic from the ideal value.

Dispersion by the environment consists of the following two factors in this example, and their levels are taken as follows:

Voltage of input source (V)	90	100 110
Frequency f (Hz)	50	60

The environmental temperature, *etc*., also changes the value of the resistance, R, and the coil inductance, L, although only slightly. However, changes due to deterioration of the resistance and coil are greater than the effects of environmental changes. After having considered changes due to dispersion of the initial-period value, deterioration, and environment, let us decide that the resistance, R, and coil inductance, L, are to have the following three levels:

First level	normal value x 0.9
Second level	nominal value
Third level	nominal value x 1.1

The levels of the noise factors are as given in Table 17.1. It should be noted that a prime has been affixed to symbols for the noise factors, R and L. In this instance, it means there is no error with respect to the noise factors V, R', and L' when they are at the second level. Frequency f is 50 Hz or 60 Hz, depending on the location in Japan. If one wishes to develop a product that can be used in both conditions, it is best to design it so that the output meets the target when the frequency is at 55 Hz, midway between the two. Sometimes one uses an intermediate value that has been weighted by the population ration.

Table 17.1. Noise factors and levels

Noise factor levels			
	First level	Second level	Third level
V	90	100	110 (V)
R'	-10	0	+10 (%)
f	50	55	60 (Hz)
L'	-10	0	+10 (%)

However, now, as is evident from Equation 17.1, the output becomes minimum with $V_1R_3'f_3L_3'$ and maximum with $V_3R_1'f_1L_1'$. If the direction of output changes is known when the noise factor levels are changed, all the noise factors can be compounded into a single factor. If the compound factor is expressed as N, it has two levels. In this case:

$N_1 =$ $V_1R_3'f_3L_3'$ minus side minimum value,
$N_2 =$ $V_3R_1'f_1L_1'$ plus side maximum value.

When we know which noise factor levels cause the output to become large, it is a good strategy to compound them so as to obtain one factor with two levels, or one factor with three levels, including the central level. When we do this, our noise factor becomes a single compounded factor, no matter how many factors are involved. Since one can determine the tendencies of all four noise factors in this example, they have been converted essentially into a single compounded noise factor, N, with two levels. Thus, we need merely investigate the value of the outgoing current for these two levels.

Compounding of noise factors is even more important when there is no theoretical equation. This is because with a theoretical equation, the calculation time is short, usually no more than several seconds. Even if noise factors are assigned to the columns of a separate orthogonal array, there is little improvement in the efficiency of calculation even with compounded noise factors of two levels as in our example. Compounding was necessary in the past when computers were not available. However, when there are too many noise factors, the orthogonal array becomes large and much time and expense is required, even with a

computer. In such case, it is still useful either to reduce the number of noise factors to a few important ones or to compound noise factors.

Parameter Design

Design calculations are performed (experiments are performed when there is no theoretical equation) for all combinations of the inner orthogonal array to which control factors *R* and *L* have been assigned (two-way layout, here) and the noise factor assignment (two-level noise factor here). This is the logical method for parameter design. The assignment is shown in the left half of Table 17.2.

Table 17.2. Calculations of S/N ratios and sensitivities

Assignment of Factors						
No.	*R*	*L*	Compound noise		S/N ratio η	Sensitivity S
			N_1	N_2		
1	1	1	21.5	38.5	7.6	29.2
2	1	2	10.8	19.4	7.5	23.2
3	1	3	7.2	13.0	7.4	19.7
4	2	1	13.1	20.7	9.7	24.3
5	2	2	9.0	15.2	8.5	21.4
6	2	3	6.6	11.5	8.0	18.8
7	3	1	8.0	12.2	10.4	20.0
8	3	2	6.8	10.7	9.6	18.6
9	3	3	5.5	9.1	8.9	17.0

The S/N ratio is the reciprocal of the square of the relative error (also termed the coefficient of variation, $\frac{\sigma}{m}$). Although the equation for the S/N ratio varies, depending on the type of quality characteristic, all S/N ratios have the same properties. When the S/N ratio becomes 10 times larger, the loss due to dispersion decreases to one-tenth.

The S/N ratio, η, is a measure for optimum design, and sensitivity, **S**, is used to select one (sometimes two or more) factor(s) by which to later adjust the mean value of the output is adjusted to the target value, if necessary.

To compare the levels of control factors, we construct a table of mean values for the S/N ration, η, and sensitivity, **S**. For example, in the case of R_1, $\boldsymbol{\eta}$ = 7.5 and **S** = 24.0.

In Table 17.3 the mean values are given for the other control factor levels.

Directing our attention to the measure of stability, the S/N Ratio, in Table 17.3, we can see that the optimum level of *R* is R_3, and the optimum level of *L* is L_1. Therefore, the optimum design is R_3L_1. This combination gives a mean value of 10.1 which is very close to the target value. If there is no difference between the mean value and the target value, we might consider this as an optimal design and therefore, we do not have to adjust control factors based on sensitivities. If there is a difference, it is required to compare the influence of the factors on the S/N ratio and on the sensitivity, and use a control factor or two whose effect on sensitivity is great compared with its effect on the S/N ratio in order to adjust the output to the target.

Table 17.3. Average factorial effects

	η	S
R_1	7.5	24.0
R_2	8.7	21.5
R_3	9.6	18.5

	η	S
L1	9.2	24.5
L2	8.5	21.1
L3	8.1	18.5

17.2 Robust Software Testing

17.2.1 Introduction

A good software [4] should perform its intended function under all combinations of the user conditions. These user conditions are referred to as

active signals and they are used to get the desired output. Examples of the active signals are: inserting the card, punching the personal identification number (PIN) and selecting the desired transaction in case of ATM machine; typing the web-site address, movement of mouse or use of key board for selecting the flight schedules, giving desired price information, *etc*., in the case of airline ticket booking using internet. For the given software the user conditions are unique and they may be very large in number. Usually, the designer tests the software performance under the user conditions separately (like one factor at a time experiments). Even after such tests, the software fails because of the presence of combination effects between the active signals. Therefore, the software designer must study all these effects and take appropriate corrective actions before the release of the software. To estimate these effects, the software should be tested under various combinations of the signals.

The different states of the signal are referred to as the different levels. For a given signal the number of levels may be very high. In the case of the ATM transaction example, the levels for the PIN number may be from 0001 to 9999. If the number such signals is very high, then the number of possible combinations will be in billions. Since it is not feasible to test the software under all the combinations, a procedure is necessary to minimize the number of combinations. This procedure should also be adequate for finding the effects of the signals and their combinations. Here we describe such a method that is developed by using the principles of robust engineering. The objective of this procedure is to obtain all possible two- factor effects by conducting all most the same number of experiments as in the case of one- factor at a time experiments. Since in most cases higher order effects (higher than the second order) are not important, it is sufficient to test only the two-factor effects.

17.2.2 Robust Engineering Methods for Software Testing

In this section, we will explain how the robust engineering methods [4] can be used for testing a software. This method of testing considers all the active signals. The important principles of robust engineering for software testing are as follows:

1. Measurement of the performance of the software under different combinations of the user conditions/active signals.
2. Use of orthogonal arrays to study two factor combinations.

Since there will be several levels of usage conditions, it is adequate to limit the number of levels to two or three. These levels should be selected in such a way that the entire spectrum of usage conditions is covered. Usually, the levels can be selected as low, middle, and high. Figure 17.4 is a *p*-diagram that shows the typical software testing arrangement used this approach. In Figure 17.4, the noise factors correspond to the hardware conditions for the software. For the ATM example, the noise factor is the condition of the ATM machine (old or new). Noise factors are not necessary for all software testing applications and hence this is shown in dotted box.

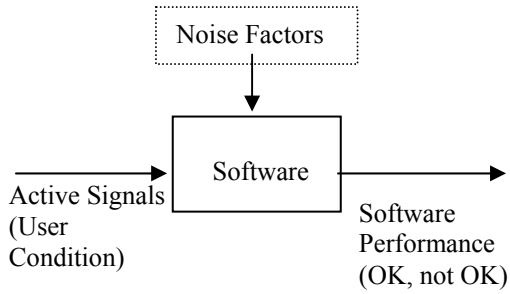


Figure 17.4. p-diagram for software testing

17.2.2.1 Role of Orthogonal Arrays

The purpose of using orthogonal arrays in the robust design or the design of experiments is to estimate the effects of several factors and required combination effects by minimizing the number of experiments. In the case of software testing, the purpose of using the OAs is to study all two-factor interactions with a minimum number of experiments. In fact the number of combinations with OAs is almost equal to the number of experiments to be conducted with one-factor-at-a time.

Let us suppose that there are 23 active signals, 11 with two levels and the remaining 12 with three levels. If we want to study all the two-factor combinations, the total number of experiments in this case would be the following.

The number of two level factor combinations = 4 x $({}^{11}C_2)$ = 220.

The number of three level factor combinations = 9 x $({}^{12}C_2)$ = 594.

The number of two-level and three-level factor combinations = 6 x 11 x 12 = 792

Total	1606

Depending on the number of signal factors and their levels, a suitable OA is selected. For this example, if a suitable OA is used the number of combinations to be run would be 36. The OAs are typically denoted as L_a (2^bX3^c). Where L denotes the Latin square design, a is the number of runs (combinations), b is the number of two-level signal factors and c is the number of three-level signal factors. The array to be used for this example is L_{36} ($2^{11}X3^{12}$).

17.2.3 Case Study

This method of software testing can be best explained with the help of following study conducted by Masahiko Suginuwa and Kazuya Inoue of Omron Company in Japan.

The software performance was required to be analyzed with 23 signals. These signals were numbered as A, B, C, U, V, W. For these factors suitable levels were selected. Table 17.4 shows some of the signal factors with chosen levels.

Table 17.4. Signal factors and number of levels

Signal	A	L	M	N	O	P	B	.....	W	K
#of levels	2	3	3	3	3	3	2	.....	3	2

The factors A, B, C, ..., U, V, W were assigned to the different columns of an L_{36} orthogonal array as described before. The results of the 36 combinations are shown in Table 17.5.

Table 17.5. Results of the different combinations of L_{36} array

Expt.no	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Response	1	0	0	0	1	1	0	1	0	0	1	1	0	0	0	0	0	0
Expt.no	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Response	0	0	0	1	0	1	0	0	0	0	1	0	1	0	0	0	0	0

0: Performance OK
1: Performance not OK

17.2.3.1 Analysis of Results

With the help of the results of Table 17.5, the two-way combination tables were constructed. As mentioned before, for the signals in the L_{36} array, the total number of two-way tables is 253. Out of all two-factor combinations, only two combinations were considered important, as these had 100% errors. These combinations are K2W1 and $Q1S1$. These combinations are shown with arrows in Table 17.6. The combinations of K and W and Q and S are shown separately in Tables 17.7 and Table 17.8.

Table 17.6. Two-factor combinations

	B 1	B 2	..	C 1	C 2	..	D 1	D 2	..	S 1	S 2	S 3	..	W 1	W 2	W 3
A 1	4	2		5	1		3	3						4	1	1
A 2	2	2		1	3		2	2						3	1	0
B 1				3	3		3	3						4	2	0
B 2				3	1		1	3						3	0	1
C 1							3	3						4	1	1
C 2							3	1						3	1	0
..																
..																
K 1														1	0	0
K 2														6	2	1
..																
..																
Q 1										4	0	0				
Q 2										1	1	0				
Q 3										1	1	2				
..																
S 1																
S 2																
S 3																
..																
V 1														3	0	1
V 2														3	1	0
V 3														1	1	0

Table 17.7. Combinations of K and W

	W1	W2	W3	Total
K1	1	0	0	1
K2	6	2	1	9
Total	7	2	1	10

Table 17.8. Combinations of *Q* and *S*

	S1	S2	S3	Total
Q1	4	0	0	4
Q2	1	1	0	2
Q3	1	1	2	4
Total	6	2	2	10

17.2.3.2 Debugging of Software

After identifying the significant combination effects, suitable corrective actions were taken. After taking the corrective actions again 36 runs of the L_{36} array were conducted. It was found that in these runs all the responses were 0's indicating that there were no bugs in the software

From the above discussions, the steps required to test software can be summarized as follows:

1. Identification of active signals and their levels.
2. Selection of a suitable OA for testing.
3. Conducting the test for different combinations of an OA.
4. Constructing the interaction tables.
5. Identification of significant interactions (by counting the number of 1's).

It should be noted that this method helps in reducing most of the bugs in given software. In some cases, even after applying this method the software may still have a few bugs because of the presence of higher order effects. Even if the number of active signals is very high, orthogonal arrays of higher size can be constructed to accommodate the signals.

Acknowledgements

The authors would like to thank Genichi Taguchi for allowing them to use his case studies in this chapter. They also would like to thank him for his tireless efforts to train industry people and explain the importance of robust engineering concepts.

References

[1] Frey Daniel D, Jugulum Rajesh. Robustness through invention Journal of Quality Engineering Society (Japan) 2002; 10(6).

[2] Taguchi Genichi. System of experimental design. ASI Press, Vol.1 and 2, 1987.

[3] Phadke Madhav S. Quality engineering using robust design. Prentice-Hall, Englewood Cliffs, NJ, 1989.

[4] Taguchi Genichi, Jugulum Rajesh. Taguchi methods for software testing. JUSE Software Quality Conference Proceedings 2000.

18

Integrating a Continual Improvement Process with the Product Development Program

Vivek "Vic" Nanda

Motorola Inc, 101 Tournament Drive, Horsham, PA 19044, USA

Abstract: The focus of this chapter is on the definition of a quality management system, deployment of the system, and continual quality improvement. The chapter describes a step-by-step process for defining a quality management system from scratch, provides guidance on training and facilitating deployment of the quality management system, and provides an overview of various mechanisms that can be leveraged for continual improvement of the quality management system after deployment.

18.1 Introduction

In recent times, while much work has been done and reported in the literature for developing process management infrastructures [1], defining product improvement mechanisms [2], and describing quality assurance engineering activities in a project [3], there appears to be a lack of succinct overview literature providing guidance on the establishment of a self-improving project based continual improvement process. Such a continual improvement process is one which leverages the standard product development process of an organization, tailors it for a project, monitors execution of the process in the project and then leads to empirically driven improvements in the organization's standard product development process. The focus of this chapter is on the definition of a quality management system, deployment of the system, and continual quality improvement.

18.2 Define a Quality Management System

18.2.1 Establish Management Commitment

First and foremost at the beginning of any improvement effort in a quality "conscious" organization is the establishment of management commitment, perhaps best exemplified by the identification of an executive sponsor who is accountable for providing the resources and establishing a vehicle to champion the establishment and continual improvement of the corporate quality management system (typically, the quality steering committee). It is not coincidence that "management responsibility" figures as the first element of the ISO-9001 quality standard [4] or as the first common feature: "commitment to perform" of all CMMi key process areas [5]. Sustained management commitment is key if any quality improvement initiative in an organization is to bear fruit.

18.2.2 Prepare a "Project" Plan

While the usage and continual improvement of an organization's quality infrastructure is an "ongoing" activity and becomes an inherent part of the product development process, the initial effort though is best implemented as an identified capability initiative. This means, launching a project with clearly identified objective(s) and scope, committed resources, identification of roles, and finally, specification of project phases (high level as a minimum) with associated milestones. Equally important is agreement on a "vision" for the quality system and its communication through the project plan. This predominantly relies on the selection of a quality model for usage by the organization, *e.g.*, ISO 9000 [4], CMMi [5]. The organization may also choose to select one model to set up the essentials of a sound quality management system and then graduate to a more rigorous model for increased maturity. A discussion on the relative strengths/weaknesses of one model relative to the others is beyond the scope of this chapter.

18.2.3 Define the Quality Policy

The definition of the system starts at the very top, by documenting the organization's quality commitment in the form of a "quality policy": the statement against which the quality management system is eventually assessed for adequacy and effectiveness.

18.2.4 Establish a Process Baseline

Establishing a process baseline, descriptive as opposed to prescriptive, is a fundamental activity at this stage. This involves mapping the overall product development process as a prerequisite. The task is simplified if the process is bounded as an end-to-end process (commencing at requirements from customer and ending at product delivery) and considering how the organization functional groups (and underlying processes) interact at this macro level [6]. It is also helpful to logically group and map the processes as per their "type":

- management processes,
- operative processes, and
- support processes.

This process map, preferably just a single chart, should identify the standard critical milestones (on phase completion, *e.g.*, end of project planning and definition phase) and the decision points for senior management review of the program and authorization of product release (typically, alpha release, beta release and final release [7]). The process map should also generally respect the time frames when a process starts or ends, although accurate time scaling is not required and not possible (because the standard process would have to be tailored for individual projects as per their unique characteristics [8]). The importance of defining this high-level process map should not be overlooked, it is to serve later as the process "containers" that are populated in the process baselining exercise when the processes are logically grouped and anchored in the appropriate process containers.

Process baselining is best accomplished by involving the practitioners in a "participative" project phase as opposed to processes being defined by a "process expert" in isolation. This is the time for demonstrating the previously pledged cross-functional commitment to the quality improvement initiative. Moreover, cross-functional participation in process definitions and reviews helps secure the buy-in by the various stakeholders and reduces "resistance to change" barriers in the deployment phase. Notice the use of the word "change", it was earlier recommended in this chapter to document descriptive (what is done) as opposed to prescriptive (what should be done) processes. At the same time, it is very likely and appropriate that the practitioners would like to incorporate minor incremental improvements to the processes due to observed deficiencies from their own work experiences. Also, the existing process may have to be updated to comply with the organization's chosen quality model's requirements. However, major rework of the processes is discouraged and unexpected at this stage, that would fall in the ambit of business process re-engineering and is beyond the scope of this chapter. Care should be taken to avoid creating

unnecessary "fat" (in terms of number of process definitions) and instead, focus on identifying and documenting key business processes and their interfaces, examples include (but are not limited to): software analysis, design and construction; test process; external and internal change request process; project planning, tracking and risk management process; configuration management; release management; customer call management and emergency provisioning of bug fixes.

Process ownership should be assigned as per the functional group in which most of the process activities are performed and process owner responsibilities for defining, monitoring and continually improving the process should be specified. The documentation of process definitions should be done using a common template containing pertinent process information. It should also be ensured that the documented processes are consistent in regards to deliverable "handshaking" and use of terminology.

Once all the processes have been identified and defined, the initially defined process map can be enhanced to map out all the individual processes and their interfaces to show the detailed process architecture. This detailed map can also serve as an excellent tool during subsequent process analysis and determining process bottlenecks.

18.2.5 Capture Process Assets

Although defining the business process involves much of the work during this stage of the development of the quality management system, there are other equally important elements that need to be defined as well: the organization's process assets [5]. For example, deliverable templates, quality glossary, best example documents, user guides, guideline documents, checklists and others.

These need to be readily accessible and centralized process assets library, as for instance required by CMMi maturity level 3 key process areas. A very relevant, but still evolving, approach that may be adopted is that of knowledge management. Knowledge management may be defined as the collective knowledge (including experience, skills, data and information) of an organization. It includes knowledge that resides internally as well as knowledge selectively acquired from external sources for improvement of the organization [9]. Thanks to the internet age, today the "corporate intranet" is a very good candidate to be used as a vehicle for knowledge management.

18.2.6 Establish a Metrics Program

Last but not least, a metrics program needs to be established for project, process and product measurements, preferably based on the goal-question-metrics (GQM) methodology [10]. Metrics are not only essential to monitor (define-measure-correct/control) and improve (define-measure-analyze-improve) a quality system but also help substantiate claims of quality improvement by quantifying benefits and help ensure continued senior management support. A discussion on the essentials of a sound measurement system is beyond the scope of this chapter, however, Daskalantonakis's reported work on the software measurement initiative at Motorola is recommended [11].

18.2.7 Define the Continual Improvement Process

With all the essential components of the quality management system defined, the key to deploying the infrastructure is the identification of the continual improvement process[1] of the organization. While this may not be a process definition *per se*, yet it is central to the success of the quality management system because it specifies how the various elements of the quality system interact to form a comprehensive support process. Note that the formality and rigorousness of an organization's continual improvement process varies depending on the duration of the product release cycle and nature of application: applications with longer lead time (say, greater

[1] The underlying fundamentals of quality process are based on measuring, analyzing, controlling/stabilizing and/or improving a process, and they can thus be substituted by other similar activities, as for example in the Six Sigma approach [12].

than nine months) and/or high degree of complexity (*e.g.*, mission critical software) typically lie at the higher end of the continual improvement process maturity spectrum. A recommended example of an organization's continual improvement process is as follows:

At the start of a project, the project team needs to proactively identify the planned deviations (and rationale) from the quality system processes and standards (process assets) and mechanism for requesting and approving process deviations after the start of the project. This exercise, called process tailoring, is based on the premise that "the one process fits all" approach to software engineering does not work, and an organization's standard software development process must be tailored to accommodate the unique characteristics and requirements of individual projects, after all no two projects are alike. Benefits of performing process tailoring and a recommended method are described in [8].

Once the project specific process has been defined as a result of this exercise, the project's software quality assurance plan can now be produced to describe: the planned quality assurance, control and management activities for the project. These include, specifying:

a) Quality objectives for each product release (alpha, beta and final release)[2], *e.g.*, product capability criteria in terms of number and severity of latent defects allowed at release; quality of product documentation at release; performance, reliability, and installability criteria for release, and confirmation of organizational preparedness to support the product after release.
b) Types of reviews planned for various project deliverables.
c) Types of testing planned (unit, system, independent, certification, performance testing).
d) Project metrics;.
e) Project and product audits planned, and so on.

A good example to refer to is the IEEE standard for software quality plans [13][3].

Once the project quality plan has been prepared and other project plans based on the project specific process have been defined, project execution is initiated. From a quality management standpoint, it involves ensuring project team peer reviews of project deliverables (degree of formality may depend on deliverable being review), capturing project metrics at key points (*e.g.*, defect fault density at alpha, beta, final release), ensuring project teams are on-track to achieve quality objectives defined for a release, product quality review (against predefined objectives) at release by project management team[4], auditing project teams to follow up that defined project plans (*e.g.*, test plans, development plan, *etc*.) are being faithfully implemented and finally performing a post-mortem on project completion to identify lessons learned and opportunities for improvement. These opportunities for improvement need to be reviewed to isolate vital few process change requests from trivial many. The metrics gathered need to be reviewed against the target values that were envisioned for the project and taking appropriate corrective action to address failures. The identified process changes need to be then assigned ownership and piloted in the next project as "capability initiatives". A successful pilot then typically leads to the acceptance of the original process change request as a "process improvement" and updating of the corporate process assets library to incorporate the change.

The continual improvement process described above is pictorially depicted in Figure 18.1.

[2] Obviously, to align with the maturity of the product during its development, stringency of criteria increases from alpha to beta to final release.

[3] Other disciplines of software engineering closely related to the quality management function – configuration management and software testing are excluded from this chapter. A look at the relevant IEEE standards is strongly recommended [14, 15].

[4] Recommended: release authorization by senior management only (typically, "director" level employees).

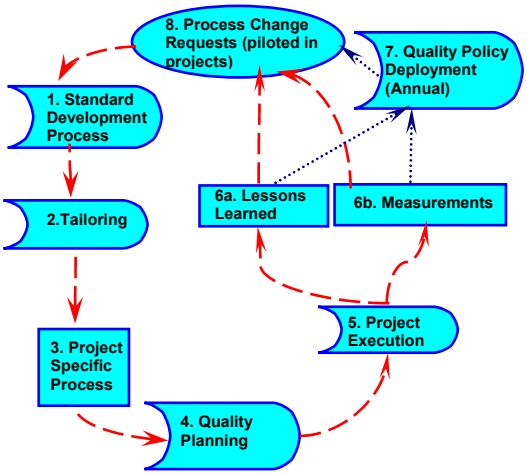


Figure 18.1. The continual improvement process

A word about quality manuals: A documented quality management system without a high level document describing its key elements is incomplete. Typical content of such a manual is: the organization's quality policy, management structure (including steering committee and process owner responsibilities), business processes, continual improvement process, continual improvement mechanisms, and traceability to the chosen quality model. The quality manual provides a brief yet sufficiently detailed overview of an organization's quality management system and is invaluable for both an organization's employees or for registrars, customer audits, and review by potential customers.

18.3 Deploy the Quality Management System

Deployment of a defined quality management system, in the form of formal training for the employees is essential to ensure faithful usage and improvement of the developed system. The training has to be not a one time exercise but ongoing, so as to account for new employees joining the organization or transfers/promotions within the organization and for communicating refinements to the quality management system. While key elements of the quality management system can be delivered as a common set of courses for all employees, much of the training has to be tailored for the employees as per their role within the organization. It is helpful to organize the training primarily on three tracks: management only (line management and process owners), practitioners by functional group (organizational departments) or all employees. The recommended content for the three training tracks is as follows (but not limited to):

a) *Management track*

How does the quality management system satisfy the chosen quality model's requirements; detailed training on the continual improvement process and communication of the organization's continual improvement mechanisms (refer to the "Continual Improvement" section of this chapter).

b) *Practitioner training by functional group*

Training on business process (what to do) the practitioner is part of; procedure level training (how to do it) and communicating relevant process assets of the quality management system.

c) *All employees*

Training on the key elements of the quality management system, for instance: quality policy, process map, purpose and scope of various business processes, structure/content of the process assets library and mechanism for providing feedback from experiential usage to process owners (to facilitate continual process improvement).

The initial analysis for determining the training audience can be done by developing a 2-D grid listing the quality management system elements *vs*. the above mentioned audience tracks[5]. The elements can then be logically grouped by

[5] Note that track 2 has to be decomposed into various sub-tracks by each functional group: *e.g.*, software development, software test, documentation (product manuals), customer support, *etc*.

audience and packaged as formal training courses, preferably starting with relatively brief overview course to increasingly detailed courses.

18.4 Continual Improvement

Continual improvement of an organization's defined quality management system cannot be stand-alone or in isolation from the project lifecycle. The continual improvement process was introduced earlier in this chapter for precisely this reason. Supplementary vehicles for continual improvement are identified below:

a) *Quality policy deployment*

The organization needs to formulate quality related goals over the, say, next three to five years and work towards them by means of formal quality policy deployment mechanisms.

b) *Audits*

The organization needs to leverage quality audits for exploring opportunities for improvement as opposed to compliance auditing [16]. While the project and product audits serve to primarily achieve "in-process control", the system audits are more appropriate for system improvements.

c) Employee suggestions

A mechanism facilitating submission, review and implementation of process improvement suggestions from employees during any project is recommended. This mechanism may be very similar to the one used for reviewing a project's lessons learned on completion. It facilitates in-process control and corrective action and may thus sometimes be advantageous over a post-mortem review.

18.5 Conclusions

This chapter outlines the essential steps for an organization to define and deploy a quality management system and to set up an infrastructure for continual improvement. It integrates the concept of a "continual improvement process" which includes practices to measure, analyze, improve and stabilize a process. The key steps and recommendations described in this chapter to establish a robust quality management system are summarized below for quick reference:

18.5.1 Key Steps and Recommendations

1. Establish management commitment for the company's quality management program and its continual improvement.
2. Execute the quality management system development as a project with set objectives, defined milestones and committed resources.
3. Define overall vision for the quality system with the selection of the guiding model and documentation of the quality policy.
4. Prepare a high-level process map to pictorially depict the business process of the organization along with the critical milestones.
5. Once a high-level process map has been developed and deployed, a finer grained process architecture map should be developed to map out all the processes of the organization. Such a mapping helps to better understand the interplay and relevance of the various business processes and also helps with focus for various quality initiatives, such as, TTM (time-to-market) improvements.
6. Prepare descriptive as opposed to prescriptive process descriptions with minor incremental improvements, if required.
7. Capture organization process assets to complement the defined processes and provide readily accessible "process support" during product development and maintenance. Further, leverage knowledge management concepts for implementing a process assets library.
8. Define a continual improvement process for the organization, *i.e.*, a process with the ultimate objective of driving continual

quality improvements in the development process.

9. Deploy the quality management system by means of executing a formal quality-training program. Such a training qualifies the practitioners to perform their work activities by using the quality management system elements and the QMS can be officially considered "switched on" once this training is complete, in other words, the system is now auditable.
10. Leverage other vehicles for continual quality improvement, such as: quality policy deployment, system audits, and employee suggestions.

References

[1] Magee Mark, Reizer Neal. An infrastructure for process management. Proceedings of the Software Engineering Process Group conference (SEPG-97), San Jose, USA.,1997; March.

[2] Haley Thomas. Software process improvement at Raytheon. IEEE Software 1996.

[3] Drabick Roger. A process model of software quality assurance/ software quality engineering. Software Quality Professional Journal 2000; 2(4).

[4] ANSI/ISO/ASQ 9001-2000: Quality Management Systems – Requirements. International Organization for Standardization (ISO), 2000.

[5] Capability Maturity Model® Integration, Version 1.2, Software Engineering Institute, Carnegie Mellon University, 2006.

[6] Nanda Vivek (Vic). Quality management system handbook for product development Companies. CRC Press, Boca Raton, FL, 2005.

[7] Pressman Roger. Software engineering: A practitioner's approach (Third Edition), McGraw Hill, New York, 1992.

[8] Hoffman Leo. Project tailoring of the standard software process. Proceedings of the Software Engineering Process Group Conference, San Jose, California, USA, 1997; March.

[9] William S. Ill, Planning for knowledge management. ASQ Quality Progress Magazine 2000; March.

[10] Basili Victor, Weiss DM. A methodology for collecting valid software engineering data. IEEE Transactions on Software Engineering 1984; Nov.

[11] Daskalantonakis Michael. A practical view of software measurement and implementation experiences within Motorola. IEEE Transactions on Software Engineering 1992; Nov.

[12] Blakesleet Jerome Jr. Implementing the Six Sigma solution. ASQ Quality Progress Magazine 1999; July.

[13] IEEE Standard for Software Quality Assurance Plans. IEEE Std 1989; 730.

[14] IEEE Standard for Software Configuration Management Plans. IEEE Std 1990; 828.

[15] IEEE Standard for Software Test Documentation. IEEE Std 1983; 829.

[16] Beeler Dewitt. Internal auditing: The big lies. ASQ Quality Progress Magazine 1999; May

19

Reliability Engineering: A Perspective

Krishna B. Misra

RAMS Consultants, India

Abstract: The most important attribute of performance is reliability and this is defined as the probability of failure free operation over a specified duration of time under a given set of conditions, which depend on location and the kind of application the item is put to. In designing for reliability, the objective must be to maximize inherent and operational reliability such that occurrences of failures are considerably reduced. Component or system reliability goals can be achieved through design and testing. Failures and consequently accidents can be avoided if their causes of can be traced and taken care of during the design process.

19.1 Introduction

The most important characteristic of product performance is reliability and there are several reasons why reliability is more important than before:

- Products are becoming more and more complex and unless reliability is improved, the performance may become inadequate.
- There exists a tough competition between the industrialized nations and only products with high reliability will eventually survive.
- There is a compulsion to minimize waste as the world population grows and the resources keep on shrinking.
- Product longevity implies less world pollution.

19.1.1 Definition

According to IEC definition, reliability is the capability of a product (or a system or a service) to perform its expected job under the specified conditions of use over an intended period of time. Obviously, this definition raises questions like:

- Can this capability be quantified?
- Can this quantification be used with all kinds of products and systems without resorting to any redefinition or modification on a case to case basis?
- Can this capability be used to compare the performance of different engineering designs and technologies for a product or a system and assess their suitability?

As an answer to all the above questions, we can say that if the capability is quantified through probability of satisfactory performance this provides us a very general approach to evaluate

relatively the performance of products and systems. The next important question then arises is: can this capability be engineered into products or systems? The answer is again affirmative and in fact our main concern in reliability engineering is to engineer reliability into products, equipment and systems.

Implicit in the IEC definition of reliability are three components, *viz.*, *probability* of *adequate operation,* over a *specified time* and under the *specified conditions of use.* These components need an explanation.

Adequate operation signifies that a failure of a product (or a system) does not necessarily constitute complete cessation of its operation, but it only represents that the product or the unit is not functioning within the intended bounds of performance or is not *operating satisfactorily*.

Mission time: is the *specified time* in the definition and can also be called *mission time.* Without specifying mission time, a figure of reliability has no meaning since reliability is dependent on mission time and decreases with the increase in length of mission time. The duration of mission time depends on the design objectives of a system and it is this length of time over which the system should not have any failures at all so that the desired mission of the system can be carried out successfully without being impaired or aborted. The choice of mission time exclusively depends upon the objective of the system.

Conditions of use basically refer to the *environmental conditions* under which the product or the system has to operate. In fact, the performance of a product can be adversely affected by these environmental conditions. Thus reliability is always dependent on specified environmental conditions. If there is a departure from the specified conditions; the intended level of performance of the product or system cannot be ensured and there is a risk that the product might even transit to a degraded performance level or even to a failure.

Further, the conditions of use render reliability engineering a challenging task. It can aptly be handled through indigenous know-how, experience and experimentation as the conditions of environment may vary considerably from place to place depending upon the geographical location.

A checklist of environmental factors that the reliability engineer may be face while designing his system is given in Table 19.1. There are two types of factors, *viz.*, *natural* and *induced*.

Table 19.1. Environmental factors that influence reliability

Natural	Induced
Electromagnetic-radiation	Acceleration
Electrostatic-discharge	Chemicals
Frost	Corona
Fungus	Electromagnetic-radiation
Gravity	Electrostatic-discharge
Humidity	Explosion
Lightning	Moisture
Pollution, air	Nuclear radiation
Pressure, high, low,	Shock, thermal
Vacuum	Space debris
Radiation, cosmic,	Temperature: high,
Rain	low,
Salt spray	Turbulence
Sand and dust	Vapour trails
Snow	Vibration:
Temperature	Mechanical ,
Wind	Vibration: acoustic

Each environmental factor requires determination of its impact on the operational and reliability characteristics of materials and parts comprising the system. This includes operational and maintenance environments as well as preoperational environments, when stresses imposed on parts during manufacturing assembly, inspection, testing, shipping and installation may have a significant impact on equipment reliability. Very often more than one environmental factor may be acting on parts or equipment. These combined or concurrent environments may be more detrimental to reliability than the effects of these single environments separately. For example, equipment may be exposed to a combination such as temperature, humidity, altitude, shock, and vibration, while it is being transported. Moreover, the superposition of effects of individual

environmental factors cannot predict the resulting influence that a combination of environmental factors will have on the reliability or performance of the equipment. In fact, the severity of the combination may be much more than individual effects added together. For example, the percentage of failures caused by temperature may be (40% of all failures) vibration (24%) and humidity (19%). Sand and dust (6%) and salinity (4%) but humidity combined with temperature can cause 75% of all failures. Humidity with a salty air environment (as may be common with coastal regions) can be a major cause of degradation of equipment performance since they promote corrosion effects in metallic components besides leading to the formation of surface films on non-metallic parts. Moisture absorption by insulating material can also induce conductivity and a dissipation factor of these materials. As pointed out earlier, the effects cannot be linearly extrapolated if two environments act simultaneously upon a product or a system. Sometimes, sudden changes of temperature may also induce a large amount of internal mechanical stresses in structural elements, particularly, when dissimilar materials are involved. The effect of thermal shock-induced stresses include cracking of seams, delamination, loss of hermeticity, leakage of fill gases, separation of encapsulating materials from components, and enclosure. Natural frequencies of items comprising equipment must also be considered in the design phase, since a resonant condition may greatly amplify subsystem deflection and may increase stresses beyond safe limits. A vibration environment can create relative motion between members and when combined with other environmental stresses, this motion can produce fret corrosion.

Therefore, in order to ensure reliability, environmental testing should form an integral part of performance demonstration. In fact, experimentation on the basis of actual environments envisaged acting upon a product or a system must be carried out or investigated into before finalizing a product design. An environmental stress test is commonly employed during the product design and development stage. For products that are in use over a long period of time, an accelerated life test is usually done in by shortening the time-to-failure by increasing the severity of loading that the product is supposed to bear under normal conditions in order to obtain meaningful results on reliability characteristics. For instance, electronic components may be tested at elevated temperatures in order to hasten the incidence of failures. Likewise, steel pipes used in nuclear power plants may be exposed to neutron irradiation that can increase the brittleness of steel causing brittle failure. However, overstressing is done to the extent that it does not change the product failure mode and mechanisms.

19.1.2 Some Hard Facts About Reliability

There are, however, certain notions that need to be clarified to a beginner in this area.

19.1.2.1 Death Is a Certain Event

Birth and death are certain events of life. This also applies to all man-made objects. It is a universal fact that anything that is born must die some day. Certainly in reliability, we do not or cannot eliminate natural death. A natural death is not considered as an undesired event in reliability but cessation of activity or function during the mission time is certainly an undesired event and is what we call a *failure* in reliability terminology. Our prime concern in reliability engineering is, therefore, to prevent failure of an item during its mission time and not outside it.

19.1.2.2 Failures Are Inevitable

Since, as mentioned earlier, it is not possible to eliminate failures completely, in reliability engineering we aim to prevent them as far as possible and to contain their influence on the functioning of system, if they do occur.

19.1.2.3 100% Reliability Is Impossible

A 100% reliability is possible only when a product or unit never ever fails. Whatever be the mission time, reliability can never be 100%. (Except theoretically, if mission time is zero, *i.e.*, we do not use it at all.) It can approach asymptotically to

unity and can be close to unity, *i.e.,* 0.999…9 but it can never be unity. Until there is a single chance of failure (or death, which is a certainty), reliability can never be unity.

19.1.2.4 The Instant of Failure Is Unpredictable

The instant of failure cannot be predicted. No mathematical equation or theory exists that can do this. The occurrence is just a chance or a random event. Therefore, it should be clear in our minds that the theory of reliability cannot predict the exact instant when a product or a system will fail. One should not hurriedly infer from this statement that reliability theory is imprecise but rahter only supports the statement that failures can occur any time and are random in nature.

19.1.2.5 Uncertainty of Results

Statistical and probabilistic methods are used for analyzing failure data, quantifying reliability during the prediction, measurement and testing phases. However, on account of the high level of uncertainty involved at various levels in the process, these can hardly be applied with the kind of precision and credibility that engineers are accustomed to when dealing with most other engineering problems. However, the mathematical and statistical methods in reliability analysis in fact allow us to have an idea of the uncertainty present.

19.1.3 Strategy in Reliability Engineering

The prioritized objectives of reliability engineering are:

- To apply engineering knowledge to understand and anticipate the possible causes of product or system failures and to take adequate measures to prevent them from occurring.
- To identify and check the failure mechanisms, which eventually lead to failures.
- Explore the ways of reducing the likelihood or frequency of failures despite the efforts to prevent them.
- To apply methods for estimating the reliability of new designs, and for analyzing reliability data with a view to improve future designs.

Basically, reliability engineering is the first and foremost application of good engineering, in the widest sense, during design, development, manufacture, and use.

19.1.4 Failure-related Terminology

There are several terms in vogue in reliability engineering, which should be defined to avoid confusion and for clarity of understanding.

Defect: A defect is the departure of a characteristic of an item from requirement.

Fault: A fault is the state of an item characterized by its inability to perform a required function.

Error: An error is a discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition.

Human error: This is a human action that produces an undesired result or consequence.

Bug: A bug is a software defect.

Failure: A failure is the cessation of the ability of an item to perform a required function.

However, a failure, in reliability engineering, has a wider connotation, which not only includes death but also the inability of an item to perform adequately over the mission time. Thus the definition of failure has been related to the level or quality of the desired performance. For example, if an electric power company guarantees that the voltage within the premises of a consumer shall be within ± 5% of the rated supply voltage, its failure to keep the supply voltage within these limits shall be construed as a failure of power supply. A failure here not only implies that no electric power is available but also an inadequate level of supply voltage. This broad definition of failure permits us to quantify the performance of a product vis-à-vis the expected level of performance.

Failure mechanism: A failure mechanism is a physical, chemical, thermal or metallurgical process that causes component characteristics to change beyond tolerance, which eventually leads to

a certain mode of component failure. Typical failure mechanisms can be electromigration, thermal instability, electrostatic field, corrosion, fatigue, *etc*.

Failure mode: A failure mode is the visible or observable effect by which a component failure is identified. A component can fail in more than one failure mode.

The examples are short circuit or open circuit mode of failure or degraded performance of electronic devices such as capacitors, diodes, *etc*., or valves stuck open or stuck closed in mechanical devices.

Several failure mechanisms may exist simultaneously at a point of time, eventually leading to a failure of a component in a particular mode. Two or more same failure mechanisms can lead different failure modes. All failure modes are known as *primary failures*.

Dependent Failures: When the failure of a component changes the operating stress on other components of a system, dependency exits and this increases the failure probability of other components.

Common mode of failure: This is a single failure mode that results into simultaneous failure of several components.

19.1.4.1 Types of Electrical Failures

Electronic or electrical components may fail in any of the following modes [54]:

- *Short circuit:* Diodes, transistors, capacitors may often fail in this mode.
- *Open circuit*: Resistors, crystals, *etc*. may often fail in this mode.
- *Degraded performance:* SCRs and capacitor aluminium may fail in this mode.
- *Functional failure:* Coils and relays may often fail in this mode.

In fact the relative frequency of occurrences of these failure modes can be different for different component types and these failure modes and their relative frequencies should be considered for a particular type of application of a component during the design of a system using these components. This makes reliability design a challenging task.

19.1.4.2 Types of Mechanical Failures

Depending upon the type of stress, the usual modes of failure in mechanical components [75, 88] can be enumerated as follows:

Material failures: This type of failure mainly occurs due to poor quality checks, fatigue cracks, weld defects, and small cracks and flaws. These defects actually reduce the allowable material strength and consequently lead to premature failure at the flawed spots.

Metallurgical failure: This failure is the result of extreme oxidation or operation in corrosive environment. Environmental factors such as heat, nuclear radiation, erosion, and corrosive media accelerate the occurrence of metallurgical failures. These are also referred as material failures.

Stress concentration failure: This type of failure occurs when uneven stress "flow" through a mechanical member. Usually, the concentration of stress occurs at sudden transitions from thick to thin gauges, at sudden variations in loading along a structure, at right-angle joints or at various attachment conditions.

Compressive failure: This failure occurs under compressive loads. The compressive failure often results in permanent deformation/cracking/ rupturing.

Bearing failure: This type of failure is similar in nature to the compressive failure and it usually occurs due to a round cylindrical surface bearing on either a flat or a concave surface like roller bearings in a race. The repeated loading may cause fatigue failures.

Tensile-yield-strength failure: This failure occurs under pure tensile stress, especially, when the applied stress exceeds the yield strength of member. Usually, it results in permanent deformation in the structure or a permanent set and is rarely catastrophic. The value of safety factors for this kind of failure could be as low as 1 (*i.e.,* design to yield) or 4 or 5 for pressure vessels and bridges.

Ultimate tensile-strength failure: This leads to a complete failure of the structure at a cross-section

and occurs only when the applied stress is greater than the ultimate tensile strength. The values of safety factors for this kind of failure may be as low as unity (*i.e.,* design to fail) or 5 or 6 for pressure vessels and bridges.

Bending failure: This failure occurs when one outer surface is in tension and the other surface is under compression and may therefore be referred as *combined failure.* The tensile rupture of the outer material is a representative of the bending failure.

Fatigue failures: Repeated cycling of the load causes metal fatigue. It is a progressive localized damage due to fluctuating stresses and strains on the material occurs mainly due to repeated loading or unloading (or partial unloading) of an item. The process consists of three stages, *viz.*, crack initiation, progressive crack growth, and finally sudden fracture of the remaining cross section.

Instability failure: This type of failure occurs in structural members such as columns and beams, particularly those manufactured using material where the loading is usually in compression. However, instability failure may also result because or torsion or by combined loading, *i.e.,* including bending and compression. Usually this type of failure is crippling or leads to a total failure of the structure. Experience indicates that a safety factor value of 2 is usually sufficient but a factor of less than 1.5 should not be used.

Shear loading failure: The occurrence of ultimate and yield failure takes place when the shear stress becomes greater than the strength of the material when applying high torsion or shear loads. Usually, these failures occur along 45^0 axis in relation to the principal axis.

Creep failures: Usually, long-term loads make elastic materials stretch even when they are stressed less than the normal yield strength of the material. The material stretches (creeps), if the load is maintained continuously and ultimately results in a rupture. Working at high temperatures accelerates creep.

Corrosion failures: Corrosion is a chemically induced damage to a material that results in deterioration of the material and its properties. This may result in failure of the component. Several factors should be considered during a failure analysis to determine the effect corrosion has played in a failure. For example, the type of corrosion, the corrosion rate, the extent of the corrosion, and the interaction between corrosion and other failure mechanisms.

Multiple failure modes: In fact, a single mechanical member can fail in various different modes of failures. For example, the gear is one of of the important and common components in mechanical equipment and the experience shows that amongst the various causes of gear failure**,** breakage (61.2%), surface fatigue (20.3%), wear (13.2%), and plastic flow (5.3%) are quite common.

19.1.5 Genesis of Failures

There can be several reasons why a product fails. Knowing the potential causes of failures is essential to prevent them. It is rarely possible to anticipate all causes of failures; therefore it is necessary to concentrate on the uncertainties involved in the reliability engineering effort during design, development, manufacture, and use. All the anticipated and possibly unanticipated causes of failure should be addressed to ensure that their occurrence is prevented or minimized. Broadly speaking, failures can occur if:

- The design is inherently weak. The list of possible reasons is endless, and every design problem presents the potential for errors, omissions, and commissions. The more complex the design, the greater is this potential!
- The stress applied exceeds the strength. Overstress failures can occur in spite of designers having provided some margin of safety. Electronic component specifications prescribe the maximum rated conditions of application, and circuit designers ensure that these rated values are not exceeded. In other words, they derate the component by ensuring that the stresses in worst conditions of use remain below the rated stress values. In the same way, mechanical designers know the properties of the materials being used (*e.g.,* ultimate tensile strength) and they ensure that there is an adequate margin of

safety between the strength of the component and the maximum applied stress. However, it is not possible to provide protection against every possible stress application, because failures in most cases can also be caused by variation in stress and strength values; there always exists some uncertainty about them. In fact, this allows us to define reliability in terms of the stress and strength distributions considering that they are random variables. To illustrate how the probability of failure can be computed from the knowledge of distributions of stress and strength, let us assume that the stress applied to a member is normally distributed with a density function $f_{\mathbf{s}}(\mathbf{S})$ with mean and variance given by $\mu_{\mathbf{S}}$ and $\sigma_{\mathbf{S}}$, respectively, and for the sake of simplicity, let us further assume that the strength of this member is determined from some non-destructive test and is determined to be S_1 – a fixed value. Obviously, the member can fail only if the stress is greater than the given strength, *i.e.,* S_1. This would mean that the probability of failure, Q is given by

$$Q \equiv P(\mathbf{s}>S_1) = \int_{S_1}^{\infty} f_{\mathbf{s}}(\mathbf{s})\, \mathrm{d}s, \qquad (19.1)$$

or the reliability of this member or unit would be:

$$R \equiv 1 - Q = 1 - \int_{S_1}^{\infty} f_{\mathbf{s}}(\mathbf{s})\mathrm{d}s = \int_{-\infty}^{S_1} f_{\mathbf{s}}(\mathbf{s})\, \mathrm{d}s = P(\mathbf{s} \le S_1)$$

The definition (19.1) provides unreliability of a component when the component has a known value of strength S_1 and is invariant. However when the variability of both stress and strength is considered, the probability of failure of the component is dependent on the area of overlap between the stress and strength distributions. Larger the area of overlap, higher is the probability of failure of the member. Now let us assume both stress and strength are variable and **s** and **S** represent the stress and strength random variables, respectively. Also the location parameters for their distributions are s_1 and S_1 for stress and strength, respectively. Therefore, the probability density functions for the stress would be given by:

$$f_{\mathbf{s}}(\mathbf{s}) = \frac{\alpha_{\mathbf{s}}}{\beta_{\mathbf{s}}}\left(\frac{\mathbf{s}-s_1}{\beta_{\mathbf{s}}}\right)^{\alpha_s - 1} \exp\left[-\left(\frac{\mathbf{s}-s_1}{\beta_{\mathbf{s}}}\right)^{\alpha_{\mathbf{s}}}\right],$$

where, s_1 is the location parameter and $\alpha_{\mathbf{s}}$, $\beta_{\mathbf{s}}$ are the shape and scale parameters for the stress distribution.

Similarly, the probability density function for strength can be

$$f_S(S) = \frac{\alpha_S}{\beta_S}\left(\frac{S-S_1}{\beta_S}\right)^{\alpha_S - 1} \exp\left[-\left(\frac{S-S_1}{\beta_S}\right)^{\alpha_S}\right], \quad S_1 \le S < \infty$$

where S_1 is the location parameter and $\alpha_s \beta_s$ are the shape and scale parameters for the strength distribution. Therefore, the probability of failure Q would be given by:

$$Q = P\{S < s\} = \int_{-\infty}^{\infty} [1 - F_s(S)] f_S(S) dS \qquad (19.2)$$

$$= \int_{S_1}^{\infty} \exp\left[-\left(\frac{S-s_1}{\beta_s}\right)^{\alpha_s}\right] \frac{\alpha_S}{\beta_S}\left(\frac{S-S_1}{\beta_S}\right)^{\alpha_S - 1} \exp\left[-\left(\frac{S-S_1}{\beta_S}\right)^{\alpha_S}\right] ds$$

If we substitute

$$\delta = \left(\frac{S-S_1}{\beta_S}\right)^{\alpha_S}, \text{ then } d\delta = \frac{\alpha_S}{\beta_S}\left(\frac{S-S_1}{\beta_S}\right)^{\alpha_S - 1} dS$$

and $S = \delta^{\frac{1}{\alpha}} S\beta_S + S_1$, we obtain $R = 1 - Q$, where

$$Q = P\{S < s\} = \int_0^{\infty} e^{-\delta} \exp\left[-\left\{\frac{\beta_S}{\beta_s}\delta^{\frac{1}{\alpha_S}} + \left(\frac{S_1 - s_1}{\beta_s}\right)\right\}^{\alpha_S}\right] d\delta$$

The integral in the above expression can be computed through numerical integration for various combinations of the parameters of stress and strength as suggested in [103]. Also, it is easy to realize that one can compute Q for various combinations of distributions for stress and strength (other than Gaussian) such as exponential, Weibull, lognormal or extreme value distributions following the same procedure. This approach, which may provide closed form expressions in some cases whereas in other cases numerical integration may have to be carried out, is generally used for

computing probability of failure of mechanical and structural members. For a more detailed discussion of the various cases, the reader is referred to Chapter 4 of [103]. Some other approaches such as that in [132] have also been proposed.

- The actual strength of any population of components varies and there are bound to be some that are relatively strong, others that are relatively weak, however a majority of them will have average strength. The applied loads can also vary. Here again the failure will not occur as long as the applied load does not exceed the strength or in other words, a high value of safety factor is used. However, if there is an overlap between the distributions of load and strength, and a load value in the high tail of the load distribution is applied to an item in the weak tail of the strength distribution so that there is overlap or interference between the distributions, then the failure will definitely occur.
- Failures can also be caused by wear out due to any mechanism or process that causes an item that is sufficiently strong at the start of its life to become weaker with the passage of time. Examples of such processes are material fatigue, wear between relatively moving surfaces that are in contact, corrosion, insulation deterioration, and the wear out mechanisms of light bulbs and fluorescent tubes. Initially the strength is adequate to withstand the applied loads, but as time passes weakening occurs and the strength decreases. In every case the average value falls and the spread of the strength distribution widens. This is also the reason why it is difficult to provide an accurate prediction of the lives of such products.
- Failures can also be caused by time-dependent mechanisms. Examples of such a mechanism are creep caused by simultaneous high temperature and tensile stress, as in turbine discs and fine solder joints, battery run-down, and progressive drift of component parameter values. Again the interested reader is referred to [103] for the time dependent cases.
- Other causes of failure can be sneaks. A sneak is a condition in which the system does not work properly even though every part does. Sneaks also occur in software designs..
- There are many other potential causes of failures, such as they can occur on account of errors, incorrect specifications in designs or software coding, or by faulty assembly or tests, by inadequate or improper maintenance, or by misuse.

Therefore, all failures have some cause and by proper anticipation, analysis and application, an engineer can reduce the chances of their occurrence. It is also true that all failures can in principle be prevented by identifying, studying and analyzing them. The O-ring seals on the space shuttle booster rockets were not classed as failures, until the ill-fated launch of Challenger. It is therefore necessary to know more about the reasons for failures and to anticipate them. A reliability engineer must be a hardcore pessimist when it comes to anticipating what can go wrong in a system and take all precautionary or remedial measures against failure but having done so, he should hope for the best and be an optimist.

19.1.6 Classification of Failures

Failures can be classified very broadly based on the causes of failures over the life span of a product. Figure 19.1 shows a typical characteristic of failures over all the three regions of the life span. If the failures occur during the early-life period or what is known as the *infancy period*, they are known as *early-life failures* or *quality failures*. Any substandard item would surely fail during its early life. The responsibility of quality failures, therefore, rightly rests with the manufacturer, as these failures can be attributed to his failure to use the right type of raw material or to control processes and to maintain high quality. As weak or substandard components fail during early life, the hazard rate of the product decreases rapidly. Early-life failures can be eliminated through debugging processes, which consist of operating the product for quite some time under simulated conditions of actual use. This would cause a vast majority of the substandard products to fail in early life and

product hazard rate reaches its lowest point at the end of this period (0-t_E) as shown in Figure 19.1. Beyond the point t_E, the useful life period of the product begins.

The failures that occur during the useful life period are designated as *catastrophic* or *chance failures* and are unpredictable due to their very nature. However, we can always quantify their likelihood statistically. Their rate of occurrence is generally constant during the entire life of a product. It is actually during this useful period of life that a product is utilized to its maximum. The catastrophic failures cannot be eliminated either through good debugging techniques or by the best maintenance practices, because they are caused by sudden stress accumulation beyond the designed strength of the product and can be minimized only by reliability improvement programs. Usually, the hazard rate in the majority of cases can be approximated to be *constant* and the *mean time to failure* can be computed by its reciprocal. An application of a sudden stress in excess of design strength or maintenance induced failures may also exhibit a constant hazard rate pattern.

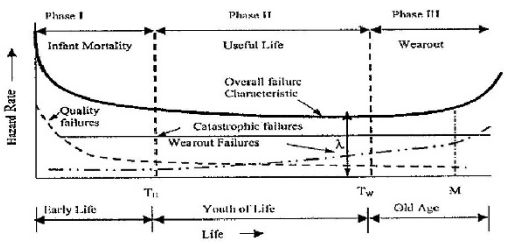


Figure 19.1. Typical bathtub curve

If a product has worked for a sufficiently long period (say 0-t_w in Figure 19.1), wear out sets in due to ageing and the old age effect shows up, causing the hazard rate to increase. Failures during this last phase of life are designated as *wear out failures*. As the time passes, death becomes more and more probable. In products involving mechanical parts, where moving parts are present, the wear out sets in as soon as they are put to use. In fact, the age at which wear out acts depends on the product and the environment under which it is functioning. Wear out failures can be minimized if the product is replaced at an appropriate time. In Figure 19.1, the *mean wear out life* or the *mean life* of product is shown to be (0-M). This, however, should not be confused with the *mean time to failure*, which is the reciprocal of the hazard rate during the useful life period, if the failure distribution is exponential. Moreover, M has to be greater than T_W. The position of M depends on the failure distribution during the wear out period.

19.2 Problems of Concern in Reliability Engineering

In specific terms, the problems that one is concerned about in reliability engineering are:

- How one can extend the useful life of a product?
- How can one minimize the chance failures of a product?
- How can one reduce the initial hazard rate and avoid product failures during its initial period?

The first two problems relate to the design and depend on material selection and the choice of derating and safety factors, with emphasis on prevention, reduction, or complete elimination of chance failures, which considerably improves the reliability in actual use. Here, one is also concerned about the overhauling or preventive replacement of the product during its design life. The third problem concerns the initial or infancy period, which may range from a few minutes to several hundred hours in certain cases. To eliminate the possibility of failures immediately after delivery, manufacturers generally conduct test-runs or debugging tests before delivery to ensure that quality failures have been eliminated and the customer is assured of better product reliability backed by a product warranty.

Since failures can occur any time during the lifetime of a product, reliability [103] can also be called a *birth-to-death* concern. Starting with preproduction activities like procurement of raw material and parts, preparing a conceptual design and detailed engineering design, the product passes through production, test and quality control,

shipment, warehouse storage and finally goes through use and maintenance phase before being discarded at the end of its life.

Quality and maintainability are the activities aimed at improving the reliability of the equipment during manufacture and operation and maintenance phase of product life. Truly, a reliability management program necessarily concerns itself with improving the reliability of a product, right from conception to disposal.

One of the measures of reliability of a product over its entire life period is designated as *operational reliability* (R_o), which can be expressed as a product of *inherent reliability*, (R_i) and the *use reliability* (R_u)*, i.e.,* $R_o = R_i.R_u$. Inherent reliability is what is built into a product during the design and manufacture phases. We cannot expect better reliability of a product than what we build into it during these phases. Within the resources available, a reliable design should use all possible means, such as structural redundancy, derating, safety, environmental factors, *etc.,* for improving product reliability. Having prepared the best possible engineering design, we can still lose on inherent reliability, if we ignore the necessity of stringent quality control during the manufacture. Quality in its simplest interpretation is reliability during the manufacturing phase and it ensures that only proper materials, processes and quality control techniques have been used.

Further, the conditions of use, maintenance and environment often affect the *use-reliability*. In fact, *maintainability* can be considered as reliability during operation and maintenance phases. Unless proper packaging, instructions for storage, shipment and use, operating manuals, maintenance procedures, spare parts, training of maintenance personnel, and conditions of environment are prescribed, it is meaningless to expect a high value of use reliability.

19.2.1 Reliability Is Built During the Design Phase

It has been estimated [144] that 80% of poor quality is caused by design. Over 90% of field failures are the result of poor design, and a high percentage of product recalls have their origin in design. Most law suits are filed on account of improper design and 70–75% of product costs are functions of design. Therefore, if there is any phase in the entire life cycle of a product that has maximum impact on reliability, it is the design phase.

Once a product has been conceived and functionally designed, a designer begins with product design from the performance consideration, which is not a straightforward process. It is an art based on the application of science. Analytical methods help only to select an alternative design or technology; thereafter the process is iterative and repetitive until the specified performance goals have been achieved. Design requires ingenuity and creativeness, and a designer ought to know what has been already tried before and did not work. Generally, a new prototype is not built because the designer knows that it will work better that way, but because he has no reasons why it will not work until it has been tried out.

In order to design reliability into a product, reasons for product failures must be clearly understood. Generally, a product fails prematurely because of inadequate design features, manufacturing and parts defects, abnormal stresses induced during packaging or distribution, human and maintenance errors, or external conditions (environmental or operating) that may exceed the designed values. Usually at the design stage, only rough reliability estimates on components reliabilities are available. The accuracy of these estimates depends upon how much data or information was available to the analyst, and on his ability to use this information or data to improve upon the product. The severity of the environment under which the system is to function must also be considered. As the design progresses, more details usually become available and at that stage it is possible to refine both the apportioned goals and the reliability estimates. In the end, the final estimates are based on the analysis of a detailed design, which incorporates failure rates of all components and parts, and the results of all developmental, qualification, and acceptance tests. The failure rates used in the estimates should be the measured failure rates of the components used in the system.

Inadequate attention to the design effort may result in faulty hardware, and retrofits rarely compensate for the original faulty design and may even be quite costly. They may create additional problems if the designer is not thorough in handling them. Therefore, there is no substitute for a good design, and it is one of the major responsibilities of top management to provide a highly competent design team to bring out a reliable product or system.

In fact, reliability should be designed and built into products and the system at the earliest possible stages of product/system development. It is the most economical approach to minimize the life-cycle costs of the product or system. One can achieve better product or system reliability at much lower costs than otherwise because the majority of life-cycle costs are locked in phases other than design and development; one pays later on in the product life for poor reliability effort at the design stage. As an example typical percentage costs in various life-cycle phases are given in Table 19.2.

Table 19.2. Life-cycle costs

Life-cycle phases	**Percentage costs**
Concept/feasibility	3
Design/ development	12
Manufacture	35
Operation/use	50

Therefore, a sincere effort at the design stage offers theadvantages that it:

- ensures that the product meets the performance goals;
- identifies potential failure mechanisms during product design;
- provides an estimation of the product warranty costs and allows life-cycle and warranty cost analyses;
- optimizes benefits accruing from design alternatives;
- finds the best reliability allocation to meet system reliability goals; and
- permits prediction of product reliability prior to finalization of changes.

For the reliability engineer, reliability during the product design and manufacturing phases should be of primary concern. Several options, such as parts and material selection, derating, stress–strength analysis, use of technology, simplification, and redundancy, are available to him to accomplish this. Very often, combinations of these options may be exercised in the actual design process because trade-offs are made between performance and costs. Each of these options shall be discussed in the following sections.

*Reducing complexity***:** The number of parts in a system is a measure of system complexity. For better performance the complexity should be reduced as far as is possible. Simpler designs are invariably more reliable. Very often the parts are serially related with respect to the system reliability; each part is required to have a very high reliability. Any alternative design that helps reduce the number of parts definitely leads to a significant improvement in reliability. Thus, consideration of simplicity should be exercised throughout all phases of the design process. The necessity of all parts should be questioned and design simplifications should be employed wherever possible. A function that can be achieved by assembling few parts with proven reliability is considered more reliable than a design that uses host of components to achieve more automated operation. Designing parts to serve more than one function or use may also reduce part counts.

In addition to parts minimization, a designer must explore the possibility of minimizing part variation. The use of common parts and components can better control material quality and manufacturing tolerances. Also, as component parameters are known to drift over time, the designer must ensure that different tolerances do not combine in such a way that is likely to degrade system functionality.

Derating: Derating consists of stressing a component significantly below its rated or designed value of stress and provides a very effective method of improving the reliability of a product. This is commonly used practice for electronic equipment and, in fact, is synonymous with the concept of the safety factor in mechanical or structural designs. Voltage and temperature are

common derating stresses for electrical components. However, derating may be applied in the case of current or power as well. One can have derating of temperature and effort should be made to keep the operating temperature as low as possible. This can be accomplished by using product heat transfer models such as reducing power, providing heat sinks and thermal conduction, and radiators, providing packaging with optimum airflow and specifying the operating environment. Stress derating can also be resorted to in the case of mechanical systems.

Redundancy: If the system reliability goal is higher than the system reliability achieved by the functional design of the system, it is necessary to improve system reliability through system structural redundancy. Also, when it is impossible to achieve the desired component reliability through inherent component design, redundancy may be the only alternative. Redundancy may also help achieve increased product reliability against external environmental stresses. Design trade-off analysis is generally carried out to obtain an optimal configuration due to the increased costs of additional components, the size or weight added to the system, and possibly the increase in repair and preventive maintenance necessary to maintain multiple components due to redundancy rather than just one. Redundant system configurations include both active and standby units or there may be the more general k-out-of-m or partial, fractional or even voting redundancy. Redundancy also provides the possibility of repairing the failed units while the other redundant unit or units are operating.

Safety margins and system compatibility: A designer should provide the highest operating margin possible for product design. He can conduct product preliminary tests at stresses beyond the margin extremes experienced during the operation. Test time constraints require accelerated tests but one should not overlook the fact that highly accelerated tests may sometimes present failure modes that may be present during the normal operation of a product under the specified conditions and thus may not reflect the product's true reliability. It should not be missed that the product user will use the product in an unspecified manner and usually not inform the designer or producer how it was being used when a failure occurred, causing unnecessary improvement expense.

Vendor and component selection: Vendor selection is critical for building reliability into a product and therefore appropriate importance should be given to the purchase of reliable components. Purchasing components from a vendor with a proven reliability history goes a long way to enhancing equipment reliability. Electrical and electronic components should have been environmentally stress screened to achieve a higher (and specified) reliability. High reliability (hi-rel) components usually have a higher price, but they help to significantly reduce the overall failure rate of the product. Sometimes, a designer may have to choose between selecting standard parts and manufacturing specialized parts that perhaps have greater tolerances and reliability.

In the design phase, one has the complete freedom to choose the suppliers according to the options available for the choice of components based on technology or type. One should intelligently trade off between cost and reliability by buying reliable components that will economize the task of designing equipment with high reliability. Generally, trade-off is struck on the basis of cost, but ease of repair, parts availability, energy requirements, weight, and size may also be taken into consideration. Databases can be very helpful in selecting parts with a better reliability value among the competing parts.

Communication with the user: It is helpful and advantageous to be in communication with the customer/consumer to improveg product reliability. This is also required to secure a negotiated value for product reliability instead of producing a design of perfect reliability; but it is costly since the customer/consumer may be satisfied with a lower value of product reliability at a much lower cost than a product of high reliability at a very high cost.

Use of alternate technology: Sometimes, alternative technologies are available and the design engineer must explore the possibility of using an alternate technology that may provide the advantage of better reliability, as he may have

considerable flexibility in meeting the design goals. Typical examples include electromechanical devices *versus* solid state devices and digital display versus analog display, *etc*.

Better design tools andstrategy: In the design of electrical and electronic equipment one can make use of a computer-based circuit layout that will help minimize electronic noise and maximize electronic voltage margins in the circuit physical design. At the design level, one has the choice of using materials that tolerate a higher level of temperature, humidity, and chemical corrosion resistance would definitely provide an improved design. These materials, which can be considered a mechanical factor, are implicit in PCB and component structures. For example, one can use a tantalum capacitor in design rather than an electrolytic capacitor to decrease failure rate and increase operating life.

Similarly, in the design of mechanical equipment, computer aided design (CAD) and computer aided manufacturing (CAM) are being used extensively these days, which facilitates producing innovative and creative systems. Tolerances can be made very tight using CNC machines, thereby helping to improve the quality of the product, and many more advanced manufacturing machines and tools are available to produce high precision products.

19.2.2 Failure Data

In reliability, we try to become wiser from past mistakes and the whole effort is to avoid such failures of which the causes have become known. Therefore, failure information or data is a must for any reliability improvement program. The success of a reliability effort depends on the availability of good failure data that is complete and accurate. This would enable a reliability specialist to estimate and predict reliability accurately, take corrective measures, improve designs, plan the production process, properly operate, or even plan maintenance strategies well in advance. Therefore, the failure data collection and storage is central to the success of any reliability management program.

The scarcity and inaccuracy of reliability data has been one of the basis difficulties in the implementation of reliability improvement programs. Although a number or reliability data banks have been established world over, the quality of reliability data cannot satisfactorily support more sophisticated models than what are being employed today. Three types of data are especially important for evaluating product reliability. These are field (operational) failure data, service life data with or without failure, and data from engineering tests. Field failures constitute a meaningful data source because they represent experience from the real world. However, the exact operational and environmental conditions before and at the time of failure may not be fully and exactly known. Nevertheless, it is helpful to have some data that is reasonably, if possible for each operational failure.

Data on service life is necessary in assessing the time characteristic of reliability. It is helpful to know how many units are in service, for what period of time and under what conditions of use. Moreover, how many units have failed at what time? Certainly, this would help obtain considerable insight into product performance. It is would further be uuseful if the above information were supplemented by results from engineering tests (accelerated life tests), since many of the parameters and test conditions can be controlled, or at least are known. As a result, this data is normally considered to be dependable for analysis purposes.

The problem of acquiring data is not an easy one. Although sufficient failure data has been generated and is available for electronic or electrical components and devices, not much published information is available on the failure of mechanical components and, in fact, this lack of information or extrapolation of the available failure information to actual conditions of use constitutes the greatest deficiency in the field of reliability today.

The fact that failure rate information is not published does not necessarily mean that it does not exist. The reality is that those who possess this information are often reluctant to publish or share it because it was not obtained under controlled conditions of experimentation and can easily be questioned. Where the data exists, the owner may

not like to share it, having spent quite a fortune in creating or developing it.

The situation is highly satisfactory in the electronic industry where a great deal of failure information is available today, yet the published material does not make it more accurate for the reliability estimates of electronic systems. This is primarily on account of the fact that each test laboratory obtains a different rate for the same component depending upon the test environment, test equipment and the procedure. Therefore, it is very common that different part manufacturers publish different failure rates for the same parts. Moreover these published failure rates generally pertain to catastrophic failures and do not include information on out-of-tolerance failures. Moreover, the published failure rates do not include the effect of degradation in reliability during manufacturing storage, or transshipment.

Once the failure data is available and environmental conditions are known, the data must be used to fit in an appropriate failure distribution and parameters of the distributions ascertained to represent the model [108, 109, 122, 123, 124, 133]. The situation for the increasing hazard rate is not that simple, since there can be more than one candidate for fitting in the distribution. There are techniques to do that (see, *e.g.,* [128, 136, 146, 147].

There are situations when we design unique equipment, assembly or redesign a product for a new environment for which no failure rates based on prior experience are available. In all such cases, it is often possible to establish a range for the unknown failure rate by comparison with existing similar systems. The analysis then can be carried out for the limiting the critical failure rates in the range. Often such an analysis can be useful in establishing a design configuration. Depending on the importance of the new component, such estimates may have to be substantiated by laboratory tests. Moreover, some knowledge of the correlation of laboratory failure rates with the actual service experience needs to be available.

19.3 Reliability Prediction Methodology

Reliability prediction is fundamental to system design and involves a quantitative assessment of system reliability prior to system development. In fact, reliability prediction [76] provides baseline values for reliability growth and demonstration testing, maintainability, supportability and logistics costs. Thus, prediction has several objectives:

- Feasibility evaluation
- Comparison of competing designs
- Identification of potential reliability problems.
- Provision of input to other reliability and maintainability tasks.

Feasibility evaluation involves evaluating the compatibility of the proposed design concept with the design requirements. Early in the system design, a feasibility evaluation would typically involve the parts count type of prediction (MIL-HDBK-217 F, Appendix A) to determine the compatibility of feasibility evaluation with required reliability. Feasibility evaluation may also include a detailed parts stress type analysis (MIL-HDBK-217 F, Sections 5–23) for components. Feasibility evaluation is usually critical for totally new system designs where no similar experience exists, as with systems with known reliability characteristics.

Comparing competing designs is similar to feasibility evaluation, but for the fact that it provides one output, the predicted reliability, to be used in making broader system level design trade-off decisions involving factors such as cost, weight, power, performance, *etc*. A parts stress type prediction is typically used to provide a quantitative assessment of relative cost-benefit of systems level trade-off considerations. Reliability predictions also provide a systematic means of checking all components and assemblies for potential reliability problems. It also offers a means of evaluating the reliability improvement in the case of potential problem areas by focusing attention on low quality, over-stressed or misapplied parts. It should be emphasized that the prediction itself does not improve the system reliability; it only provides a means for identifying

potential problems that, if resolved, will lead to improvement of the system reliability. Therefore, predictions provide an excellent ground for reviewing and evaluating the progress of system design ahead of testing.

Reliability predictions also provide key inputs to other R/M tasks such as maintainability analysis, testability evaluation, and failure modes and effects analysis (FMEA). Because prediction identifies weak reliability spots, it provides key inputs to weigh the benefits of adding test points, making locations for maintenance more readily accessible or introducing redundancy to minimize the influence of a particularly critical failure mode. Reliability prediction begins at the lowest level in the system hierarchy, *i.e.*, at the components level and proceeds thorough the intermediate level, which is a subsystem level, until system reliability is obtained. In general, there is a hierarchy of reliability prediction technique available, depending on the depth and knowledge of the design and the availability of collected reliability data on the equipment and any useful information on it.

The general procedure of prediction can be outlined as follows:

- Define the system and its operating conditions.
- Define system performance criteria (in terms of either *success* or *failure*).
- Develop a system model using *reliability block diagrams* (*RBD*) or *fault tree methodology*.
- Compile a parts list for the system.
- Assign failure rates and modify *generic failure rates* using an appropriate procedure.
- Select a *prediction procedure* and perform a *parts count* or *parts stress* method for the system.
- Combine part failure rates.
- Estimate system reliability.

The main effort in the reliability predictive sequence lies in carrying out the following tasks:

- A list of components is prepared for the product. The component reliability data for components is usually obtained from the applicable sources or relevant databanks.
- Reconciliation is often needed between the differing values of the failure data available from various sources. A tentative and eventually accepted value for each component is determined.
- Various operating stresses are usually projected for the preliminary design, and expected operating conditions are projected into the prediction of the failure rate of each component. Stress factors are generated as appropriate multiplying factors for the part failure rates for a specific application. One can improve the reliability of a system by carefully anticipating the intended environment of use. In fact, the system being designed may have to function in the presence of harsh environments like extreme temperatures, humidity, salt spray, moisture, dust, sand, gravel, vibration and shock, and electromagnetic induction (EMI), *etc*.
- Product reliability then can be computed to provide a product level estimation of the reliability. This procedure, when applied repeatedly to new evolving products becomes:
  - an accurate indicator of unreliable components in the new products,
  - an accurate indicator of the total system reliability determined by catastrophic failure of components, and, finally
  - a product reliability document.

In fact, a components' level synthesis of product reliability is recommended for all serious product designs. The process becomes more accurate with repeated use and evolves into the reliability design tool for the system.

19.3.1 Standards for Reliability Prediction

Depending on the nature and type of components, whether electrical, electronic or mechanical, several documents are available for reliability prediction procedure. The engineer can select the model that is best suited to the part types and requirements of the component or product whose

reliability is being predicted. It is important that predictions are made as precise as possible, since if the reliability predictions are made too low then one may arrive at an over design and the design can be costly. On the other hand, if the predicted values are too optimistic and high this may lead to catastrophic consequences. The standards for reliability prediction use a series of models for various categories of electronic, electrical and electro-mechanical components to predict failure rates that are affected by environmental conditions, quality levels, stress conditions, and various other factors. Some of these procedures can be found in the following documents:

MIL-HDBK-217: This standard has been the mainstay of reliability predictions for about 40 years. The most recent revision of MIL-HDBK-217 is *Revision F Notice 2*, which was released in February 1995 and has not been updated since then. This is the most widely used and accepted document for the prediction of electronic components and equipment reliability. Reliability prediction using this procedure in electronic design often results in a reduction in design lag time and savings in lifetime costs. MIL-HDBK-217 can be used for both commercial and military grade components. The handbook includes a series of empirical failure rate models developed using historical piece part failure data for a wide range of components. They predict reliability in terms of failures per million operating hours and assume an exponential distribution, which is justified in the case of electronic and electrical components. MIL-HDBK-217 allows a *parts count* analysis and a *parts stress* analysis to be performed. One can use *parts count* for quick estimates and early design analyses or a *part stress* method covering 14 separate operational environments, such as ground fixed, airborne inhabited, *etc*., for taking actual temperature and stress information into account. It therefore offers relatively an accurate estimate of the failure rate. Typical factors used in determining a part's failure rate include the temperature factor (π_T), the power factor (π_P), the power stress factor π_S, the quality factor (π_Q), and the environmental factor (π_E) in addition to the base failure rate (λ_b).

To improve on some of the handicaps of this standard, one can extend the *parts count* and *parts stress* methods by incorporating the mathematical models from the *Telcordia* procedure, which can also be used for the prediction of reliability of electronic components and equipment and allows the consideration of burn-in as well as laboratory and field data.

There are other standards that are useful in reliability prediction process. They are MIL-STD-1629A, BS 5760 Part 5 for carrying out a *failure mode, effects and criticality analysis (FMECA)*. The *FMECA* module provides interactive graphical aid in constructing block diagrams indicating the logical connection between the system and its subassemblies, and components on the other side. This graphical representation can be extended to relate failure modes at various system levels. For maintained systems, standards such as MIL-STD-472 can be helpful in estimating *mean time to repairs (MTTR*) for subsystems and components.

Telcordia SR-332: The Telcordia method was originally developed by AT&T Bell Labs and modified by Bell Communications Research (*Bellcor*e) to improve upon the representation of mathematical equations of MIL-HDBK-217 in accordance with what their equipment was experiencing in the field. However, the main concepts in MIL-HDBK-217 and Telcordia are very similar, but Telcordia has an added the ability to take into account burn-in, field, and laboratory testing, which makes it quite popular with commercial establishments. The current version of Telcordia is *Issue 1*, which was released in May 2001 and follows *Bellcore Issue 6* in order of release. The Telcordia method also assumes an exponential failure distribution and calculates reliability in terms of failures per billion part operating hours, or FITs.

Telcordia also has the ability to perform a *parts count* or *part stress* analysis and also provides models for predicting the failure rates of units and devices during the first year of operation. In fact, the failure rate during this period is expressed as a multiplying factor (*first year multiplier or FYM)* operating on the predicted steady-state failure rate. The prediction module automatically calculates the

first year multiplier based on the specified system, unit and device burn-in times and temperatures.

The Telcordia standard allows reliability predictions to be performed using three methods. The method I parts count approach applies when there is no field failure data available. Method II provides a modification to Method I to include laboratory test data, and the Method III variation includes field failure tracking. Method I includes a first year multiplier to account for infant mortality. Method II includes a Bayes weighting procedure that covers three approaches depending on the level of previous burn-in that the part or unit has undergone. Method III also includes a Bayes weighting procedure but is based on three different cases depending on how similar the equipment is to the one from which the data was collected. For the most widely used Method I, where the burn-in varies, the steady-state failure rate depends on the basic part steady-state failure rate and the quality, electrical stress and temperature factors as follows:

$$\lambda_{SSi} = \lambda_{Gi}\ \pi_{Qi}\ \pi_{Si}\ \pi_{Ti}\,. \qquad (19.3)$$

Telcordia offers ten different *calculation methods*. Each of these methods is designed to take into account different information relating to stress data, burn-in data, field data, or laboratory test data.

Comparison between MIL-HDBK-217 and Telcordia: Since MIL-HDBK-217 was the original standard for reliability prediction analyses, it is known and accepted worldwide, whereas Telcordia is primarily accepted in the United States Although its popularity is gradually growing internationally, it has not been completely accepted by the international community as yet. Moreover, when AT&T Bell Labs developed Bellcore (now Telcordia), they concentrated primarily on commercial equipment. Telcordia was specifically designed to focus on telecommunications, whereas MIL-HDBK-217 was much more broadly based in scope, is useful to both military and commercial equipment, and had no specific focus.

Although the basis of the Telcordia and MIL-HDBK-217 calculations are very similar, it is often observed that calculations in Telcordia are more optimistic than calculations in MIL-HDBK-217. Moreover, Telcordia calculations require fewer parameters for components. This, however, does not mean that Telcordia failure rates are always better. It simply indicates that, depending on the component types, the difference in failure rates can be predicted.

As stated earlier, the Telcordia model has the additional capability of considering burn-in data, laboratory test data, and field data. This feature is extremely helpful in calculating failure rates that are based on historical data, rather than simply calculating stress data. In addition, burn-in data is used to quantify the *first year multiplier*, which is indicative of infant mortality.

One of the differences is that MIL-HDBK-217 calculates failure rates in *failures per million hours,* whereas the Telcordia model calculates failure rates in *failures in time* (or *FITs*), which is expressed as *failures per billion hours*. MIL-HDBK-217 provides models for printed circuit boards, lasers, SAWS, magnetic bubble memories, and tubes, whereas the Telcordia does not support these parts. Telcordia provides models for gyroscopes, batteries, heaters, coolers, and computer systems. However, these part types are not supported by MIL-HDBK-217. Nevertheless, one can always use MIL-HDBK-217 for the majority of parts in the analysis and use Telcordia for those part types that are not supported by MIL-HDBK-217 (or *vice versa*).

Since Telcordia was initially designed for use in the telecommunications industry, the operating environments that Telcordia supports are very limited. For example, Telcordia only supported three different variations of *ground*-based environments, initially. However, Telcordia is evolving rapidly and in the most recent issue of Telcordia, the additional operating environments of *Airborne, Commercial* and *Space,* and *Commercial* have been made available. MIL-HDBK-217, on the other hand, has always offered a number of different operating environments. Currently, MIL-HDBK-217 supports a variety of ground, sea, air, and space environments.

In MIL-HDBK-217, the quality levels used differ from one part type to another and they are derived from specific data that is component dependent. Therefore, the quality levels for resistors are different than the quality levels for

semiconductors and the quality levels for semiconductors are different from the quality levels for integrated circuits. However, the assignment of quality levels in Telcordia is very simple and it currently supports four standard quality levels. These quality levels are identical for all component types, and are simply based on the origin and screening of components.

PRISM: This procedure was developed at the Reliability Analysis Center (RAC) and was released in 2000. It provides the ability to update predictions based on test data and addresses factors such as development process robustness. PRISM interfaces directly with RAC's automated data-bases and provides methodology to assess the quality of the system development process. It has been incorporated into the Relex Reliability Prediction module for carrying out system reliability analysis and MTBF prediction. It has the ability to model the effects of thermal cycling and dormancy. It allows one to select parts from both the electronic parts reliability data (EPRD) and non-electronic parts reliability data (NPRD-95) documents published by RAC and permits the use of predecessor data and process grading factors in the reliability analyses.

The Bayesian approach has facilitated the use of test and field data at the assembly level to enhance predicted component failure rates with real-life experiences. PRISM includes means to deal with software reliability but is limited by the fact that it does not yet include models for all commonly used devices. The system reliability model presented by PRISM is:

$$\lambda_S = \lambda_{IA}\left(\pi_P\pi_{IM}\pi_E + \pi_D\pi_G + \pi_M\pi_{IM} + \pi_E\pi_G + \pi_S\pi_G + \pi_I\pi_E + \pi_N + \pi_W\pi_E\right) + \lambda_{SW} \tag{19.4}$$

where λ_{IA} is the initial assessment failure rate (based on *RACRates* component failure rate models) for the system and the other factors involved address parts processes (π_P), infant mortality (π_{IM}), environment (π_E), design processes (π_D), reliability growth (π_G), manufacturing processes (π_M), item management processes (π_S), induced processes (π_I), no-defect processes (π_N), and wear out processes (π_W). Also, λ_{SW} is the software failure rate. Quantitative values for the individual factors are determined through an interactive process intended to benchmark the extent that measures known to enhance reliability are used in design, manufacturing and management processes.

NPRD-95: This document provides failure rates for a wide variety of items, which include mechanical and electromechanical parts and assemblies. This document provides detailed failure rate data on over 25,000 parts for numerous part categories grouped by environment and quality level. Because the data does not include time-to-failure, the document is forced to report average failure rates to account for both defects and wear out. Cumulatively, the database represents approximately 2.5 trillion-part hours and 387,000 failures accumulated from the early 1970s through to 1994. The environments addressed include the same ones covered by MIL-HDBK-217; however, data is often very limited for some environments and specific part types.

NSWC-98/LE1: This document is also known as the *Handbook of Reliability Prediction Procedures for Mechanical Equipment* (NSWC-98/LE1) and was primarily developed by the United States Navy. This document uses a series of modules for several categories of mechanical components to predict the failure rates that are affected by stresses, flow rates, temperature, and several other factors. In fact, it provides models for various types of mechanical devices including springs, bearings, seals and gaskets, electric motors including motor windings, brushes, armature shafts, *etc*. It also deals with brakes and clutches, compressors, threaded fasteners, mechanical couplings, and slider-crank mechanisms. This is a relatively new standard and also contains reliability models for solenoids, gears and splines, valves, actuators, pumps, filters, *etc*.

CNET 93: This is a document developed by *France Telecom* and provides reliability models for a wide range of components. CNET 93 is a comprehensive model similar to MIL-HDBK-217, which provides a detailed stress analysis.

RDF 2000: This is a newer version of the CNET UTEC80810 procedure developed by UTE and has not received much attention in the US but has the potential of eventually becoming an international standard. It uses cycling profiles and their applicable phases to provide a completely different basis for failure rate calculations. The models take into account power on/off cycling as well as temperature cycling and are very complex with predictions for integrated circuits requiring information on ambient and print circuit ambient temperatures, type of technology, number of transistors, year of manufacturing, junction temperature, working time ratio, storage time ratio, thermal expansion, number of thermal cycles, thermal amplitude of variation, application of the device, as well as transistor technology related and package related base failure rates.

HRD5: This is a reliability prediction procedure developed by *British Telecommunications plc,* which provides models for a wide range of components. In general, HRD5 is similar to CNET 93, but provides simpler models and requires fewer data parameters for reliability analysis.

Document 299B: This document is based on the Chinese standard *GJB/z 299B*. It has been translated into English by Beijing Yuntong Forever Sci.-Tech. Co. Ltd. Document 299B is very similar to the MIL-HDBK-217 reliability procedure and permits one to take temperature and stress information into consideration.

The Physics-of-Failure Procedure: This has a family of approaches that differ significantly from other empirical methodologies and attempts to identify the *weakest link* of a design to ensure that equipment reliability exceeds the design value, and the methodology ignores the problem of defects escaping the manufacturing process and assumes that the product reliability is constrained by the predicted life of the weakest link. The model addresses problems such as microcircuit die attach fatigue, bond wire flexure fatigue and the die fatigue cracking. The models require detailed device geometry and material properties They are, however, used primarily at the subdevice level during the early design stage in electronic system reliability predictions.

*The IEEE Gold Book: **Viz.**, IEEE STD 493-1997* is available for the design of reliable industrial and commercial power systems and provides data on equipment used in industrial and commercial power distribution systems besides dealing with reliability analysis, probability methods, power system reliability evaluation, economic dispatch, and the cost of power outage data. This document was updated in 1997 although the most recent data is from 1989.

19.3.2 Prediction Procedures

The task of predicting the reliability of a product is straightforward if the reliability data of the product is available either from the field, from testing laboratories or from databanks. However, usually if a product that is being designed is new and there is not be enough information available from either of the above-mentioned sources, then the reliability engineer has to use some alternative procedure. There are a variety of reliability prediction procedures that can be used in such a situation.

The Similar Product Technique: This approach is used to estimate the reliability of a new product based upon the known reliability of an existing product with similar attributes. These attributes can be the type of technology used, digital circuitry, the complexity of the product and the operating environmental conditions, and the quality of the product.

The Similar Complexity Technique: In this approach, the reliability of the product under design is estimated by comparing its relative complexity with a known product of similar complexity.

The Prediction by Function Technique: This approach uses the correlations between function and reliability in order to predict the reliability of a new design. However, there are two basic empirical techniques that are often found useful in the task of product reliability estimation, *viz.*:

- The parts count prediction method.
- The parts stress prediction method.

Failure data for both these methods are available in latest release of MIL-HDBK-217F if the product

belongs to the electrical or electronic category. These methods are also used with modification in the case of mechanical equipment, particularly under certain conditions of use.

19.3.2.1 The Parts Count Method

This method is used for obtaining preliminary design and development and consists of preparing a list of the each generic part type such as capacitors, resistors, and so on in an electronic circuit, and their numbers used in the design of electrical or electronic equipment. It assumes that these components are reasonably fixed and over all design complexity is not expected to change substantially during later stages of design, development and prediction process. The parts count method is generally used in the early design phase as sufficient information is not available then, and a full stress method cannot be used. MIL-HDBK-217 provides a set of default tables, which provide a generic failure rate (λ_g) for each component type based upon the intended operational environment. This component generic failure rate is modified by a quality factor (π_Q), which represents the quality of the components in question, *i.e.*, the components are manufactured and tested to a full military standard or to a lesser commercial standard. In addition to this, a learning factor (π_L) is also used for microelectronic circuits and represents the number of years that the component has been in production. Thus, using the component generic failure rate for a given environment and modifying it for quality and learning factors in the case of microelectronics, a component's final failure rate is established. The summation of the individual component's failure rates will yield the overall failure for the circuit. With this and the summation of the other Circuit Card Assembly, the failure rate of a line replaceable unit can be established.

Finally, following this process an overall failure rate for the system can be established. This approach assumes a constant failure rate of each component, assembly, equipment, and the system. The system/subsystem failure rate can be obtained by summation of part failure rates assuming that all components are in series. In the case where the model consists of non-series components or redundant units, the item reliability can still be determined either by considering only series elements of the model as approximation or by summing part failure rates for the individual elements and calculating an equipment series failure rate for non-series elements of the model.

19.3.2.2 The Parts Stress Method

This is an accurate method of system reliability prediction other than measuring reliability under actual or simulated conditions. This method is usually used when the design is almost completed and a detailed parts list and parts stresses are known. The approach requires a detailed knowledge of all the stresses such as temperature, humidity, vibration, *etc*., and their effect on the parts failure rate, to which each part shall be subjected to under actual conditions of use. The part stress analysis also assumes that all times to failure of parts are exponentially distributed. The data necessary for the parts stress analysis include: specific part types (including device complexity of microelectronics), quantity of parts, part quality levels, environment of use, and part operating stresses.

To enable a full stress analysis to be conducted there must be sufficient details of the systems' design available to the reliability engineer. In short, the design of the system must be such that the electronic and electrical design of the hardware is known down to the components level. There will be detailed parts lists and circuit schematics as this is required to take into consideration the electrical and thermal stresses that may be experienced by various components. With the detailed knowledge of the electrical and electronic design and the specific data pertaining to each component type used within the design the stress analysis can be done. Component information, or data sheets, is usually available from the manufacturer and these days this information can also be obtained over the Web. In the case of a parts stress analysis, the mathematical models are available in MIL-HDBK-217 for each component type, *i.e.,*

microelectronics, resistors, capacitors, and electro/mechanical devices.

The most general approach used by MIL-HDBK-217 is that each generic component type is assigned a base failure rate (λ_b) and is modified by influence factors. These factors, such as $\pi_{E,}$ which is the environmental factor, are based upon the intended operation environment of the equipment or system. The other factor considered is π_Q, which is the quality factor and is a general look up factor that represents the quality of the component in question. There are other factors as well that are used for multiplying the generic failure rate. These factors should all be known or can be determined based upon the state-of-hardware, for which the parts stress method is being applied and assumptions regarding the various factors associated with the failure rates can be justified. Some of the factors will result in a linear degradation of the base failure rate, while others may result in an exponential degradation, in particular, those factors associated with temperature. There are many environmental factors for which the generic failure rate can be modified; however, some of the environments factors used in MIL-HDBK-217 are: Ground Benign (GB), Naval Shelter (NS), Airborne, Uninhabited Cargo (AUC), and Space Flight (SF), the details of which can be found in the MIL Standard.

Therefore, the part failure models may vary with different part types. However, their general form is:

$$\lambda_i = \lambda_B \pi_E \pi_A \pi_Q \cdots \pi_N , \qquad (19.5)$$

where

λ_B = base part failure rate; the value is obtained from the part stress data for each generic part type. The data is generally presented in the form of failure rate against normalized stress and temperature factors. The value of λ_B usually determined by the stress level (current, voltage, *etc.*) at the expected operating temperature.

π_E = environmental factor; this factor accounts for the influence of environment other than temperature and is related to other operating conditions such as vibration, humidity, *etc*.

π_Q= quality factor; this factor accounts for the degree of manufacturing control with which the part was fabricated and tested before shipment to the user.

π_N = additional adjustment factor; this can account for cyclic effects, the construction class and other factors that modify data.

Modification for Mechanical Components: Unfortunately, mechanical parts typically do not follow the exponential failure distribution or constant failure rate. Instead they exhibit wear-out characteristics or have an increasing failure rate with time. The procedure developed by RAC makes it possible to still use the standards for the prediction of reliability for mechanical components. While the actual time-to-failure distribution may be Weibull or lognormal, it may appear to be exponentially distributed over a long period of time. However, this is so only when the components are replaced upon failure. This condition is usually true for the vast majority of mechanical components [75].

19.3.3 Reliability Prediction for Mechanical and Structural Members

Mechanical components wear out due to friction, overload, plastic deformation, fatigue, changes in composition due to excessive heat, corrosion, abuse, *etc*. The traditional method of guarding against stress related failures has been to specify a safety factor greater than 1, where the safety factor is defined as: SF = S/s, SF being the nominal safety factor, S is the nominal strength or allowable stress and s is the maximum principal stress. This definition assumed that the values of stress and strength are known exactly and the difference between them provides the safety margin for overloading and reduction of strength over time due to corrosion, cracking, *etc*. If a high value of the safety factor is chosen, the design tends to become heavy, bulky and costly. Thus a designer needs to make a trade-off and use his experience and judgement in arriving at an adequate value of the safety factor.

There is always uncertainty present in the measurements of strength as well as in stress calculations. Therefore, stress and strength must be

treated as random variables and following the principles of probabilistic design (as against the deterministic approach using safety factors) as introduced in (19.1) and (19.2), one can predict the reliability of a mechanical or structural member.

Probabilistic mechanical or structural component reliability [11, 74, 89, 141, 152] is gaining importance of recent due to the fact that today we have high performance materials due to advances in material technology, but these materials often possess detrimental side effects and the other reason is that the need for higher performance is constantly pushing operating stresses to higher levels. The probabilistic design model consists of four major activities; *viz.*, design process, material production, manufacturing and operations. Output from the design process is the expected operating stress distribution resulting from load spectra. The remaining three activities provide the material strength distributions, determined through Monte Carlo simulation of random variables representing random variation of incoming material strength, manufacturing defects and operational factors. The probability of failure can be computed from (19.2) as the probability of stress exceeding the strength. The integral can be computed numerically using the trapezoidal rule or more refined methods such as the Simpson rule, or methods based on polynomials such as Laguerre–Gauss or Gauss–Hermite quadrature formulae.

Analytical methods such as FORM and SORM are also available to calculate the probability of failure. There are first order second moment (FOSM) and advanced first order second moment (AFOSM) methods. These methods derive their names from the fact that they use the first order Taylor series approximation of the performance function linearized at the mean value of the random variable. In FOSM, the information on the distribution of random variables is ignored whereas in AFOSM, the information on the distribution of random variables is taken into account. FOSM is also known as the mean value first order second moment method (MVFOSM). There are other methods such Hasofer–Lind (H–L) method [9], which is basically an AFOSM approach when the random variables are normally distributed. H–L methods are available for linear and non-linear performance equations or limit state equations. One can determine the reliability index, which in both cases is basically the distance between the origin and the design point on the performance equation.

The second order reliability method (SORM) takes into account the curvature of the limit state equation by considering second order derivative terms in the Taylor series expansion, which were actually neglected in FORM approach. Thus SORM is supposed to be a more accurate approach. SORM was first suggested by Fiessler *et al.* [25], who used quadratic approximation. A simple closed form solution for the probability computation using second order approximation was given by Breitung [50], who used the theory of asymptotic approximations.

The reliability computation when limit states are implicit can be done using the analytical methods described earlier but by using a simple simulation technique it is possible to calculate the probability of failure for explicit or implicit limit state functions. In fact, to evaluate the accuracy of these sophisticated techniques, or to verify a new technique, a simulation technique is routinely used to independently evaluate the probability of failure.

A good description of all these approaches can be found in [55, 58] and also in Chapter 63 in this handbook.

19.4 System Reliability Evaluation

Since system reliability design, as we all know, is basically an iterative process and system reliability computation is repeatedly required at each cycle of iteration of the design procedure; reliability evaluation is a must for any system reliability design. This necessitates the development of efficient and fast procedures for system reliability evaluation in order to economize on the time required for the system design. In fact, a considerable amount of research has been done to develop fast methods of system reliability computation.

System reliability computation basically involves a three-step procedure. In the first step, one develops a logical model for the system, and in

the second step, the system logical relationship is transformed into an algebraic relationship of the system reliability expression in terms of component reliabilities. In the third step, one can substitute for component reliabilities in the algebraic expression available for system reliability. Sometimes, computerized algorithms combine steps 2 and 3 and produce a system reliability value without transforming the logical relationship into an algebraic reliability expression. Reference [6] does exactly that for a series-parallel configuration and is the fastest method for computing system reliability. For non-identical parallel components, an algorithm [16] computes reliability very quickly. If analytical procedures are not used, Monte Carlo methods [103, 150, 155] can be used to estimate the system reliability.

19.4.1 Reliability Modelling

Reliability modelling is the first important step in the system reliability evaluation. In order to model a system, it is always possible to decompose it into its constituent parts. For a complex system, the number of such parts may be quite large and a multi-level approach is always helpful to achieve this decomposition. A component by definition is the system constituent at the lowest level. Therefore, it may be necessary to model this multi-component system at various levels. The system can be maintained (where repairs of failed units are possible) or may just be a non-maintained system. Modelling for these two types is done differently. In reliability modelling, we try to achieve a relationship between individual components, or subsystems failures with the system failures for the known system objective. One can model system failure in two ways, *viz.*, using either the black-box approach or the white box-approach. In black-box approach the state of the system is described either in terms of two states (working/failed) or more than two states (a multi-state model) without linking them to the components of the system. In the white-box approach the state of the system is specified in terms of the states of the various components. In the white-box approach we have a *forward* or *bottom- up* approach, in which one starts with the failure events at the part level and then proceeds to the system level to assess the consequences of such failures. Failure mode and effects analysis (FMEA) belongs to this type of modelling. In the backward (top-down) approach, one starts at system level and proceeds downwards to the component level to link the system performance to the failures at part level. Fault tree analysis belongs to this category.

Linking the system performance to the performance of its constituents can be done qualitatively and quantitatively. In the first case, one builds up the logical relationship, whereas in the latter, one obtains a measure of system performance (which may be the system reliability) to the performance (reliabilities) of components. The logical relationship can be expressed graphically either by what is known as the reliability logic diagram (RLD) in the success frame of reference or in the failure frame of reference through a fault tree diagram, where the failure of the system is related to the failures of system constituents at various levels. Both approaches have their own advantages in system analyses.

Fault tree analysis is a well-documented methodology and is being used extensively for assessing the safety and reliability of high risk systems such as the nuclear, chemical, and aerospace industries. A detailed discussion of this technique can be found in Chapter 38 of this handbook and in Chapter 8 of [103]. Other graphical relationships are possible by which the same task can be achieved, *viz.,* events trees, binary decision diagrams (BDD) (Chapter 25 of this handbook], causal trees or diagraphs (Chapter 8 of 103]) *etc*. Petri nets [22, 38, 39, 66, 117] and even neural nets [99] have been found to be useful in system reliability assessment or fault diagnosis programs. This handbook provides a discussion of some of these topics.

The underlying assumption in reliability modelling is that each component or system can have only two states, which means that it is either good, or in working state, or bad, which means not working. Thus the model is a two-state model.

In fact, three-state models [103] have been widely discussed in the past and the optimal design of these systems has also been discussed widely.

Three-state systems are those systems where two modes of failure, such as short circuit and open circuit failures in electrical passive devices and a valve getting stuck open or stuck closed in mechanical systems, are considered in computing the system reliability.

Recently, considerable attention has been paid to the analysis of multi-state systems [139, 142], where the usual assumption of binary states for components and the system is shed to include multi-state components, which may be useful in considering degraded states in addition to working and failed states. The analysis and design of such systems using conventional methods becomes quite cumbersome particularly when repairs are being considered. Also, reliability modelling of nano-scale devices [154] is also becoming important as nanotechnology is being more widly acceptable. Therefore, new approaches are becoming naturally important; this handbook includes Chapters 28, 29, 30 and 58 on recent research in this direction.

Alternatively, a component can be modelled as a two-terminal passive device, which allows a signal to pass through it from its input terminal to its output terminal if it is good and blocks it if it is bad. In other words, a component can be considered as a directed branch with its reliability as its gain. This modelling criterion helped to model a system as a graph like structure known as the *probabilistic graph* and, in fact, facilitated the use of graph theory for system reliability evaluation. The first two papers using this approach [5, 6] were published in 1970 and were trendsetters for the use of graph theory in system reliability evaluation. Reference [5] was subsequently helpful in developing the topological method [23] of system reliability evaluation.

The application of graph theory [5] also led to the definition of the path set and the cut set. A *path set* is a set of those components whose success leads to system success, and this definition works well with the block diagram approach of system representation. Likewise, a cut set is a set of those components in a system whose failure yield system failure, and this definition works well with the fault tree approach. One also defines *minimal path sets* and *minimal cut sets* as sets having the minimum number of components of the system. There can be very many path sets and cut sets in a system. These definitions and developments led to several competing system reliability evaluation techniques [103, 149].

It is needless to emphasize here that this modelling consideration is found to be particularly useful in the performance evaluation of communication systems [63, 72, 151, 153], transportation systems or water supply systems with or without the capacity of links being specified [33, 41, 103]. One can define the system success and thereby its reliability if the communication system is able to communicate between the two specified terminals of the system. Therefore, this is aptly known as two-terminal reliability (or terminal-pair reliability) of the communication system. This leads us to define *k-terminal* [47, 56, 72] or *n-terminal (or all-terminal)* or *global* reliability of these systems, if it is possible to communicate between specified k-terminals or all the n terminals of the system so that all terminals of the system are able to communicate with each other or remain connected with each other. Imperfect nodes were also considered in several papers including [27].

19.4.2 Structures of Modelling

Based on the modelling procedure, several system structures are obtained, such as series, parallel, series-parallel, parallel-series, standby, non-series-parallel, k-out-of-n. Again k-out-of-n , which has been widely researched [18, 19, 28, 32, 45, 52, 62, 83, 84, 85, 92, 104, 105, 115, 116, 129, 130, 134, 145] has a family of its own such as the consecutive-k-out-of-n model and many other models such as the circular consecutive-k-out-of-n model, the circular m-consecutive-k-out-of-n model, the circular r-within-consecutive-k-out-of-n model based on related definitions and possibilities. A good discussion of the above can be found in [103]. Among all the series-parallel (or reducible networks or not non-series parallel) structures, the most widely used and general model is k-out-of-n:G, which consists of n components in parallel out of which at least k components should be good. Likewise one can define k-out-of-n:B or k-out-of-n:F, where at least k units must fail for the

system to fail. In fact, other models like series, parallel, *etc*., can be derived as special cases of this k-out-of-n model. Therefore, it was considered important to include a discussion of this structure and to provide an indication of the new trends in research in this area. The load-sharing model (see Chapter 20 of this handbook) is another realistic model of a parallel or k-out-of-n system, where the failure of any unit increases the hazard rate of the remaining units in parallel.

There are models [17, 103] that help to compute system reliability with the assumption of dependency of failures to approach realistic situations where the analyst cannot ignore the dependency of failures.

The non-series-parallel system or the non-reducible system is a more general category of models but it is difficult to handle. However, methods are available to compute the reliability of such systems.

Markov chains provide a modelling procedure for the availability or reliability modelling of maintained systems under various assumptions of practical importance. Markov models that are discrete in states but continuous in time have been found to be very useful in analysing systems with repairs under varying repair strategies and support facility considerations. However, the main drawback of these models is the size of Markov models, which grows very rapidly with the number of components in the system and therefore restricts its applicability to large systems. A good discussion of Markov modelling of maintained systems can be found in Chapter 7 of [103], where approaches such as state space, network, and conditional probability approaches for maintained systems have been provided. The three-state Markov model is presented in [12, 103].

Several other reliability models have been developed based on conditions of use and physical design constraints but the basic consideration in developing a model is to provide the means to compute its performance as realistically as possible under the assumptions made.

19.4.3 Obtaining the Reliability Expression

System reliability evaluation methods can be classified into two broad categories, *viz.*, those that employ path sets and cut sets for deriving the system reliability expression and those that use recursive method [7, 8, 59] network reduction [6, 96, 113], decomposition [21, 82, 96, 112] or transformation techniques [29, 34, 36]. A good discussion of these techniques is available in [103]. A comparative assessment of earlier methods and error computation was provided in [13, 14].

Early research on evaluation methods was also oriented towards determining path sets and cut sets of a system economically, because the number of path sets and cut sets can be very large even for a system of moderate size. For example, a 33-element system may give as many as 1681 path sets and unionizing them to obtain the algebraic system reliability expression can be time consuming and sometimes unwieldy on all accounts. In general, if there are m path sets of a system, the union of these path sets should normally yield an expression containing 2^m-1 terms, of which many of course will combine, but one can roughly figure out the number of resulting terms by calculating 2^m-1, which for m = 100 provides approximately a value of 1.27×10^{30}. One can imagine what it will be for m = 1681. One should not forget that it was a system with 33 elements only that yielded the number of path sets as 1681. What will be the number of path sets if the system is large, say with 1000 elements?

To overcome this problem, initial research was focused on obtaining directly the non-cancelling terms of the system reliability expression in uncomplemented terms. This led to the development of topological methods [5, 20, 23] of generating directly the terms of the reliability expression. However, it can be easily visualized that the number of non-cancelling terms would not be small. For example, for a 7-element system [5] with 7 path sets, 29 non-cancelling terms are obtained, whereas 2^7-1 is 127.

This difficulty or handicap led to further research in the development of reduction and transformation techniques for obtaining the system reliability expression. For series-parallel systems

decomposition is straightforward and one may use a computerized system decomposition technique such as that suggested in [6], which incidentally computes the system reliability value without obtaining explicitly an expression for the system reliability and is the fastest method of computing system reliability even today. Also, originally it was suggested for redundant systems with active redundancy but it can consider any type of redundancy (*viz,* standby, active, partial, or voting). However, for non-series parallel systems or non-decomposing systems (which cannot be decomposed into series or parallel structure) Bayes theorem or the factoring theorem [5, 6, 65] has been effectively used to obtain the system reliability expression by factoring out one element at a time from the system, which generates two sets of systems (one, with the element being factored out by open circuiting it and the other with this element short-circuited). The resulting configurations can be further used for decomposition by repeatedly applying the factoring theorem until a series parallel configuration is obtained. Simultaneous factoring of several elements is also possible [6]. Each time an element is factored, two configurations are generated. However, here again the computation time increases exponentially with the number of elements being factored out. Work on directed networks [49, 71, 94] has received considerable attention since the factoring theorem with directed components cannot be applied as with undirected elements.

Another direction of research has focussed on transformation techniques [29, 34, 36], which are basically approximate methods but that have been improved upon to provide reasonably accurate results from an engineering point of view.

Yet another direction that is receiving considerable attention and in which a significant amount of work is being done is the use of parallel processing algorithms [114] to reduce computation time and to develop the capability of handling very large systems.

In order to further improve the reliability evaluation procedure and to obtain a compact form of the system reliability expression involving complemented (unreliability) as well as uncomplemented variables (reliabilities), there were suggestions to generate disjointed path sets so that the reliability expression can be obtained just by summing up the probabilities of the disjointed path sets. This approach yielded far less number of terms in the system reliability expression than were obtained using the methods available at that time, usually in terms of uncomplemented variables representing component reliabilities. In fact, the system reliability expression was often very lengthy even for a moderate size system and required many multiplications, which affected the accuracy of the computation of system reliability.

The first attempt to achieve a minimized system reliability expression using the concept of producing disjointed path sets from simple path sets in a general computerized algorithmic procedure was made in 1975 in [15] and is known as the AMG-algorithm. This was basically a single variable inversion technique. Later, several improvements to the procedure were suggested starting with the Abraham [26] algorithm, and a large number of papers started appearing in the literature [31, 40, 51, 53, 60, 61, 67, 69, 70, 81, 90, 102], each claiming to provide an ever-decreasing number of terms in the system reliability expression.

This concept was further extended to include multi-variable inversion [95, 111, 137] and a highly compact form of the system reliability expression. These procedures offered the advantage of a compact expression, which not only saves computation time but can provide a more accurate numerical value of the system reliability as it involves fewer multiplications and handles less terms.

19.4.4 Special Gadgets and Expert Systems

Another important development in reliability evaluation techniques has been in the area of the development of special electronic gadgets or dedicated desktop systems in determining the path sets or cut sets of a system. We can represent a system by a network of two-terminal components and a signal (generated by a signal generating device) is passed through the system. When the signal is able to pass through the system (where each element is in a particular *on* or *off* state) it

simulates the system up-state and is analogous to creating a path set if we are able to record the state of each component. The digital part of this gadget would take care of the algebraic computation of reliability. This gadget is also useful in demonstrating to reliability beginners the idea of path sets and cut sets. The basic idea of the gadget (called "reliability analyzer") was introduced in [24, 121] and was further developed in [35, 37, 43] using a microprocessor platform. Later, this idea was commercially exploited by Laviron [42] to develop a desk-top aid in the form of ESCAF. Of course these developments came about at a time (around the early 1970s) when digital computer capabilities had not expanded to the limits they now have. Today, we have very fast computers to do any job that in the real time domain.

Another related development was in the direction of developing expert systems [57, 73, 77, 78, 100, 120]. In fact, there are expert systems available to carry out failure mode and effects analysis (FMEA). Several expert systems have been developed for specific reliability programs in organizations and companies. For example, REMM [140] was developed to help examine design decisions in the production of a new product in relation to dependability requirements imposed on the product and for environmental concerns in product operation in addition to the expert's opinion and views on various aspects. Another expert system, ARDA [110], helps analyse reliability data. Yet another expert system, RAMES [101], has been developed to assist a weapon system program in weapon system RAM performance analysis and enhancement and many other considerations.

19.5 Alternative Approaches

The main drawback of the probabilistic approach to performance evaluation of an engineering system is the uncertainty associated with the results, which puts the entire process in question. Specifying uncertainty by specifying mean and variance or confidence levels is not found to be the best way of estimating the quality of results. Although some intuitive methods of accounting, combination and propagation of uncertainty exist, these have not been found satisfactory by engineers. While Bayesian models have been extensively used, primarily as a numerical for representation and inference with uncertainty, this again masks the problem of uncertainty when priors are selected and ignorance remains hidden in the priors. All these shortcomings of the probabilistic approach led researchers to look for alternative approaches to system performance assessment.

The conventional probabilistic approach treats failure events as random occurrences and low *probability* of an event does not necessarily mean low *possibility* or that it will rarely occur. In fact, the worst accidents in human history had very low probability evaluated for their occurrence. Zadeh [3] put forward a fuzzy set theory, which appears to resolve these inconsistencies by offering a *possibilistic* approach to performance evaluation based on the premise that small probability does not always mean low possibility, whereas a low probability necessarily should imply low probability. In fact, a large number of papers has published in this area, which holds the promise of providing an alternative approach to the probabilistic approach. Fuzzy set theory also provides to resolve the gap between the *perceived risk* (subjective) and the *statistical risk* (objective), and in the opinion of the editor of this handbook this is a very appropriate area of application of fuzzy set theory. In fact, fuzzy set theory has the capability of providing models close to human thinking or the brain, which has the asset of inferring and decision making in a fuzzy environment. There have been several papers [30, 46, 68, 79, 80, 91, 97, 98, 107, 118 and 125] on the system analysis and design based on fuzzy set theory and it appears logical that this area will be explored extensively in near future.

Another approach that is being actively pursued is the Dempster–Shafer theory [93, 119], which may offer an interesting alternative approach to system performance assessment. This handbook therefore includes an expository chapter with a long list of references to familiarize the reader with these aspects of performance assessment.

19.6 Reliability Design Procedure

The usual design procedure followed by a system designer is:

- Define system terms of the operational requirements.
- Develop an index of system effectiveness and arrange the system into several non-interacting subsystems.
- Apply mathematical techniques to evaluate alternate system configurations in terms of reliability (or any other system effectiveness index) and constraints on resources,
- Specify a system configuration, maintenance policy and inter-relationship with other factors.
- Allocate failure and repair rates to each individual component so as to meet the specified system reliability goals.

In general, reliability is considered to be a good criterion for system effectiveness. However, depending upon the mission, some other criteria may be selected for design. Some of the other parameters that may be of interest are: availability or maintainability, probability of mission success, mean time to failure, duration of single downtime, or operational readiness, *etc*.

Any one of the above (or more) may form the criterion of optimal system design and, therefore, be traded off with some of the constrained resources such as cost, weight, power consumption, *etc*. For non-maintained systems, generally an index of reliability is sufficient for the system reliability effectiveness. However, for maintained systems, it is not enough to base system design on the reliability criterion. For almost all process systems or energy systems, the basic necessity is to know the percentage of time that the systems are available. This establishes criteria for the design based on the system availability; thus one may be interested in maximizing the system availability. Alternately one may rather be interested in comparing the design alternatives based on the duration of the single downtime or the frequency of failures. Whatever the criterion of assessment of various alternatives for design may be, one should be able to build a mathematical model for the design problem that will fit into the present-day techniques of solution.

The above guidelines are by no means the ultimate rule; the actual design procedure depends entirely upon the system under study. However, it is an established fact that, in order to arrive at an optimal design, the allocation process either of reliability or redundancy forms an integral part of the whole design procedure.

We have already seen in an earlier section that the use of either redundancy or high reliability components is a means of achieving a desired level of system reliability. Therefore, the design includes an allocation of either redundancy or reliability or both in a system. For a maintained system design, usually maximization of availability is desired rather than system reliability. However, if maximization of the system reliability is the objective and the state-of-art permits it, failure and repair rates are allocated to each component of the system in order to maximize its system reliability subject to some specified techno-economic constraints on the system design. Moreover, because we cannot stock any number of spares due to limited resources, it becomes imperative to seek an optimal allocation for spare parts while maximizing system availability or reliability subject to constraints on cost, *etc*., or else one can minimize the cost of spares subject to the specified level of availability.

The subject of optimal system design is discussed in two chapters, *viz.,* Chapters 32 and 33, where various formulations for the system design problem and their solution techniques are discussed in depth.

19.7 Reliability Testing

An important feature of reliability engineering today, as distinct from the past when we could have talked qualitatively only, is that we are in a position to say and demonstrate how reliable a product is. This has been made possible by reliability testing and demonstration. Reliability testing is also a major source of generating reliability data. Testing is also required for design review, *failure mode and effect analysis* (FMEA), trade-off studies, *etc*.

Component testing is an important activity in any reliability improvement program. Here tests are generally carried out to determine design margins and failure modes. Testing is also a must on all unproven components. Although component level testing can provide basic design data and helps weed out weak designs, it is not adequate enough in comparison to product or system testing. System testing comprises testing the complete unit or product and is carried out as far as possible under actual stress and environmental conditions. For thorough effectiveness system testing is done on an iterative basis, *i.e.*, test, fail, fix-retest cycle.

Reliability demonstration is done based on life tests. As such, these tests are time consuming and expensive. It is therefore imperative that tests are planned in such a way so as to give maximum information with the fewest items put to test. It is also important that the items to be tested and the performance of the tests be closely controlled in order to assure their validity. Very often products may be put to *accelerated life tests* and may therefore be tested at higher temperature, pressure or other stresses to reduce the test time. This may not be possible for many types of products, particularly when the failure mode is likely to change with an increase in the stress level.

Usually the following tests are in vogue:

Development tests: These are initiated at the time of first prototype assembly and constitute

- Performance tests conducted in a normal environment.
- Environment tests under the specified environment conditions.
- Endurance tests providing data determining the degree of degradation resulting from operating the item over an extended period of time.

Qualification tests: These tests are primarily designed to subject a product to the various environmental conditions and operating stress levels that it is expected to encounter in use. The details of the tests are actually worked out on a mutual basis between producer and consumer and are witnessed by the agents of the consumer. Generally, the decisions are of failure/success or go, no-go type, with no gradation between the two. For these tests the sample sizes are generally small.

Reliability demonstration tests: These tests are performed to demonstrate the product's ability to perform its functions repeatedly, and therefore the criterion is based on MTBF or MTTF. The purpose of these tests is to determine how long a device will continue to function under the specific environment or loading conditions. The maximum number of samples within the economic limits is subjected to these tests.

Accelerated life test: Traditional "*life data analysis*" involves analyzing the time-to-failure data (of a product, system or component) obtained under "*normal*" operating conditions in order to quantify the life characteristics of the product, system or component. In many situations, and for many reasons, such life data (or time-to-failure data) is very difficult, if not impossible, to obtain. The reasons for this difficulty can include the long life times of today's products, the small time period between design and release, and the challenge of testing products that are used continuously under normal conditions. Given this difficulty, and the need to observe failures of products to better understand their failure modes and their life characteristics, reliability practitioners have attempted to devise methods to force these products to fail more quickly than they would under normal use conditions. In other words, they have attempted to accelerate their failures.

Accelerated tests are necessary for obtaining life data quickly. Life testing of products under higher stress levels, without introducing additional failure modes, can provide significant savings of both time and money. Correct analysis of data gathered via such accelerated life testing can yield parameters and other information for the product's life under use stress conditions.

Types of Accelerated Tests:

Different types of tests, that have been called accelerated tests, provide different information about the product and its failure mechanisms.

Generally, accelerated tests can be divided into three types:

Qualitative tests: in general, qualitative tests are not designed to yield life data that can be used in subsequent analysis or for "accelerated life test analysis." In general, qualitative tests do not quantify the life (or reliability) characteristics of the product under normal use conditions. They are designed to reveal probable failure modes. However, if not designed properly, they may cause the product to fail due to modes that would not be encountered in real life. Qualitative tests have been referred to by many names, including elephant tests, torture tests, HALT (highly accelerated life testing) and shake and bake tests.

Elephant tests: These tests are known by several other names, such as design margin tests, design qualification tests, toture tests, shake and bake tests or killer tests. Generally, the sample is small or just one and the specimen is subjected to a single extreme value of stress or thermal cycling, or to a number of stresses, simultaneously or sequentially. If a product passes this test, the designer is satisfied with the design but if the product fails this test, the deginer has to redesign the product or appropriate measure is taken to improve manufacturing. It is not necessary that an elephant test produce a failure that the product may encounter in actual use. Therefore, it may be necessary to devise different elephant tests, such as a high voltage test to reveal electrical failure modes and vibration tests to reveal mechanical failure modes.

Environmental stress screening (ESS): ESS is a process involving accelerated testing of products in an environment such as random vibration and thermal cycling, and shock and bake. The goal of ESS is twofold. The first is as an elephant test during development; its purpose is to expose design and manufacturing problems. The other is accelerated burn-in during manufacturing to improve reliability. MIL-HDBK-344 for electronic equipment and MIL-STD-883C for microelectronics are used.

Burn-in: Burn-in consists of running items under design or accelerated conditions. Burn-in can be regarded as a special case of ESS. Burn-in is a test performed for the purpose of screening or eliminating freak or marginal devices with inherent defects or defects with manufacturing aberrations before customers receive them. If items fail early, they have manufacturing defects. Burn-in is generally used for electronic components and equipment. Static and dynamic burn-in is used on the devices depending upon the complexity and their failure mechanisms.

ESS and burn-in are performed on the entire population and do not involve sampling. ESS includes burn-in as one of its purposes. Although ESS has evolved from burn-in, it is far more advanced process. ESS is an accelerated process of stressing a product in continuous cycles between predetermined environmental extremes mainly comprising temperature cycling and random vibrations. Burn-in, therefore, is a special case of ESS where the temperature change rate for thermal cycling is zero and vibration is sinusoidal if used. The interested reader is referred to the classical book of Kececioglu and Sun [127] on the subject of burn-in.

Quantitative accelerated life tests: Quantitative accelerated life testing, unlike qualitative testing methods, consists of quantitative tests designed to quantify the life characteristics of a product, component or system under normal use conditions, and thereby provide information on the probability of failure of the product under use conditions, mean life under use conditions, and projected returns and warranty costs. It can also be used to assist in the performance of risk assessments, design comparisons, *etc*.

Accelerated life testing can take the form of "usage rate acceleration" or "overstress acceleration." For all life tests, time-to-failure information for the product is always required

Usage rate acceleration: For products that do not operate continuously under normal conditions, if the test units are operated continuously, failures are encountered earlier than if the units are tested under normal usage. For example, if we assume an average washer use of six hours a week, one could conceivably reduce the testing time 28-fold by testing these washers continuously. Data obtained

through usage acceleration can be analyzed with the same methods used to analyze regular time-to-failure data.

Overstress acceleration: For products with very high or continuous usage, the accelerated life-testing practitioner must stimulate the product to fail in a life test. This is accomplished by applying stress levels that exceed the levels that a product will encounter under normal use. The time-to-failure data obtained under these conditions is then extrapolated to use conditions. Accelerated life tests can be performed at high or low temperatures, humidity, voltage, pressure, vibration, *etc*., and/or combinations of stresses to accelerate or stimulate the failure mechanisms.

Accelerated life test (ALT) stresses and stress levels should be chosen so that they accelerate the failure modes under consideration but do not introduce failure modes that would never occur under use conditions. Normally, these stress levels should fall outside the product specification limits but inside the design limits. Usually it is assumed that intrinsic failures due to wear out may only exist and this assumption may not be quite valid in certain cases particularly in the presence of randomly occurring defects due to the manufacturing process. In those cases one may use the methodology described in [135].

HALT and HASS: HALT and HASS are not meant to simulate the environment in field but their sole purpose is to expose weak links in the design and processes while using only a small sample size and in a very short time. The stresses are stepped up to well beyond the expected environment in actual use until the "fundamental limit of technology" is reached. Each weak link discovered provides an opportunity to improve the product design or the processes that may lead to the improved reliability of a product, reduced costs, and reduced design time. It is basically ruggedization of design as a robust product exhibits higher reliability than a non-robust product.

HASS is a 100% screening of the production of items using stresses that are higher than those met in normal use. In HASS, accelerated stresses are applied to production in order to shorten the time to failure of the defective unit, and to shorten the corrective action time and the number of units built with the same flaw. HASS is generally not possible without comprehensive HALT. Without HALT, fundamental design limits will restrict the acceptable stress levels in the production screens.

The originator of HALT and HASS is Gregg K. Hobbs [131] and he has authored a chapter in this handbook on HALT and HASS.

Multiple Environment Overstress Tests (MEOST)
MEOST claims to provide powerful tools that can predict and correct potential field failures at the design stage of the product, besides claiming that it [144] can reduce the design test cost both in terms of labor and the number of units required to demonstrate reliability, as well as reducing the design cycle times. In MEOST the objective is not to pass a product but to fail it, which will highlight the weakness of the design. A single stress or environment is not sufficient to generate failures. More than one stress applied sequentially is not enough to ferret out the interaction effects. Therefore, several stresses or environments are combined simulating the field conditions as closely as possible to create synergy of interaction effects. The combined overstresses go beyond the design stress level to a maximum possible overstress limit (MPOSL) and the rate of overstress is accelerated to produce failures in the shortest possible time. It is claimed that the Apollo lunar module was the first to be subjected to MEOST methodology. Since 1960, MEOST has been successfully applied to aircraft engines, helicopters, automobiles aerospace equipment, *etc.*

19.8 Reliability Growth

The objective of reliability growth is to improve reliability over time during product development. This is primarily during the design and manufacturing phase of the product and is achieved by following a process of test-fix-test-fix cycle. Reliability tests are conducted on prototypes to ensure that reliability goals have been met. Failure analysis is conducted to identify the high failure modes in case the goal is not met and these modes are then fixed. We try to eliminate these modes or attempt to lessen their effects in order to improve

reliability. This cycle is repeated and failure data generated from the tests are plotted in the form of a growth curve called the *reliability growth curve*. As has been mentioned, this growth curve is obtained through continuous tests, evaluation and redesign activity. The earliest reliability growth model was proposed by Duane [2], who enunciated that a plot of the logarithm of the cumulative number of failures per test time *versus* the logarithm of the test time during growth testing is approximately linear. There are other growth models such as Crow-AMSAA [10]. Crow observed that the Duane model could be stochastically represented as a Weibull process and this stochastic extension became what is known as the Crow-AMSAA model; this model was first developed at the US Army Material System Analysis Activity. It is used with systems when usage is measured on a continuous scale. There are other models as well, such as the Lloyd and Lipow model [1], the Gompertz model [4], the Crow extended model [143], and the logistic [87] model. A good coverage of various other models is provided in [44, 106, 126].

References

[1] Lloyd DK, Lipow M. Reliability growth models. In Reliability Management, Methods and Mathematics. Prentice-Hall, Englewood Cliffs, NJ, 1962; 330–338.

[2] Duane JT. Learning Curve Approach to Reliability Monitoring. IEEE Trans. on Aerospace 1964; 2(2):563–566.

[3] Zadeh LA. Fuzzy sets. Information Control 1965;8: 338–353.

[4] Virene EP. Reliability growth and the upper reliability limit, How to use available data to calculate. Proc. Annual Symp. on Rel. (IEEE cat. no. 68 C33-R) Jan. 1968: 265–270.

[5] Misra KB, Rao TSM. Reliability analysis of redundant networks using flow graphs. IEEE Trans. on Rel. 1970; Feb., R-19(1):19–24.

[6] Misra KB. An algorithm for reliability evaluation of redundant networks. IEEE Trans. on Rel. 1970; Nov., R-19(4):146–151.

[7] Hansler E. A fast recursive to calculate the reliability of a communication network. IEEE Trans. on Com. 1972; June, Com-20(3): 637–640.

[8] Kershenbaum A, Van Styke RM. Recursive analysis of network reliability. Networks 1973; 3: 81–94.

[9] Hasofer AM, Lind NC. Exact and invariant second moment code format. J. of the Engg. Mechanics Div.ASCE 1974; 100: 111–121.

[10] Crow LH. Reliability Analysis for complex, repairable systems in reliability and biometry. SIAM. Proschan F. and Serfling RJ. (Eds.) 1974: 379–410.

[11] Rao SS. A probabilistic approach to the design of gear trains. Int J. of Machine Tool Design and Research 1974; 14: 267–278.

[12] Proctor CL, Singh B. A three-state system Markov model. Microelectronics and Rel. 1975; 14 (5/6):463–464.

[13] Aggarwal KK, Gupta JS, Misra KB. Reliability evaluation: A comparative study of different methods. Microelectronics and Rel. 1975; 14(1):49–56.

[14] Aggarwal KK, Gupta JS, Misra KB. Computational time and absolute error comparison for reliability expression derived by various methods. Microelectronics and Rel. 1975; 14: 465–467.

[15] Aggarwal KK, Misra KB, Gupta JS. A fast algorithm for reliability evaluation. IEEE Trans. on Rel. 1975; April, R-24(1): 83–85.

[16] Balagurusamy E, Misra KB. Reliability and mean life of a parallel system with non-identical units. IEEE Trans. on Rel. 1975; R-24 (5): 340–341.

[17] Balagurusamy E, Misra KB. Failure rate derating chart for parallel redundant units with dependent failures. IEEE Trans. on Rel. 1976; R-25 (2): 122.

[18] Misra KB, Balagurusamy E. reliability analysis of k-out-of –n: G system with dependent failures. Int. J. System Science 1976; Nov., 7(11): 1209–1215.

[19] Balagurusamy E, Misra KB. Avaliability and failure frequency of repairable m-order systems. Int. J. System Science 1976; Nov., 7(11): 1209–1215.

[20] Lin PM, Leon BJ, Huang TC. A new algorithm for symbolic system reliability analysis. IEEE Trans. on Rel. 1976; R-25(1): 2–15.

[21] DeMercado J, Spyratos N, Bowen BA. A method for calulation of network reliability. IEEE Trans. on Rel. 1977; R-25(2): 71–76.

[22] Sifakis J. Use of timed Petri nets for performance evaluation. 3rd Int. Symp. Beliner and Gelenbe, Editors. Measuring, Modeling and Evaluating Computer System 1977; 75–95.

[23] Satyanarayana A, Prabhakar A. New topological formula and rapid algorithm for reliability analysis

of complex networks. IEEE Trans. on Rel. 1978; June, R-27(2):82–100.
[24] Misra KB, Raja AK. A laboratory model for system reliability analyzer. Microelectronics and Rel. 1979; 19(3): 259–264.
[25] Fiessler B, Neumann H-J, Rackwitz R. Quadratic limit states in strucural reliability. J. of the Engg. Mechanics Div.ASCE 1979; 105: 661–676.
[26] Abraham JA. An improved algorithm for network reliability. IEEE Trans. on Rel. 1979; April, R-28(1):58–62.
[27] Gadani JP, Misra KB. Reliability evaluation of a system with imperfect nodes and links using network approach. Systems Science 1979; 5(3): 265–274.
[28] Kontoleon JM. Reliability determination of a r-successive-out-of-n:F system. IEEE Trans. on Rel. 1980; Dec., R-29 (5): 327.
[29] Gadani JP, Misra KB. Network reliability evaluation of three-state devices using transformation technique. Microelectronics and Rel. 1981; 21(2): 231–234.
[30] Misra KB, Sharma A. performance index to quantify reliability using fuzzy subset theory. Microelectronics and Rel. 1981; 21(4): 543–549.
[31] Locks MO. Recursive disjoint products: A review of three algorithms. IEEE Trans. on Rel. 1982, R-31(1): 33–35.
[32] Bollinger RC, Salvia AA. Consecutive –k-out-of-n: F networks. IEEE Trans. on Rel. 1982; April, R-31 (1): 53–56.
[33] Misra KB, Prasad P. Comment on reliability evaluation of a flow network. IEEE Trans. on Rel. 1982; June, R-31(2):174–176.
[34] Gadani JP, Misra KB. A network reduction and transformation algorithm for the assessment of system effectiveness indices. IEEE Trans. on Rel. 1981; April, R-30 (1): 48–57.
[35] Bansal VK, Misra KB. Hardware approach for generating spanning trees in reliability studies. Microelectronics and Rel. 1981; 21(2): 243–253.
[36] Gadani JP, Misra KB. Quadrilateral-star transformation: an aid for reliability evaluation of large complex systems. IEEE Trans. on Rel. 1982; April, R-31 (1): 49–59.
[37] Bansal VK, Misra KB, Jain MP. Minimal path sets and minimal cut sets using a search technique. Microelectronics and Rel. 1982; 22(6): 1067–1075.
[38] Hura GS. Petri nets as a modeling tool. Microelectronics and Rel. 1982; 22(3): 433–439.
[39] Molloy MK. Performance analysis using stochastic Petri nets. IEEE Trans. on Rel. 1982; Sep., R-31(9): 913–917.
[40] Bennetts RG. Analysis of reliability block diagrams by Boolean techniques. IEEE Trans. on Rel. 1982; June, R-31(2): 159–166.
[41] Aggrawal KK, Chopra YC, Bajwa JS. Capacity consideration in reliability analysis of communication systems IEEE Trans. on Rel. 1982; June, R-31(2): 177–181.
[42] Laviron A, Carnino A, Manaranche. ESCAF- A new and cheap system for complex reliability analysis and computation. IEEE Trans. on Rel. 1982; R-31(4):339–349.
[43] Bansal VK, Misra KB, Jain MP. Improved Implementation of a search technique to find spanning trees. Microelectronics and Rel. 1983; 23(1): 141–147.
[44] Crow LH. Methods for reliability growth assessment during development. In Electronic Systems Effectiveness and Life Cycle Testing. Skwirzynski JK (Ed.) Springer-Verlag, 1983.
[45] Kenyon RL, Newell RJ. Steady-state availability of k-out-of-n:G system with single repair. IEEE Trans. on Rel. 1983; June, R-32 (2): 188–190.
[46] Tanaka H, Fan LT, Lai FS, Taguchi K. Fault tree analysis by fuzzy probability. IEEE Trans. on Rel. 1983; Dec., R-32 (5); 453–457.
[47] Satyanarayana A, Wood RK. A linear-time algorithm for computing k terminal reliability in series-parallel networks. SIAM Journal of Computing 1983; 14: 818–832.
[48] Agrawal A, Barlow RE. A survey of network reliability and domination theory. Operations Research 1984; May-June, 32: 478–492.
[49] Agrawal A, Satyanarayana A. An O(/E/) time algorithm for computing the reliability of a class of directed networks. Operations Research 1984; May-June, 32: 493–517.
[50] Breitung K. Asymptotic approximations for multinormal Integral. J. of the Engg. Mechanics Div. ASCE 1984; 110: 357–366.
[51] Schneeweiss WG. Disjoint Boolean products via Shanon's expansion. IEEE Trans. on Rel. 1984; Oct., R-33(4):329–332.
[52] Fu JC. Reliability of a large consecutive-k-out-of-n: F system. IEEE Trans. on Rel. 1985; June, R-34 (2): 127–130.
[53] Locks MO. Recent developments in computing of system reliability. IEEE Trans. on Rel. 1985; Dec., R-34(5):425–436.
[54] O'Connor Patrick DT. Practical reliability engineering. John Wiley & Sons, Chichester,U.K., 1985.
[55] Madson HO, Krenk S, Lind NC. Methods of structural safety. Prentice-Hall Inc. Englewood, New Jersey, 1986.

[56] Wood RK. Factoring algorithms for computing k-terminal network reliability. IEEE Trans. on Rel. 1986; Aug., R-35 (3): 269–278.
[57] Andrew PK. Improvement of operator reliability using expert systems. Int. J. of Rel. Engg. 1986; 14(4): 309–319.
[58] Melcher RE. Structural reliability analysis and prediction. Ellis Horwood, Chichester, U.K.,1987.
[59] Rai S, Kumar A. Recursive technique for computing system reliability. IEEE Trans. on Rel. 1987; April, R-36(1): 38–44.
[60] Beichelt F, Spross L. An improved Abraham method for generating disjoint sums. IEEE Trans. on Rel. 1987; April, R-36(1): 70–74.
[61] Locks MO. A minimizing algorithm for sum of disjoint products. IEEE Trans. on Rel. 1987; Oct., R-36(4): 445–453.
[62] Rushdi AM. Efficient computation of k-to-l-out-of-n system reliability. Int. J. of Rel. Engg. 1987; 17:157–163.
[63] Rushdi AM. Performance Indexes of a telecommunication network. IEEE Trans. on Rel. 1988; April, 37(1): 57–64.
[64] Yoo YB, Deo N. A comparison of algorithms for terminal-pair reliability. IEEE Trans. on Rel. 1988; June, 37(2): 210–215.
[65] Page LB, Perry JE. A practical implementation of the factoring theorem for network reliability. IEEE Trans. on Rel. 1988; Aug., R-37 (3): 259–267.
[66] Hura GS, Etessami FS. The use of petri nets to analysis coherent fault trees. IEEE Trans. on Rel. 1988; Dec., R-37 (5): 469–474.
[67] Ball MO, Provan JS. Disjoint products and efficient computation on reliability. Operations Research 1988; Oct., 36:703–715.
[68] Misra KB, Weber GG. A new method for fuzzy fault tree analysis. Microelectronics and Rel. 1989; 29(2): 195–216.
[69] Heidtmann KD. Smaller sums of disjoint products by subproduct inversion. IEEE Trans. on Rel. 1989; Aug., R-38 (3): 305–311.
[70] Beichelt F, Spross L. Comments on: An improved Abraham method for generating disjoint sums. IEEE Trans. on Rel. 1989; Oct., R-38 (4): 422–424.
[71] Page LB, Perry JE. Reliability of directed networks using the factoring theorem. IEEE Trans. on Rel. 1989; Dec., R-38 (5): 556–562.
[72] Mandaltsis D, Kontoleon J. Enumeration of k-trees and their applications to reliability evaluation of communication networks. Microelectronics and Rel. 1989; 29 (5): 733–735.
[73] Moureau R. FURAX: Expert system for automatic generation of reliability models for electrical or fluid networks. Proc. 7th International Conf. on Rel. and Maint., Brest, France 1990.
[74] Dumai A, Winkler A. Reliability prediction model for gyroscopes. Proc. Annual Rel. and Maint. Symp. Los Angeles, California, USA 1990; 5–9.
[75] Vannoy EH. Improving MIL-HDBK-217 type models for predicting mechanical reliability. Proc. Annual Rel. and Maint. Symp. Los Angeles, California, USA 1990; 341–345.
[76] Bowles JB, Klein LA. Comparison of commercial reliability prediction programs. Proc. Annual Rel. and Maint. Symp., Los Angeles, California, USA 1990; 450–455.
[77] Elliott MS. Knowledge-based systems for reliability analysis. Proc. Annual Rel. and Maint. Symp., Los Angeles, California, USA 1990; 481–489.
[78] Lehtela M. Computer-aided failure mode and effect analysis of electronic circuits. Microelectronics and Rel. 1990; 30 (4): 761–773.
[79] Misra KB and Weber GG. Use of fuzzy set theory for level-1 studies in probabilistic risk assessment. Fuzzy Sets and Systems 1990; 37: 139–160.
[80] Onisawa T. An application of fuzzy concepts to modeling of reliability analysis. Fuzzy sets and Systems 1990; 37:389–393.
[81] Wilson JM. An improved minimizing algorithm for sum of disjoint products. IEEE Trans. on Rel. 1990; April, R-39 (1): 42–45.
[82] Helman P, Rosenthal A. A decomposition scheme for the analysis of fault trees and other combinatorial circuits. IEEE Trans. on Rel. 1990; April, R-39 (1): 76–86.
[83] Kuo W, Zhang W, Zuo M. A consecutive k-out-of-n: G system: The mirror image of a consecutive-k-out-of-n: F system. IEEE Trans. on Rel. 1990; June, R-39 (2): 244–253.
[84] Rushdi AM. Some open questions on: Strict consecutive-k-out-of-n: F systems. IEEE Trans. on Rel. 1990; June, R-39 (2): 380–381.
[85] Papastavridis S. m-consecutive-k-out-of-n:F systems. IEEE Trans. on Rel. 1990; Aug., R-39 (3): 386–388.
[86] Politof T, Satyanarayana A. A linear time algorithm to compute the reliability of planer cube-free networks. IEEE Trans. on Rel. 1990; Dec., R-39(5): 557–563.
[87] Kececioglu DB. Reliability growth. In Reliability Engineering Handbook Ed. 4, Vol 2. Prentice-Hall, Englewood Cliffs 1991; 415–418.
[88] Clark WB. Analysis of reliability data for mechanical systems. Proc. Annual Rel. and Maint. Symp. Orlando, Florida, USA 1991; 438–441.

[89] Thien-My D, Lin Z, Massoud M. Mechanical strength reliability evaluation using an iterative approach. Proc. Annual Rel. and Maint. Symp., Orlando, Florida, USA 1991; 446–450.

[90] Noh S, Rai S. Experiment results on preprocessing of paths/cuts terms in some of disjoint product techniques. Proceedings of the Infocom 1991; 533–542.

[91] Kenaranuie R. Event-tree analysis by fuzzy probability. IEEE Trans. on Rel. 1991; April, R-40 (1): 120–124.

[92] Rushidi AM. Comments on: An efficient non-recursive algorithm for computing the reliability of k-out-of-n system. IEEE Trans. on Rel. 1991; April, R-40 (1): 60–61.

[93] Inagaki T. Interdependence between safety-control policy and multiple sensor schemes via Dempster-Shafer theory. IEEE Trans. on Rel. 1991; June, R-40 (2): 182–188.

[94] Theologu OR, Carlier JG. Factoring and reductions for networks with imperfect vertices, IEEE Trans. on Rel. 1991; June, R-40 (2): 210–217.

[95] Veeraraghavan M, Trivedi KS. An improved algorithm for the symbolic reliability analysis of networks. IEEE Trans. on Rel. 1991; Aug., R-40 (3): 347–360.

[96] Shooman AM, Kershenbaum A. Exact graph-reduction algorithms for network reliability analysis. Technical repot, IBM TJ Watson Research Center, Hawthorne, New York, 1991.

[97] Onisawa T. Fuzzy reliability assessment considering the influence of many factors on reliability. IEEE Trans. on Rel 1991; Dec., R-40 (5): 563–571.

[98] Guth MAS. A probabilistic foundation for vagueness and imprecision in fault tree analysis. IEEE Trans. on Rel. 1991; Dec., R-40 (5): 563–571.

[99] Karunanithi N, Whitney D, Malaiya YK. Using neural networks in reliability prediction. IEEE Software. July/Aug. 1992; 9(4) : 53–59.

[100] Zaitri CK, Keller AZ, Fleming PV. A smart FMEA (Failure Modes and Effects Analysis) package. Proc. Annual Rel. and Maint. Symp., Las Vegas, USA 1992; 414–421.

[101] Hansen WA, Edson BN, Larter PC, Reliability, availability and maintainability expert system (RAMES), Proc. Annual Rel. and Maint. Symp. Las Vegas, USA 1992; 478–482.

[102] Locks MO, Wilson JM. Note on disjoint product algorithms. IEEE Trans. on Rel. 1992; March, R-41 (1): 81–84.

[103] Misra KB. Reliability analysis and prediction: A methodology oriented treatment. Elsevier Science Publishers BV, Amsterdam, 1992.

[104] Iyer S. Distribution of lifetime of consecutive k-within m-out-of-n: F systems. IEEE Trans. on Rel. 1992; Sept., R-41 (3): 448–450.

[105] Boehme TK, Kossow A, Preuss W. A generalization of consecutive k-out-of-n: F systems. IEEE Trans. on Rel. 1992; Sept., R-41 (3): 448–450.

[106] Xie M, Zhao M. On some reliability growth models with simple graphical interpretations. Microelectronics and Rel. 1993; 33(2): 149–167.

[107] Soman KP, Misra KB. Fuzzy fault tree analysis using resolution identity. Int. J. of Fuzzy Sets and Mathematics 1993; 1:193–212.

[108] Soman KP, Misra KB. A least square estimation of three parameters of a Weibull distribution. Microelectronics and Rel. 1992; 32(3): 303–305.

[109] Soman KP, Misra KB. Moments of order statistics using the orthogonal inverse expansion method and its application in reliability. Microelectronics and Rel. 1992; 32 (4): 469–473.

[110] Ansell J, Al-Doori M. ARDA: Expert system for reliability data analysis. Proc. Int. Conf. on APL 1993; 1–5.

[111] Veeraraghavan Malathi, Trivedi Kishor S. Multi-variable inversion techniques. In Misra KB, (Ed.) New Trends in System Reliability Evaluation. Elsevier, 1993; 39–73.

[112] Beichelt Frank. Decomposition and reduction techniques. In Misra KB, (Ed.). New trends in system reliability evaluation. Elsevier, 1993; 75–114.

[113] Shooman Andrew M. Probabilistic graph-reduction techniques. In Misra KB, (Ed.) New Trends in System Reliability Evaluation. Elsevier, 1993; 117–163.

[114] Deo Narsingh, Medidi Muralidhar. Parallel algorithms and implementations. In Misra KB, (Ed.) New Trends in System Reliability Evaluation. Elsevier, 1993; 165–182.

[115] Rushdi Ali M. Reliability of k-out-of-n systems. In Misra KB, (Ed.) New Trends in System Reliability Evaluation. Elsevier, 1993; 185–221.

[116] Papastavridis SG, Koutras MV. Consecutive-k-out-of-n systems. In Misra KB, (Ed.) New Trends in System Reliability Evaluation. Elsevier, 1993; 228–242.

[117] Hura GS. Use of Petri nets for system reliability evaluation. In Misra KB, (Ed.) New Trends in System Reliability Evaluation. Elsevier, 1993; 339–364.

[118] Onisawa Takehisa, Misra KB. Use of fuzzy set theory (Part-II: Applications). In Misra KB, (Ed.) New Trends in System Reliability Evaluation. Elsevier, 1993; 551–583.
[119] Inagaki T. Dempster-Shafer theory and its applications. In Misra KB, (Ed.) New Trends in System Reliability Evaluation. Elsevier, 1993; 587–623.
[120] Russomanno DJ, Bonnell RD, Bowles JB. Expert systems for reliability evaluation. In Misra KB, (Ed.) New Trends in System Reliability Evaluation. Elsevier, 1993; 625–651.
[121] Misra KB. Reliability analyzer. In Misra KB, (Ed.) New Trends in System Reliability Evaluation. Elsevier, 1993; 653–700.
[122] Soman KP, Misra KB. On Bayesian estimation of system reliability. Microelectronics and Rel. 1993; 33 (10): 1455–1493.
[123] Soman KP, Misra KB. Bayesian sequential estimation of two parameters of a Weibull distribution. Microelectronics and Rel. 1994; 34 (3): 509–519.
[124] Soman KP, Misra KB. A simple procedure of computing variance sensitivity coefficients of top events in a fault tree. Microelectronics and Rel. 1994; 34 (5): 929–934.
[125] Soman KP, Misra KB. Estimation of parameters of failure distributions with fuzzy data. Int. J. Systems Science. 1995; 26(3): 659–670.
[126] Reliability growth-statistical test and estimation methods. IEC-1164 International Electrotechnical Commission, 1995.
[127] Kececioglu Dimitri, Sun F-B. Burn-in testing: Its quantification and optimization, Prentice Hall PTR, New Jersey, 1997.
[128] Meeker WQ, Esobar LA. Statistical methods for reliability data. John Wiley & Sons, New York, 1998.
[129] Zuo Ming J, Lin Daming, Wu Yanhong. Reliability evaluation of combined k-out-of-n:F, consecutive-k-out-of-n:F, and Linear connected-(r; s)-out-of-(m; n):F system structures. IEEE Trans. on Rel. 2000; March, 49(1): 99–105.
[130] Zuo MJ, Lin Daming, Wu Y. Reliability evaluation of combined k-out-of-n:F, consecutive-k-out-of-n:F and linear connected-(r, s)-out-of-(m, n):F system structures. IEEE Trans. on Rel. 2000; March, 49(1): 99–104.
[131] Hobbs Gregg K. Accelerated Reliability Engineering: HALT and HASS. John Wiley & Sons, Chichester, U.K.2000.
[132] Roy Dilip, Dasgupta Tanmoy. A discretizing approach for evaluating reliability of complex systems under stress-strength model. IEEE Trans. on Rel. 2001; June, 50(2): 145–150.
[133] Jones Jeff, Hayes Joe. Estimation of system reliability using a "non-constant failure rate" model. IEEE Trans. on Rel. 2001; Sept., 50(3): 286–288.
[134] Boushaba M, Ghoraf N. A 3-Dimensional consecutive-k-out-of-n:F models. Int. J. Rel. Qua. & Safety. 2002; 9(2): 111–125.
[135] Kim CM, Bai DS. Analysis of accelerated life test data under two failure modes. Int. J. Rel. Qua. & Safety. 2002; 9(2): 111–125.
[136] Kececioglu Dimitri. Reliability & Life Testing Handbook , Vol. I and II, DEStech Publications, Lanceste, .Pa., U.S.A. 2002.
[137] Chaturvedi SK, Misra KB. An efficient multi-variable inversion algorithm for reliability evaluation of complex systems using path sets. Int. J. of Rel., Qua. and Safety Engg 2002; 9(3): 237–259.
[138] Chaurvedi S.K., Misra K.B. A hybrid method to evaluate reliability of complex system. Int. J. Qua. Rel. Management 2002; 19 (8/9): 1098–1112.
[139] Levitin G. Reliability evaluation for acyclic transmission networks of multi-state elements with delays. IEEE Transactions on Rel. 2003; June, 52(2): 231 – 237.
[140] Jones JA, Marshall JA, Aulak G, Newman B. Development of an expert system for reliability task planning as part of REMM methodology. Pro. Annual Rel and Maint. Symp. 2003; 423–428.
[141] Lee Jungwon Huh, Haldar SY, Yosu A. Reliability evaluation using finite element method. Fourth International Symposium on Uncertainty Modeling and Analysis I SUMA 2003: 28 – 33.
[142] Levitin Gregory. Reliability of multi-state systems with two failure-modes IEEE Trans. on Rel. 2003; Sept., 52(3): 340–348.
[143] Crow LH. An extended reliability growth model for managing and assessing corrective actions. IEEE Proc. of Annual Rel. and Maint. Symp. 2004; 73–80.
[144] Bhote KR, Bhote AK. World class reliability: Using multiple environment overstress tests to make it happen. American Management Association ,New York, 2004.
[145] Lin Min-Sheng. An O(k2 log(n)) algorithm for computing the reliability of consecutive-k-out-of-n:F systems. IEEE Trans. on Rel. 2004; 53(1): 3-6.
[146] Nelson Wayne B. Applied Life Data Analysis. Wiley-Interscience, New Jersey, U.S.A. 2004.
[147] Nelson Wayne B. Accelerated testing: Statistical models, test plans, and data analysis. Wiley-Interscience, New Jersey, U.S.A. 2004.

[148] Xinjian Xiang, Dingfei-Ge. Research on reliability evaluation of electronic products under environmental conditions. Fifth World Congress on Publication Intelligent Control and Automation 2004; June 15–19, 4: 3146–3149.

[149] Hongbin Li, Qing Zhao. A cut/tie set method for reliability evaluation of control systems. Proc. of the 2005 American Control Conference; 8–10 June, 2: 1048–1053.

[150] Wang H, Pham H. Reliability and optima maintenance. Springer, London, U.K., 2006.

[151] Lin Yi-Kuei. System reliability of a limited-flow network in multicommodity case. IEEE Trans.on Rel. 2007; March, 56(1):17–25.

[152] Turkkan Noyan, Pham-Gia Thu. System stress-strength reliability: The multivariate case. IEEE Trans. on Rel. 2007; March, 56(1):115–124.

[153] Lin Yi-Kuei. Reliability evaluation for an information network with node failure under cost constraint. IEEE Trans. on Systems, Man and Cybernetics, Part A 2007; 37 (2): 180–188.

[154] Bae Suk Joo, Kang Chang Wook, Choi Jung Sang. Quality and reliability evaluation for nano-scaled devices. IEEE International Conference on Management of Innovation and Technology 2006; June, 2: 798–801.

[155] Crespo Adolfo, Iung Marquez Benoît. A structured approach for the assessment of system availability and reliability using Monte Carlo simulation. J. of Qual. in Maintenance Engg. 2007; 13 (2):125–136.

20

Tampered Failure Rate Load-Sharing Systems: Status and Perspectives

Suprasad V. Amari[1], Krishna B. Misra[2], and Hoang Pham[3]

[1] Relex Software Corporation, USA
[2] RAMS Consultants, Jaipur, India
[3] Department of Industrial Engineering, Rutgers University, USA

Abstract: Load-sharing systems have several practical applications. In load-sharing systems, the event of a component failure will result in a higher load, therefore inducing a higher failure rate, in each of the surviving components. This introduces failure dependency among the load-sharing components, which in turn increases the complexity in analyzing these systems. In this chapter, we first discuss modeling approaches and existing solution methods for analyzing the reliability of load-sharing systems. We then describe tampered failure rate (TFR) load-sharing systems and their properties. Using these properties, we provide efficient solution methods for solving TFR load-sharing models. Because load-sharing *k*-out-of-*n* systems have several practical applications in reliability engineering, we provide a detailed analysis for various cases of these systems. The solution methods proposed in this chapter are applicable for both identical and non-identical component cases. The proposed methods are not restricted to the exponential failure distributions and are applicable for a wide range of failure time distributions of the components. In most cases, we provide closed-form analytical solutions for the reliability of TFR load-sharing *k*-out-of-*n*:G systems. As a special case, efficient solutions are provided for systems with identical components where all surviving components share the load equally. The efficiencies of the proposed methods are demonstrated through several numerical examples.

20.1 Introduction

In reliability engineering, it is a common practice to use redundancy techniques to improve system reliability [1]. In most cases, when analyzing redundancy, independence is assumed across the components within the system. In other words, it is assumed that the failure of a component does not affect the failure properties (failure rates) of the remaining components. In the real-world, however, many systems are load-sharing, where the assumption of independence is no longer valid. In a load-sharing system, if a component fails, the same workload has to be shared by the remaining components, resulting in an increased load shared by each surviving component. In most circumstances, an increased load induces a higher component failure rate [2]. Many empirical studies of mechanical systems [3] and computer systems [4, 5] have proved that the workload strongly

affects the component failure rate. Applications of load-sharing systems include electric generators sharing an electrical load in a power plant, CPUs in a multiprocessor computer system, cables in a suspension bridge, and valves or pumps in a hydraulic system [6]. Therefore, it is important to develop reliability models that incorporate stochastic dependencies among the system's components.

The stochastic dependency models can be broadly classified as shock models and load-sharing models [7, 8]. In shock models, the system is exposed to shocks that cause random amounts of damage [9]. The shocks themselves can occur according to a random process. The intensity and occurrence frequency of the shocks may vary with time. Generally, the occurrences of shocks are modeled using homogeneous or non-homogeneous Poisson processes. The additional damage to the system at a given shock may depend on the intensity of the shock, damage that already experienced, and the age of the system. The system fails when the cumulative damage exceeds a certain level. An example of a shock model is the failure of a dam due to excessive water in the reservoir after several successive rainfalls [10]. Another class of shock models includes common-cause failures. For example, the bivariate shock model introduced by Marshall and Olkin [11] analyzes component dependencies by incorporating latent variables to allow simultaneous component failures. In load-sharing models, the component failure rates depend on the operating status of the other system components and the effective system structure function. In 1945, Daniels [12] adopted the load-sharing model to describe how the strain on yarn fibers increases as individual fibers within a bundle break. For example, a bundle of fibers can be considered as a parallel system subject to a steady tensile load. In this chapter, we concentrate on load-sharing models.

Load-sharing models have a wide range of engineering applications. They are extensively used in the textile engineering (fibers) [12], material science and testing (fatigue and crack growth) [13], mechanical engineering, and civil and structural engineering (welded joint on large support structures) [8] disciplines. Further, load-sharing models have interesting applications in nuclear reactor safety, software reliability [14], distributed computing [15], population sampling [8], combat modeling [16], modeling the incubation period for the human immunodeficiency virus (HIV) [17], and condition-based maintenance [18]. For a summary of these applications, refer to Kvam and Peña [8].

Even though load-sharing systems have been studied for a long time and have a wide range of applications, the methods that are applicable for studying the time-dependent reliability characteristics of these systems are limited. A majority of research papers related to this topic are published in journals on material science, physics, and applied statistics journals. These papers focus on the statistical properties of materials (strength of materials) subjected to load-sharing rules such as equal load-sharing, local load-sharing, monotone load-sharing. The research publications that consider both time-dependent failures (also failure rates) and the dynamic effects of loads are limited [2]. In this chapter, we present existing methods and their useful extensions for analyzing time-dependent reliability characteristics of load-sharing systems. We focus our attention on a specific class of load-sharing models called tampered failure rate (TFR) load-sharing models [19]. Whenever applicable, we also present simplified results for some special cases that include exponential failure distributions and identically distributed components.

Section 20.2 discusses the background and basic concepts in modeling load-sharing systems. Section 20.3 presents a brief overview of static and dynamic methods. It also discusses the related works that are used for analyzing the time-dependent reliability characteristics of load-sharing systems. Section 20.4 presents the system description, assumptions, and details of the tampered failure rate (TFR) models. Section 20.5 presents the reliability analysis of load-sharing k-out-of-n systems with exponential failure distributions, and Section 20.6 focuses on the general failure distributions. Section 20.7 presents the conclusions and future directions of research.

20.2 The Basics of Load-sharing Systems

In order to analyze the reliability of load-sharing systems, we must consider the pattern of loads acting on the system, load-sharing policies that dictate how a load on the system is distributed among its components, and the relationship between the dynamic load and the failure behavior of the components over a time period.

20.2.4 The Load Pattern

In load-sharing systems, the components of the system are subjected to varying loads due to numerous reasons including changing demands of the system, failure of some components, changes in the operating conditions, *etc*. Therefore, the total load on the system can be categorized as:

- Constant total load: In this case, the total load on the system is constant. However, the components experience different loads due to the unavailability of some components as a result of failure or preventive maintenance. The constant total load assumption is applicable for a wide range of applications. The majority of published works are based on this assumption. In this chapter, we also focus on this assumption.
- Time-varying total load: The total load on the system may vary with time. The variation can be deterministic or random. Therefore, the components can experience varying loads due to the variations in the demand. Hence, the load on a component not only changes when other components fail but also when system demands fluctuate.

20.2.4 The Load-sharing Rule

The most important element of the load-sharing model is the rule that governs how the loads on the working components change after some components in the system fail [20].

- Equal load-sharing rule: A constant system load is distributed equally among the working components. Examples of this kind include yarn bundles and untwisted cables that spread the stresses uniformly after individual failures.
- Local load-sharing rule: A load on a failed component is transferred to adjacent components, and the proportion of the load that the surviving components inherit depends on their "distance" to the failed component. Examples of this kind include cables supporting bridges and other structures, composite materials with bounding matrix joins, and transmission systems that are modeled using consecutive *k*-out-of-*n* systems.
- Monotone load-sharing rule: The load on any individual component is non-decreasing as other components fail. This is a generalization to the previous two load-sharing rules. This load-sharing rule is applicable if we are not redistributing any portion of a load from a good component.

The same rules are also applicable for time-varying loading conditions. It should be noted that for the 1-out-of-2 systems subjected to constant total load, all of these load-sharing rules produce the same effects (or coincide).

A generalization to the above load-sharing rules includes the non-monotone load-sharing rule, where the load on working components may increase or decrease depending on the dynamics in the systems. A simple example of this kind includes load on a processor due to the variations in the demand [15]. The non-monotone load-sharing rule may also be applicable (even if the total load on the system is constant) when the components have discrete load-carrying capacities (power generators). Similarly, a modification to the equal load-sharing rule to analyze twisted fiber bundles is proposed in [21].

20.2.3 Load–life Relationship

In order to analyze the reliability of load-sharing systems, we should consider the relationship between the load and the failure behavior of a component. In general, failure rate of a component increases with the applied load. Accelerated life

testing models play an important role in determining the relationships between load and failure rate. There is a wide range of literature available on the accelerated life testing models [22].

20.2.3.1 Proportional Hazards Model (PHM)

PHM was first introduced by Cox [23] and has recently gained popularity in the engineering field [24–26]. PHM assumes that the hazard (failure) rate of a component is the product of both a baseline hazard rate (which can be a function of time t) and a multiplicative factor based on the values of a set of conditions (loads in this case). In PHM, the component failure rate is expressed as:

$$h(t;z) = h_0(t) \cdot \exp(z\beta), \qquad (20.1)$$

where $z = \{z_1, \ldots, z_m\}$ is a set of conditions (loads) acting on the component, and $h_0(t)$ is the baseline failure rate function for the standard set of conditions (at the baseline load). In fact, $\exp(z\beta)$ can be replaced by any known function $g(z,\beta)$. When there is only one type of load, $z = L$, it reduces to:

$$h(t;L) = h_0(t) \cdot \exp(L\beta). \qquad (20.2)$$

If the failure rate of the component at a fixed load is a constant function of time, then we have: $h_0(t) = \lambda_0 = \lambda(L_0)$. Then, we have:

$$\lambda(t;L) = \lambda(L) = \lambda_0 \cdot \exp(L\beta). \qquad (20.3)$$

When the baseline failure distribution is Weibull or exponential, under certain situations, the PHM model is also equivalent to the accelerated failure time model (AFTM) [27].

20.2.3.2 Accelerated Failure Time Model (AFTM)

AFTM was first proposed by Pike [27] and has been widely applied since then [22]. This model specifies that the effect of the load is multiplicative in time. In AFTM, component reliability is expressed as:

$$R(t;z) = R_0(t \cdot \phi(z)). \qquad (20.4)$$

$R_0(.)$ is a survival function of an arbitrary distribution such as Weibull, Gaussian, lognormal, and gamma. Hence, it follows that

$$\begin{aligned} h(t;z) &= \phi(z) \cdot h_0(t \cdot \phi(z)) \\ H(t;z) &= H_0(t \cdot \phi(z)) \end{aligned}. \qquad (20.5)$$

$h_0(.)$ and $H_0(.)$ are the hazard rate and cumulative hazard rate corresponding to the survival function $R_0(.)$. When there is only one type of load, $z = L$, commonly used forms of $\phi(L)$ include:

- The power law: $\phi(L) = L^{\alpha}$.
- The exponential law: $\phi(L) = e^{L\alpha}$.

If the baseline distribution is Weibull (or exponential) and the multiplicative factor (acceleration factor) follows the power law, then AFTM and PHM coincide. However, in general, there is no direct duality between the models in all cases [28].

If the failure distribution is exponential and the multiplicative factor follows the power law, then

$$\lambda(L) = \lambda(L_0)(L / L_0)^{\alpha}. \qquad (20.6)$$

20.2.4 The Effects of Load History on Life

In the previous section, we discussed how the load effects the failure distribution of a component. These models are applicable when a constant, fixed load is acting on a component. However, in load-sharing systems, a component operates at different loads during different time intervals. Therefore, it is important to consider the effects of load history on the component failure rate. Hence, we should also consider other details that are applicable for step-stress acceleration life testing models, where the component experiences different loads at different time intervals. However, unlike in accelerated life testing, in a load-sharing system, the load varies at random time intervals. Hence, analyzing load-sharing systems is much more complex than analyzing fixed duration step-stress acceleration life testing models.

In this section, we present the step-stress accelerated models that describe the failure rate and the remaining life time of the products for a given loading history.

20.2.4.1 The Tampered Failure Rate (TFR) Model

The TFR model was first proposed by Bhattacharrya and Soejoeti [29] and then generalized by Madi [30]. The acceleration of failure when the stress is raised from a lower level to a higher level is reflected in the hazard rate function. The TFR model is relatively simple and has been studied by several researchers [31]. In this model, the failure rate of a component completely depends on the current applied load and the age of the component. In other words, the failure rate is independent of the history of the load applied on the component. However, the cumulative failure rate and reliability of a component is a function of the load history and the ages at which the loads are applied. As pointed out in [32], it should be noted that the Khamis and Higgins model [33] is a special case of the TFR model where the baseline failure distribution is Weibull.

20.2.4.2 The Cumulative Exposure (CE) Model

The cumulative exposure model was proposed by Nelson [34]. It is also called the cumulative damage model [35]. It suggests that, in calculating cumulative failure rate or reliability, the life-stress model must take into account the cumulative effect of the applied stresses when dealing with data from accelerated tests with step stresses. Alternatively, the cumulative failure rate is calculated using the effective age of the component, where the effective age is the sum over all load durations multiplied by the corresponding acceleration factors.

Consider a component that is subjected to the loads $z_1, z_2, \ldots, z_n$ for the durations $\tau_1, \tau_2, \ldots, \tau_n$. Let the acceleration factor corresponding to the load z_i be α_i. The effective age of the component at the baseline failure rate is then: $T_a = \alpha_1\tau_1 + \alpha_2\tau_2 + \ldots + \alpha_n\tau_n$, whereas the actual age is $T = \tau_1 + \tau_2 + \ldots + \tau_n$.

The disadvantage of this model is that the cumulative failure rate or reliability of a component depends only on the duration of the load, but not on the sequence of loads (no sequence effect) or the ages at which the loads are applied. Further, the cumulative damage is additive, and the remaining life of a component depends only on the current stress and the current cumulative distribution function, regardless of the damage accumulation history. Some studies suggest that it is important to consider the effects of load sequencing on the failure behavior [36].

Some variations and generalizations of these models are presented in [37–39]. When the baseline failure distribution is exponential, all these models coincide. In this chapter, we concentrate on the TFR model while studying load-sharing systems subjected to general failure distributions.

20.3 Load-sharing Models

The majority of work on load-sharing models has studied the failure properties of composite materials using the concept of fiber bundles. In these analyses, the failure model of the individual fibers that make up the fiber bundle is specified. The model can be either static or dynamic (or time-dependent). In the static case, the probability of the failure of a fiber is specified in terms of the stress on the fiber [12, 21]. The static models mainly concentrate on the strength distribution of the system (bundle of fibers) in terms of the strength distribution of individual system elements (fibers). These models generally ignore the time-varying properties of materials, *i.e.*, failure is assumed to occur instantaneously. In the dynamic case the statistical distribution of times to failure for the fibers is specified in terms of stresses on the fibers [40]. Experiments generally favor the dynamic failure fiber bundle models [8, 41].

20.3.1 Static Models

Static models generally focus on the influence of fiber strength, bundle length, bundle size, fiber packing, and interface properties. Most of these models assume that components are arranged in parallel (parallel array of fibers) [12]. These studies are also called parallel bundle theories. On the other hand, twisted bundle theories are used to study the twisted mechanical structures such as yarns, ropes, and cables [21].

The earliest work on static models dates back to 1945. In a seminal paper, Daniels [12] showed through a long and complicated proof that when

the load from fiber breaks is redistributed equally among the remaining intact fibers (equal load sharing), the strength of a large bundle asymptotically approaches a Gaussian distribution. Daniels derived expressions for the asymptotic mean and standard deviation as a function of the underlying strength distribution of the fibers and bundle size in terms of number of fibers. Here, the asymptotic value for mean is independent of n. Smith [42] derived a correction factor for mean that depends on n to improve the accuracy for relatively small bundles. For a discussion of load-sharing schemes, we refer to Harlow and Phoenix [20]. For a recent review on parallel bundle theories, we refer the reader to Phoenix and Beyerlein [43].

20.3.2 Time-dependent Models

Time-dependent analysis can broadly be classified as: (1) finite population analysis, and (2) asymptotic analysis. In this chapter, we concentrate on finite population analysis where the number of elements in the system is finite. Analyses for finite populations are published in the reliability journals [2, 44]. On the other hand, the asymptotic behavior (limiting behavior) is studied by assuming the number of elements in the system approaches infinity (are very large). These studies are published in physics, material science, and applied statistics journals [40, 42–54]. Coleman [45, 46] has shown that under certain conditions, as the number of fibers increases, the asymptotic failure time of the bundle approaches the normal distribution. Similarly, using extreme value theory, Harlow *et al*., [53–55] have shown that the time to failure of a parallel bundle follows the Weibull distribution. However, as pointed out by Borges [55], even for the case of exponential failure time distributions, this approximation is unsuitable from the application standpoint because for each fixed value of t (time), the deviation from its true value increases as n (number of elements) increases. In addition to this, using the large deviation theorem of the Cramer–Petrov type and a ranking limit theorem of Loève [56], Borges proposed a better approximation for failure time distribution. These results are further extended for series-parallel systems [55]. Recently, Newman and Phoenix [57], assuming exponential failure time distribution and a power law relationship between failure rate and applied load, developed asymptotic theories and new computational algorithms for local load-sharing models.

20.3.3 Related Models

In this chapter, we focus on the reliability analysis of load-sharing systems with a limited number of components. These models have a wide range of applications in reliability engineering [1–6, 58–61]. Most approximations and asympotic behaviors that are applicable for systems with a large number of elements (fiber bundles) are not applicable when the number of components (elements) in the system is very small. Therefore, these models require a different treatment as compared to fiber bundle models. In addition, it is important to consider the effects of time-varying failure rates, imperfect switching mechanisms, repair policies, *etc*.

In spite of a wide range of applications for load-sharing systems, the literature on the reliability analysis of load-sharing systems is limited [2]. The main reason for this is due to the inherent complexity of these models that is introduced by the load-sharing mechanisms.

As we have already noted, load-sharing systems introduce dependecies among component lives. Bivariate and multivariate distribution play important roles in modeling these dependencies. However, only a certain class of multivariate distributions is applicable for load-sharing systems [7]. Freund [62] first introduced a bivariate exponential distribution to model a two-unit load-sharing system.

20.3.3.1 Freund's Load-sharing Model

Freund's model is the first bivariate model that is physically motivated [7, 62]. Let X and Y represent the lifetimes of components *C1* and *C2* of a two-component system. Further, assume $X \sim \exp(\lambda_1)$ and $Y \sim \exp(\lambda_2)$. According to the Freund's model, the failure rate of *C2* changes to λ'_2 from λ_2 ($\lambda'_2 > \lambda_2$), upon the failure event of component *C1*

because of extra stress. Similarly, λ_1 changes to λ'_1 in the case where component *C2* fails first, ($\lambda'_1 > \lambda_1$), due to the same reason. Assuming that $\lambda_1 + \lambda_2 - \lambda'_1 \neq 0$ and $\lambda_1 + \lambda_2 - \lambda'_2 \neq 0$, the joint density of (X, Y) is:

$$f(x,y) = \begin{cases} \lambda_1 \lambda'_2 \exp[-\lambda'_2 y - (\lambda_1 + \lambda_2 - \lambda'_2)x], \\ \text{if } 0 < x < y \\ \\ \lambda'_1 \lambda_2 \exp[-\lambda'_1 x - (\lambda_1 + \lambda_2 - \lambda'_1)y], \\ \text{if } 0 < y < x \end{cases} \tag{20.7}$$

It should be noted that the marginal distributions of X and Y are not exponential distributions except for the special cases: $\lambda'_1 = \lambda_1$ and $\lambda'_2 = \lambda_2$. However, the marginal distributions can be shown to be mixtures or weighted averages of exponential distributions [7].

If the system functions as long as one out of two components are functioning, the system failure time is equal to $T = \max(x, y)$. Integrating the density function over the region $t < T$ gives the unreliability of the system. Therefore, the system unreliability is:

$$Q(t) = \frac{\lambda_1}{\lambda_1 + \lambda_2}\left(1 + \frac{\lambda'_2 \cdot e^{-(\lambda_1+\lambda_2)t} - (\lambda_1 + \lambda_2)\cdot e^{-\lambda'_2 t}}{\lambda_1 + \lambda_2 - \lambda'_2}\right) + \frac{\lambda_2}{\lambda_1 + \lambda_2}\left(1 + \frac{\lambda'_1 \cdot e^{-(\lambda_1+\lambda_2)t} - (\lambda_1 + \lambda_2)\cdot e^{-\lambda'_2 t}}{\lambda_1 + \lambda_2 - \lambda'_1}\right) \tag{20.8}$$

Therefore, the system reliability is:

$$R(t) = \frac{\lambda_1}{\lambda_1 + \lambda_2}\left(\frac{(\lambda_1 + \lambda_2)\cdot e^{-\lambda'_2 t} - \lambda'_2 \cdot e^{-(\lambda_1+\lambda_2)t}}{\lambda_1 + \lambda_2 - \lambda'_2}\right) + \frac{\lambda_2}{\lambda_1 + \lambda_2}\left(\frac{(\lambda_1 + \lambda_2)\cdot e^{-\lambda'_2 t} - \lambda'_1 \cdot e^{-(\lambda_1+\lambda_2)t}}{\lambda_1 + \lambda_2 - \lambda'_1}\right) \tag{20.9}$$

The reliability expression can be rearranged as:

$$R(t) = e^{-(\lambda_1+\lambda_2)t}\left(1 - \frac{\lambda_1}{\lambda_1 + \lambda_2 - \lambda'_2} - \frac{\lambda_2}{\lambda_1 + \lambda_2 - \lambda'_1}\right) + \frac{\lambda_1}{\lambda_1 + \lambda_2 - \lambda'_2} e^{-\lambda'_2 t} + \frac{\lambda_2}{\lambda_1 + \lambda_2 - \lambda'_1} e^{-\lambda'_1 t} \tag{20.10}$$

The above system behavior can be modeled using a four-state Markov chain, and the closed-form solution can be obtained using either convolution integrals or Laplace transformations [63, 64]. The above model is applicable for all types of load-sharing rules: equal, local, or monotone load-sharing rules. In fact, this model is independent of the load-sharing rule.

Now assume that $\lambda_1 \neq \lambda_2$, but $\lambda'_1 = \lambda'_2 = \lambda'$. This assumption is valid if both the components are identical and load is distributed unequally when both components are working. However, after a failure, the surviving component carries the full load. Hence, we have:

$$R(t) = e^{-(\lambda_1+\lambda_2)t} + \frac{\lambda_1 + \lambda_2}{\lambda_1 + \lambda_2 - \lambda'}\left(e^{-(\lambda_1+\lambda_2)t} - e^{-\lambda' t}\right) . \tag{20.11}$$

If the two components are equal and the load is distributed equally among these two components, we have: $\lambda_1 = \lambda_2 = \lambda$, and $\lambda'_1 = \lambda'_2 = \lambda'$. Hence, we have:

$$R(t) = e^{-2\lambda t} + \frac{2\lambda}{2\lambda - \lambda'}\left(e^{-2\lambda t} - e^{-\lambda' t}\right) . \tag{20.12}$$

Only a few reliability engineering textbooks that discuss the load-sharing systems cover more than this simple model [1, 6, 59].

Freund's model can be viewed as a simple load-sharing model for a system with two components. As noted above, Freund did not consider the underlying load-sharing rules that dictate how failure rates change after some components in the system fail. Weier [66] was the first to actually analyze the reparametrization of Freund's model. He modeled the post failure hazard rate θ_2 by $\gamma\theta_1$, $\gamma > 0$. Here $\gamma = 1$ implies independence, and $\gamma > 1$ corresponds to an increased work load on the remaining component, while $\gamma < 1$ corresponds to a reduced work load. This parameterization allows researchers to extend the Freund's model for general cases, such as *k*-out-of-*n* systems, and make general statistical inferences on the details of possible dependencies among components in a system [7] .

20.3.3.2 The k-out-of-n System with IID Components

Scheuer [44] studied the reliability of a *k*-out-of-*n*:G system where component failure induces higher failure rates in the survivors. His work assumed that the components are IID with constant failure rates. Although it is not mentioned explicitly, the model inherently assumes the equal load-sharing rule. Scheuer modeled the system failure time as the sum of independent exponential distributions. He identified three cases.

- *Case 1* arises when all these exponential distributions are identical. In this case, the system failure follows the Erlang distribution (a special case of the Gamma distribution).
- *Case 2* arises when all these exponential distributions are distinct. In this case, the system failure time follows the hypo-exponential distribution.
- *Case 3* arises when all these exponential distributions are neither equal nor distinct. This happens when distinct groups of distributions exist. Within each of these groups, all of the distributions are equal. In this case, the system failure time is the sum of Erlangian distributions with different parameters. Scheuer [44] mentioned that there is no convenient closed-form solution for this case. However, recently Amari and Misra [65] provided a closed-form solution to this case. This case has a wide range of applications not only in reliability engineering but also in other fields such as control systems and telecommunications [67, 68].

20.3.3.3 The k-out-of-n System with Repair

Shao and Lamberson [69] provide an analysis of a repairable *k*-out-of-*n*:G system with load-sharing components considering imperfect switching. In this model, all components in the systems are identical and follow exponential failure distributions. As in most cases, it also assumes the equal-load sharing rule. The sensing and switching mechanism is responsible for detection of component failures and the redistribution of the load of the system equally among surviving components. System performance measures such as reliability and availability are analyzed using Markov chains. Unfortunately, several errors exist in the above paper, which are corrected by Akhtar [70]. Newton [71] provides an alternative argument for evaluation of the MTTF and MTBF of such systems. A corrected version of this model is presented in [72]. However, [72] did not provide a complete solution to this model, but provided the differential equations for solving the Markov chains. Recently, Chan [73] discussed availability analysis of a load-sharing system and advocated the combining of performance and reliability analyses within the Markov reward framework.

20.3.3.4 Multivariate Exponential Models

Lin *et al*., [74] extended Freund's bivariate exponential model to the multivariate exponential case. In this model, the system consists of *n* non-identical components. The failure rate of a component depends on the number of failed components, but it is independent of the actual set of components that are failed. For example, when there is only one failed component in the system, the failure rate of component 1 is the same, regardless whether component 2 or component 3 failed. This assumption is applicable for the equal load-sharing rule, where the load on a surviving component is a function of the number of failed components. Even with this assumption, the failure time distribution of a 1-out-of-3 system is too complex, and the equation for the system reliability occupies almost two full columns of that paper. Lin *et al*. [74] also presented a closed-form solution for *k*-out-of-*n* systems with IID components following exponential failure distributions. However, this is equivalent to Case 2 studied by Scheuer [44], where the closed-form solution is well known. Later, Amari [64] provided a compact closed-form solution to *k*-out-of-*n* systems with non-identical components.

20.3.3.5 General Failure Distributions

There is not much published work on the reliability analysis of load-sharing systems with components

subjected to general failure distributions. Even though there are some papers, they do not explicitly mention the underlying assumptions. In modeling load-sharing systems with general distributions, it is important to consider an appropriate model to incorporate the effects of loading history. For details, the reader is referred to Section 20.2.4.

Several researchers have extended Freund's bivariate exponential model to other cases that include the case of non-exponential distributions such as Weibull and gamma [75, 76]. However, only a few of these extensions are useful for modeling load-sharing systems. Lu [76] proposed a bivariate Weibull distribution that can be applied to load-sharing systems. In this model, the failure distribution (parameters) of the surviving component changes after load redistribution due to the failure of other component. However, in this model, it is assumed that the effective age of the component becomes zero after the load redistribution, which is not a realistic assumption.

Kececioglu and Jiang [77] presented a 1-out-of-2 load-sharing system with Weibull failure time distributions. In this analysis, it is assumed that after load redistribution, the component age changes according to an accelerated failure-time model (AFTM) as *per* the cumulative exposure model. This model is also available in [59]. Later Liu *et al*. [26, 78, 79] proposed similar concepts for analyzing 1-out-of-2 parallel systems subjected to variable working conditions. Liu [2] further extended this model for analyzing load-sharing *k*-out-of-*n*:G systems with arbitrary load-dependent component lifetime distributions. However, the solution provided in [2] is too complex. Therefore, as mentioned in [2, 6], the solution can only be applied for simple systems where $n \leq 6$ (even using MatLab). Therefore, more efficient methods for handling arbitrary load-dependent component lifetime distributions are needed.

Recently, Amari *et al*. [19] provided a closed-form analytical solution for the reliability of tampered failure rate (TFR) load-sharing *k*-out-of-*n*:G systems with identical components where all surviving components share the load equally. This model can be considered as a generalization of the 1-out-of-2 load-sharing model presented by Hassett [80], where the solution is provided using a numerical integration technique applicable for semi-Markov chains [81].

20.4 System Description

In this chapter, we provide a detailed treatment of TFR load-sharing systems subjected to exponential and general failure time distributions. Because *k*-out-of-*n* systems have a wide range of applications in reliability engineering, a detailed analysis of these systems is presented in this chapter. The concepts presented here can easily be extended to analyze general system configurations. In this chapter, we also would like to relax the IID assumption used in [19].

General Assumptions

1. After a component failure, the load is equally distributed among all surviving components. This assumption will be relaxed in some cases.
2. The failure rate of a component varies as *per* the TFR model. The baseline failure rate of the TFR model can follow an arbitrary distribution such as Weibull, Gaussian, lognormal, and gamma.
3. The redistribution and reconfiguration mechanisms are perfect.
4. The system and its components are non-repairable.

20.4.1 Load Distribution

In a load-sharing system, on component failure, the load on the failed component is redistributed among the surviving components. In the majority of cases, the load is equally distributed over all surviving components. If the total load is L, and there are m good components, then the load on each component is $z = L/m$.

Let n be the total number of components in the system and z_i be the load on each of the surviving components when i components are failed. Hence,

$$z_0 = L/n; \quad z_i = L/(n-i) = z_0 \cdot \frac{n}{n-i}. \quad (20.13)$$

20.4.2 The TFR Model

In the TFR model, the acceleration of failure when the stress is raised from a lower level to a higher level is reflected in the hazard rate function. In this section, we describe this model in terms of *k*-out-of-*n* systems. Consider a component that is subjected to an ordered sequence of loads, where load z_i ($i = 0,1,\ldots, n-k$) is applied during the time interval $[\tau_i, \tau_{i+1}]$, where $\tau_0 = 0$. In other words, the load changes at times $\tau_1, \tau_2, \ldots, \tau_{n-k}$. According to the TFR model, the hazard rate of the component at time t is:

$$h(t) = h_i(t) = \delta_i \cdot h_0(t) \quad \text{for} \quad \tau_{i-1} \le t < \tau_i \ , \quad (20.14)$$

where $\delta_0 = 1$, $h_0(t)$ is the hazard rate at the lower load z_0, and δ_i is the tampered factor at load level z_i. The tampered factor is a function of the applied stress. Hence, the TFR model can be expressed as:

$$h(t) = \delta(z) \cdot h_0(t), \quad (20.15)$$

where z is the load at time t.

20.4.3 System Configuration

In this chapter, we considered a *k*-out-of-*n* structure, which is a common form of redundancy used in reliability engineering. A system is called called a *k*-out-of-*n* system if at least k out of n components must work for the successful operation of the system [1, 6]. The *k*-out-of-*n*:G structure redundancy finds wide applications in both industrial and military systems. Several examples of *k*-out-of-*n*:G systems are available [1, 6]. Both series systems and parallel systems are special cases of the *k*-out-of-*n* system.

20.5 *k*-out-of-*n* Systems with Identical Components

In this section, we discuss the load-sharing *k*-out-of-*n* systems with identical components. The additional assumptions are:

- There are n IID components in the system.
- The system functions successfully if and only if there are at least k good components.

20.5.1 Exponential Distributions

When the system is put into operation at time zero, all components are working, and they are equally sharing the constant load that the system is supposed to carry. In this case, the failure rate of every component is denoted by λ_0. Because there are n working components in the system, the first failure occurs at rate $\alpha_1 = n.\lambda_0$. When the system experiences the first failure, the remaining $(n-1)$ working components must carry the same load on the system. As a result, the failure rate of each working component becomes λ_1, which is typically higher than λ_0. The second failure occurs at rate $\alpha_2 = (n-1).\lambda_1$. When i components are failed, the failure rate of each of the $(n-i-1)$ working components is represented by λ_i $(0 \le i \le n-k)$. The i_{th} failure occurs at rate $\alpha_i = (n-i+1).\lambda_{i-1}$. The system is failed when more than $(n-k)$ components are failed.

Because all components are IID following the exponential distributions, the inter-arrival times of failures are independent random variables X_i, where X_i follows the exponential distribution with parameter α_i for $1 \le i \le n-k+1$. Hence, the lifetime of the system is equal to the $(n-k+1)$-st failure time. Alternatively, the lifetime of the system is equal to the sum of $(n-k+1)$ independent random variables following exponential distributions with possibly different parameters (rates).

$$\begin{aligned} T &= X_1 + X_2 + \ldots + X_{n-k+1} \\ \text{Hence} \quad R(t) &= \Pr\{T \le t\} \end{aligned} \quad . \quad (20.16)$$

To find the distribution of T and the reliability function of the system, we need to distinguish the following three cases.

Case 1: All α_i are equal (say α) [44].

$$\begin{aligned} R(t) &= \sum_{i=0}^{n-k} \frac{(\alpha t)^i \exp(-\alpha t)}{i!} \\ &= gamfc(\alpha t; n-k+1) \end{aligned} \quad (20.17)$$

where *gamfc*() is the complimentary cumulative distribution of the gamma distribution. This case arises when the failure rate of each surviving

component is directly proportional to the load it carries. Hence, in the TFR model, $\delta(z) \propto z$.

Case 2: All α_I are distinct [44].

$$\begin{aligned} R(t) &= \sum_{i=1}^{n-k+1} A_i \cdot \exp(-\alpha_i t) \\ A_i &= \prod_{j=1; j\neq i}^{n-k+1} \frac{\alpha_j}{\alpha_i + \alpha_j} \end{aligned} \tag{20.18}$$

Case 3: α_I are neither equal nor distinct. Specifically, assume that these α_I take a ($1 < a < n-k+1$) distinct values, β_1, β_2, …, β_a. With possibly some renumbering of these α_i values, assume:

$$\begin{aligned} \alpha_1 = \cdots = \alpha_{r_1} &= \beta_1 \\ \alpha_{r_1+1} = \cdots = \alpha_{r_2+r_2} &= \beta_2 \\ \vdots & \\ \alpha_{r_2+r_2+\cdots+r_{a-1}+1} = \cdots = \alpha_{r_2+r_2+\cdots+r_a} &= \beta_a \end{aligned} \tag{20.19}$$

where the assumptions are:

- $a \geq 1$ and an integer.
- All β_{li} are distinct.
- The sum of r_I is equal to n.
- Each $r_i \geq 1$ and an integer.

Hence, $T = V1 + V_2 + ... + V_a$. V_i is a random variable, which follows the Erlangian distribution. The shape parameter is r_i, and the scale parameter is β_i. From [44], we have:

$$R(t) = B\sum_{j=1}^{a}\sum_{l=1}^{r_j} \frac{\Phi_{jl}(-\beta_j)}{(l-1)!(\beta_j)^{r_j-l+1}} .\text{poif}\,(r_j\text{-}l;\beta_j \cdot t)$$

where

$$\begin{aligned} B &= \prod_{j=1}^{a} (\beta_j)^{r_j} \\ \Phi_{jl}(t) &= D^{l-1}\left(\prod_{i=1; i\neq j}^{a} (\beta_i + t)^{-r_i} \right) \\ \text{poif}\,(r_j - 1; \beta_j \cdot t) &\equiv \sum_{i=0}^{r_j-l} \frac{\exp(-\beta_j t)(\beta_j t)^i}{i!} \end{aligned} \tag{20.20}$$

Scheuer [44] mentioned that there seems to be no closed-form expression for $\Phi_{jl}(t)$. Using a multi-function generalization of the Leibnitz rule, Amari and Misra [65] provided a closed-form solution for $\Phi_{jl}(t)$, which in turn completes the closed-form solution for $R(t)$.

$$\begin{aligned} \Phi_{jl}(t) &= (-1)^l (l-1)! \sum_{\Omega} \prod_{i=1; i\neq j}^{a} \nu(i, m_i, t) \\ \nu(i, m_i, t) &= \binom{r_i + m_i - 1}{m_i} (\beta_j + t)^{-(r_i + m_i)} \\ \Omega &\equiv m_1 + \cdots + m_a = l - 1; \text{ where } m_j = 0; m_{i\neq j} \geq 0 \end{aligned} \tag{20.21}$$

Case 3 arises when $\delta(z)$ in the TFR model is either a piece-wise linear function or an *S*-shared increasing function. Case 3 is also applicable when there are some additional spares in standby. In such cases, the load on the surviving components remains the same until the exhaustion of the standby spares. Hence, the values of some α_I will be the same.

20.5.2 General Distributions

In this section, we show that solving TFR models with arbitrary baseline failure distributions is equivalent to solving TFR models with exponential distributions. The basic idea is that using a time-transformation, a TFR model with an arbitrary baseline distribution can be converted into an equivalent problem with an exponential baseline distribution. This in turn reduces the problem under consideration to a simplified problem: the problem of a *k*-out-of-*n*:G load-sharing system with exponential distributions.

Lemma 1: For any failure distribution $F(t)$:

1. The reliability function is $R(t) = 1 - F(t)$.
2. The cumulative hazard function is $H(t) = \ln[R(t)]$.
3. The function $H(t)$ is a non-decreasing function in t.
4. The random variable $y = H(t)$ follows an exponential distribution with a mean of 1.
5. For any constant "a", the random variable $y = a.H(t)$ follows an exponential distribution with a mean of "$1/a$" and a failure rate of "a".

Proof: Points 1–3 are straightforward, basic reliability engineering concepts. Because $R(t) = e^{-y}$, points 4−5 can easily be proved using transformation of variables (see [1]).

Lemma 2: For a TFR model with a standard exponential (mean = rate = 1) baseline failure time distribution:

$$\begin{aligned} h(t) &= \delta_i \\ H(t) &= H(\tau_{i-1}) + \delta(t - \tau_{i-1}) \\ &\text{for} \quad \tau_{i-1} \le t < \tau_i \end{aligned} \qquad (20.22)$$

Proof: Straightforward from (20.15).

Lemma 3: For a TFR model with a baseline failure rate of $h_0(t)$ and a baseline cumulative failure rate of $H_0(t)$:

1. Under the regular scale t:

$$\begin{aligned} h(t) &= \delta_i \cdot h_0(t) \\ H(t) &= H(\tau_{i-1}) + \delta_i \cdot [H_0(t) - H_0(\tau_{i-1})] \\ &\text{for} \quad \tau_{i-1} \le t < \tau_i \end{aligned} \qquad (20.23)$$

2. Under the transformed scale $y \equiv H_0(t)$:

$$\begin{aligned} &\text{Let} \quad \nu_i = H_0(\tau_i) \\ h_y(y) &= \delta_i \\ H_y(y) &= H_y(\nu_{i-1}) + \delta_i \cdot [y - \nu_{i-1}] \\ &\text{for} \quad \nu_{i-1} \le y < \nu_i \end{aligned} \qquad (20.24)$$

where $H_y(y)$ is the cumulative hazard rate in the transformed scale.

Proof: Point 1 is straightforward from the definition of cumulative hazard rate and the $h(t)$ in (20.15). Because $t = H_0^{-1}(y)$ and $H_0(t) = y$, point 2 follows from point 1.

Theorem 1: If the effects of load variations on the hazard rate of an individual component follow a TFR model with $h(t) = \delta_i.h_0(t)$, the reliability of a load-sharing system at time t is equivalent to the reliability of the corresponding exponential load-sharing model at time $y = H_0(t)$, where the failure rate of a component when i components failed is $\lambda_i = \delta_i$ for $i = 0,\ldots, (n-k)$.

Proof: There is a one-to-one relationship between reliability and cumulative failure rate. For example, if the cumulative failure rates of two components at two different time points are equal, then their reliabilities are also equal at those points. Mathematically, if $H_1(t_1) = H_2(t_2)$, then $R_1(t_1) = R_2(t_2)$. From Lemma 2 and Lemma 3, $H_y(y) = H(t)$, where $Hy(y)$ is the cumulative failure rate of a component with an arbitrary baseline failure rate in the transformed scale y, and $H(t)$ is the cumulative failure rate of a component with a constant baseline failure rate (rate = 1) in the regular scale. Therefore, under the transformed scale, all TFR models are equivalent to their corresponding constant failure rate models. Hence, under the transformed scale, the reliability of a load-sharing system can be calculated using $\lambda_i = \delta_i$, where λ_i is the failure rate of a component when i components are failed.

As long as the baseline failure rate in the TFR model is the same, theorem 1 is also applicable for non-identical component cases where δ_i are different for the non-identical components. It should be noted that the results of Theorem 1 are not restricted to k-out-of-n:G systems. However, in this chapter, we apply these results for solving k-out-of-n:G systems.

20.5.3 Examples

Example 1: Consider a 5-out-of-10:G system with Weibull as the baseline failure distribution.

$$\text{Model}: \quad k = 5; \quad n = 10; \quad t = 1000$$

$$\text{Baseline}: \quad h_0(t) = \frac{\beta}{\eta} \cdot \left(\frac{t}{\eta}\right)^{\beta-1}; \quad H_0(t) = \left(\frac{t}{\eta}\right)^{\beta}$$

$$R_0(t) = \exp[-H_0(t)] = \exp\left[-\left(\frac{t}{\eta}\right)^{\beta}\right]$$

$$\text{Baseline Parameters}: \quad \eta = 2000; \quad \beta = 2$$

$$\text{TFR}: \quad h(t) = \delta(z) \cdot h_0(t)$$

$$\delta(z) = z^{1.5} \Rightarrow \delta_i = \delta(z_i) = \left(\frac{n}{n-i}\right)^{1.5}$$

Solution : $y = H_0(t) = 0.25; \quad \lambda_i = \delta_i$

$$\alpha_i = (n-i)\cdot\lambda_i = 31.623(n-i)^{-0.5}$$

Hence : $\alpha_1 = 10; \quad \alpha_2 = 10.541; \quad \alpha_1 = 11.18;$

$\alpha_4 = 11.952; \quad \alpha_5 = 12.91; \quad \alpha_6 = 14.142$

Here all α_i are distinct. Hence, from (20.18), $R_y(0.25) = 0.92415 \Rightarrow R(t = 1000) = 0.92415$.

Example 2: Same as example 1, except: $\delta(z) = z$.

Solution : $\delta(z) = z \Rightarrow \alpha_1 = \cdots = \alpha_6 = \alpha = 10$

Here all α_i are equal. Hence, from (20.17), $R_y(0.25) = 0.95798 \Rightarrow R(t = 1000) = 0.95798$.

Example 3: Same as example 1, except: $\delta(z)$ is piece-wise linear in z.

$$\text{TFR}: \quad \delta(z) = \begin{cases} z & : \quad z < 1.2 \\ 1.1z & : \quad 1.2 \le z < 1.5 \\ 1.2z & : \quad z \ge 1.5 \end{cases}$$

Solution : $\alpha_1 = \alpha_2 = 10; \alpha_3 = \alpha_4 = 11; \alpha_5 = \alpha_6 = 12$

Here α_i are neither equal nor distinct. Hence, from (20.20) and (20.21), $R_y(0.25) = 0.94005 \Rightarrow R(t = 1000) = 0.94005$.

Example 4: Same as example 2: $\delta(z) = z$. Additionally, it has two spares in standby, which are used to replace the first two failed components. The failure rate of a spare in standby is:

In Standby : $h(t) = \gamma \cdot h_0(t)$; where $\gamma = 0.5$

Solution : $\alpha_1 = 11, \alpha_2 = 10.5; \alpha_3 = \cdots = \alpha_8 = 10$

Here α_i are neither equal nor distinct. Hence, from (20.20) and (20.21), $R_y(0.25) = 0.98433 \Rightarrow R(t = 1000) = 0.98433$.

Example 5: Same as example 4, except the spare are in cold standby where the failure rate is zero, and $\delta(z) = z^{1.5}$.

Solution : $\alpha_1 = \alpha_2 = \alpha_3 = 10; \alpha_4 = 10.541;$

$\alpha_5 = 11.18; \alpha_6 = 11.952; \alpha_7 = 12.91; \alpha_8 = 14.14$

Here α_i are neither equal nor distinct. Hence, from (20.20, 20.21), $R_y(0.25) = 0.97874 \Rightarrow R(t = 1000) = 0.97874$.

20.6 *k*-out-of-*n* Systems with Non-identical Components

In this section, we consider a *k*-out-of-*n* system with non-identical components. We first discuss the exponential distribution case that is considered by Lin *et al*. [74] and later extend this model to the general failure distribution case.

20.6.1 Exponential Distributions

In this model, the system consists of n non-identical components. The failure rate of component i when there are j failures in the system is $\lambda(i,j)$. Because the system reaches a failed state when there are $n-k+1$ failed components, we need to consider the j values in the region: $0 \le j \le n-k$. The existing analysis for this model is too complex even for the 1-out-of-3 systems. In this section, we provide a different approach for solving these systems.

One approach to solve this problem is automatic generation of Markov chains. In this approach, as in dynamic fault tree analysis [82, 83], we generate Markov chain that describe the system behavior and solve the Markov chain using numerical integration methods. The number of states generated is:

$$N = \sum_{i=0}^{n-k+1} \binom{n}{i} \qquad (20.25)$$

If we merge all failed states into one single state, then we have:

$$N = 1 + \sum_{i=0}^{n-k} \binom{n}{i} \qquad (20.26)$$

The number of states increases with both n and $n-k$. For a parallel system, the number of states is equal to 2^n. It should be noted that if the failure rate is dependent on both the number of component failures and the actual set of failed components, then the number of states increases drastically. In the later case, because a failed state with k component failures can be reached in $k!$ ways, a parallel system with 10 components can have as many as 9,864,101 states [83]. The existing Markov chain solvers can handle a maximum of 100,000 states. Hence, $2^n \le 100{,}000$. Therefore, n should be less than or equal to 16. There are

several approaches to improve the efficiency of the computation. They include: (1) eliminating the states that contribute an insignificant portion of probability to the failure, (2) solving the Markov chains while generating the states, and (3) utilizing the bounds. Obviously, another alternative is to use simulation methodology. However, in all these methods, we can only have numerical solutions.

In some cases, we may be interested in the closed-form analytical solutions. We use a method proposed in [64] to obtain the closed-form solutions to this problem. The method is demonstrated using a 2-out-of-3 load-sharing system. In this method, we first generate all sequences of component failures that lead to the system failure. The sequences are mutually exclusive. In this case, we have 6 failure sequences. They are: {1, 2}, {1,3}, {2,1}, {2,3}, {3,1} and {3,2}. The overall system failure probability is the sum of the probability of each failure sequence. The Markov model for this sequence is shown in Figure 20.1. The labels in the Markov chain explain the properties of the states and transitions.

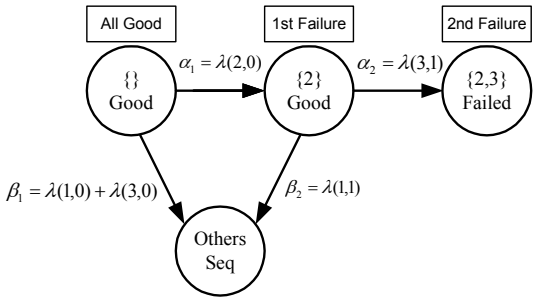


Figure 20.1. Markov chain for sequence {2,3}

The Laplace transform for the failed state is:

$$F(s) = \frac{\alpha_1\alpha_2}{s(s+\alpha_1+\beta_1)(s+\alpha_2+\beta_2)} \quad (20.27)$$

Using [65], the time-dependent failure probability contribution of sequence {2, 3} is:

$$F(t) = A_0 + A_1\exp(-\gamma_1 t) + A_2\exp(-\gamma_2 t) \quad (20.28)$$

where

$$\gamma_i = \alpha_i + \beta_i$$
$$A_0 = \prod_{i=1}^{2}\frac{\alpha_i}{\gamma_i} \quad (20.29)$$
$$A_{j\neq 0} = -\frac{\alpha_j}{\gamma_j}\prod_{i=1;i\neq j}^{2}\frac{\alpha_i}{\gamma_i-\gamma_j}$$

where $n-k+1 = 2$. For the general case, we can replace the *2* with $n-k+1$.

20.6.2 General Distributions

In this model, the system consists of n non-identical components. The failure rate of component i at time t when there are j failed components in the system is $h(i,j,t)$. In addition to this, we also assume that the baseline failure rate of all these components is the same. (or failure rates/are) Hence, we have:

$$h(i,j,t) = \lambda(i,j)\cdot h_0(t) \quad (20.30)$$

Therefore, extending the concepts used for the indentical component case, we can compute the system reliability with general failure distributions using the solutions that are applicable for the exponential failure distributions.

Theorem 2: If the effects of load variations on the hazard rate of an individual component follow a TFR model with $h(i,j,t) = \lambda(i,j).h_0(t)$, the reliability of a load-sharing system at time t is equivalent to the reliability of the corresponding exponential load-sharing model at time $y = H_0(t)$, where the failure rate of a component i when j components are failed is $\lambda(i,j)$.

Proof: This is similar to the proof of *Theorem 1*.

20.6.3 Further Examples

Example 6: Consider a 2-out-of-3:G system with Weibull as the baseline failure distribution.

$$\text{Model}: \quad k=2; \quad n=3; \quad t=1000$$

$$\text{Baseline}: \quad h_0(t) = \frac{\beta}{\eta}\cdot\left(\frac{t}{\eta}\right)^{\beta-1}; \quad H_0(t) = \left(\frac{t}{\eta}\right)^{\beta}$$

$$R_0(t) = \exp\left[-H_0(t)\right] = \exp\left[-\left(\frac{t}{\eta}\right)^{\beta}\right]$$

Baseline Parameters : $\eta = 2000; \quad \beta = 2$

TFR : $h(i, j, t) = \lambda(i, j) \cdot h_0(t)$

$$\lambda(i, j) = \delta_i(z_j)$$

$$z_j = \frac{n}{n-i} \cdot z_0 = \frac{n}{n-i} \text{ (where } z_0 = 1)$$

Hence:

$$\delta_i(z_j) = a_i \cdot (z_i)^{b_i} \Rightarrow \lambda(i, j) = a_i \cdot \left(\frac{n}{n-i}\right)^{b_i}$$

$$a_1 = 1; \quad a_2 = 1.2; \quad a_3 = 1.3;$$

$$b_1 = 1; \quad b_2 = 1.1; \quad b_3 = 1.2;$$

Hence:

$$\lambda(1,0) = 1.0; \quad \lambda(2,0) = 1.2 \quad \lambda(3,0) = 1.3;$$

$$\lambda(1,1) = 1.5; \quad \lambda(2,1) = 1.875 \quad \lambda(3,1) = 2.115;$$

Solution : $y = H_0(t) = 0.25;$

Sequence probabilities at y = 0.25 are:

$$F(1,2) = 0.032195; \quad F(1,3) = 0.036321$$

$$F(2,1) = 0.031808; \quad F(2,3) = 0.044842$$

$$F(3,1) = 0.035101; \quad F(3,2) = 0.043865$$

Hence, the overall failure probability is 0.224131. Therefore, from Theorem 2, $R_y(0.25) = 0.775869$ $\Rightarrow R(t = 1000) = 0.775869$.

It should be noted that as long as the baseline failure rate is the same, this procedure can also be used to compute the reliability of non-equal load-sharing rules.

20.7 Conclusions

In this chapter, various concepts that are important in the modeling and analysis of load-sharing systems, have been presented along with a state-of-the-art review on existing modeling techniques and solution methods. Although load-sharing systems have a wide range of applications, due to the inherent complexity of these systems, the methods available for analyzing these systems are limited.

The existing literature covers only a small portion of these systems that include exponential failure time distributions, equal load-sharing rules, and identically distributed components. Therefore, in order to widen the state-of-the-art, we have proposed efficient methods for computing the reliability of load-sharing *k*-out-of-*n*:G systems with identical and non-identical components where all surviving components share the load equally. The method can be applied for a wide range of failure time distributions including Weibull, lognormal, and gamma distributions. As long as the baseline failure time distribution of all components are the same, the solution proposed in this chapter is also applicable for unequal load-sharing rules. It may be observed here that all TFR models including non-identical baseline failure rate cases can also be solved using semi-Markov chains [64, 80]. However, due to the well-known state space explosion of the Markov chains, the semi-Markov solution approach cannot directly be applied to solving large models. Hence, there is a need for better solutions. Similarly, at present, there are no efficient methods for solving load-sharing cumulative exposure models. In addition to this, it is interesting to study the optimal dynamic load distribution of these systems.

References

[1] Misra KB. Reliability analysis and prediction: A methodology oriented treatment. Elsevier, Amsterdam, 1992.

[2] Liu H. Reliability of a load-sharing k-out-of-n:G system: Non-iid components with arbitrary distributions. IEEE Trans. on Reliability 1998; 47: 279–284.

[3] Kapur KC, Lamberson LR. Reliability in engineering design. Wiley, New York, 1977; 405–414.

[4] Iyer RK, Rossetti DJ. Effect of system workload on operating system reliability: A study on IBM 3081. IEEE Trans. on Software Engineering 1985; SE-11:1438–1448.

[5] Iyer RK, Rosetti DP. A measurement-based model for workload dependency of CPU errors. IEEE Trans. on Computers 1986; C-35: 511–519.

[6] Kuo W, Zuo MJ. Optimal reliability modelling. Wiley, New York, 2003; 258–264.

[7] Kim H. Reliability modelling with load-shared data and product-ordering decisions considering uncertainty in logistics operations. PhD Dissertation, Georgia Institute of Technology, 2004.
[8] Kvam PH. Peña EA. Estimating load-sharing properties in a dynamic reliability system. Journal American Statistical Association, 2005; 100: 262–272.
[9] Aven T, Jensen U. Stochastic models in reliability. Springer, Berlin, 1999.
[10] Nakagawa T. Shock and damage models in reliability theory. Springer, Berlin, 2006.
[11] Marshall AW, Olkin I. A multivariate exponential distribution. Journal American Statistical Association, 1967; 62: 30–44.
[12] Daniels H.E. The statistical theory of the strength bundles of threads I. Proc. Royal Society London, Series A 1945; 183: 405–435.
[13] Carlson RL, Kardomateas GA. An introduction to fatigue in metals and composites. Chapman and Hall, New York, 1996.
[14] Jelinski Z, Moranda P. Software reliability research. In: Freiberg W, editor. Statistical computer performance evaluation. Academic Press, New York, 1972; 465–484.
[15] Wang YT, Morris RJT. Load sharing in distributed systems. IEEE Trans. on Computers 1985; 34: 204–217.
[16] Kvam P.H. and Day D., The multivariate Polya distribution in combat modeling. Naval Research Logistics 2001; 48: 1–17.
[17] Jewell N.P. and Kalbfleisch J.D., Marker processes in survival analysis. Lifetime Data Analysis 1996; 2: 15–19.
[18] Amari S.V, McLaughlin L, and Pham H, Cost-effective condition-based maintenance using Markov decision processes. Proc. IEEE Annual Reliability and Maintainability Symposium, Jan. 23–36, Newport Beach, CA, 2006; 464–469.
[19] Amari S.V, Misra K.B, and Pham H. Reliability analysis of tampered failure rate load-sharing k-out-of-n:G systems. Proc. 12th ISSAT Int. Conf. on Reliability and Quality in Design, Honolulu, Hawaii, Aug. 4–6, 2006; 30–35.
[20] Harlow D, Phoenix S.L. The chain-of-bundles probability model for the strength of fibrous materials. I – Analysis and conjectures. Journal of Composite Materials 1978; 12: 195–214.
[21] Porwal P.K, Beyerlein I.J, Phoenix S.L. Statistical strength of a twisted fiber bundle: an extension of Daniels equal-load-sharing parallel bundle theory. Journal of Mechanics of Materials and Structures 2006; 1: 1425–1447.
[22] Nelson W. Accelerated Testing: Statistical Models, Test Plans, and Data Analysts. Wiley, New York, 1990.
[23] Cox D.R. Regression models and life tables (with discussion). J. Royal Statistical Society, Series B 1972, 34(2): 187–220.
[24] Jardine A.K.S, Ralston P, Reid N, Stafford J. Proportional hazards analysis of diesel engine failure data. Quality and Reliability Engineering International 1989; 5: 207–216.
[25] Kumar D, Klefsjo B. Proportional hazards model: A review. Reliability Engineering and System Safety 1994; 44: 177–188.
[26] Liu H. Makis V. Cutting-tool reliability assessment in variable machining conditions. IEEE Trans. on Reliability 1996; 45: 573–581.
[27] Pike M.C., A method of analysis of a certain class of experiments in carcinogenesis. Biometrics 1966; 22: 142–161.
[28] Solomon P.J,. Effect of misspecification of regression models in the analysis of survival data. Biometrika 1984; 71: 291–298.
[29] Bhattacharyya G.K, Soejoeti Z. A tampered failure rate model for step-stress accelerated life test. Communications in Statistics: Theory Method 1989; 18: 1627–1643.
[30] Madi M.T. Multiple step-stress accelerated life test: The tampered failure rate model. Communications in Statistics, Theory and Methods 1993; 22: 2631–2639.
[31] Wang R, Fei H. Uniqueness of the maximum likelihood estimate of the Weibull distribution tampered failure rate model. Communications in Statistics: Theory and Methods 2005; 32: 2321–2338.
[32] Xu H, Tang Y. Commentary: The Khamis/Higgins model. IEEE Trans. on Reliability 2003; 52: 4–6.
[33] Khamis H, Higgins J.J. New model for step-stress testing. IEEE Trans. on Reliability 1998; 47: 131–134.
[34] Nelson W. Accelerated life testing-step-stress models and data analysis. IEEE Trans. on Reliability 1980; R-29: 103–108.
[35] Mettas A, Vassiliou P. Application of quantitative accelerated life models on load sharing redundancy. Proc. Ann. Reliability and Maintainability Symp. 2003; 551–555.
[36] Van Paepegem W, Degrieck J. Effects of load sequence and block loading on the fatigue response of fiber-reinforced composites. Mechanics of Advanced Materials and Structures 2002; 9: 19–35.
[37] Degroot MH, Goel PK. Bayesian estimation and optimal design in partially accelerated life-testing.

Naval Research Logistics Quarterly, 1979; 26: 223–235.

[38] Zhao W, Elsayed E. A general accelerated life model for step-stress testing. IIE Transactions 2005; 37: 1059–1069.

[39] Pan R, Ayala S. Two statistical models for step-stress accelerated life test analysis. 47th Fall Tech. Conf. of ASQ and ASA 2003.

[40] Coleman BD. Statistics and time dependence of mechanical breakdown in fibers. Journal of Applied Physics 1958; 29: 968–983.

[41] Rundle JB, Turcotte DL, Shcherbakov R, Klein W, Sammis C. Statistical physics approach to understanding the multiscale dynamics of earthquake fault systems. Reviews of Geophysics, 2003; 41: 5.1–5.30.

[42] Smith RL. The asymptotic distribution of the strength of a series-parallel system with equal load-sharing. The Annals of Probability 1982; 10: 137–171.

[43] Phoenix SL, Beyerlein IJ. Statistical strength theory for fibrous composite materials, Comprehensive composite materials, editor: Kelly A *et al*., Elsevier, Amsterdam, 2000; 1: 559–639.

[44] Scheuer EM. Reliability of an m-out-of-n system when component failure induces higher failure rates in survivors. IEEE Trans. on Reliability 1988; 37: 73–74.

[45] Coleman BD. Time dependence of mechanical breakdown in bundles of fibers I: Constant total load. Journal of Applied Physics 1957; 28: 1058–1064.

[46] Coleman BD. Time dependence of mechanical breakdown in bundles of fibers II: The infinite ideal bundle under linearly increasing loads. Journal of Applied Physics 1957; 28: 1065–1067.

[47] Kuo CC, Phoenix SL. Recursions and limit theorems for the strength and lifetime distributions of a fibrous composite. Journal of Applied Probability 1987; 24: 137–159.

[48] Phoenix SL. The asymptotic distribution for the time to failure of a fiber bundle. Advances in Applied Probability 1979; 11: 153–187.

[49] Phoenix SL. The asymptotic time to failure of a mechanical system of parallel members. SIAM Journal on Applied Mathematics 1978; 34: 227–246.

[50] Phoenix SL. Probabilistic theories of time dependent failure of fiber bundles. Oceans 1976; 8: 206–216.

[51] Mahesh S, Phoenix SL. Lifetime distributions for unidirectional fibrous composites under creep-rupture loading. International Journal of Fracture 2004; 127: 303–360.

[52] Tierney L. Asymptotic bounds on the time to fatigue failure of bundles of fibers under local load sharing. Advances in Applied Probability 1982; 14: 95–121.

[53] Harlow DG, Smith R, Taylor HM. The asymptotic distribution of certain long composite cables. Tech. Report 384, Dept. of Operations Research, Cornell University, 1978.

[54] Harlow DG, Smith RL, Taylor HM. Lower tail analysis of the distribution of the strength of load-sharing systems. Journal of Applied Probability 1983; 20: 358–367.

[55] Borges WDS. On the limiting distribution of the failure time of fibrous materials. Advances in Applied Probability 1983; 15: 331–348.

[56] Loève M. Ranking limit problem. Proc. 3rd Berkeley Symp. Math. Stat. Prob. 1956; 2:177–194.

[57] Newman WI, Phoenix SL. Time-dependent fiber bundles with local load sharing. Physical Review E 2001, 63: 021507.

[58] Høyland A, Rausand M. System reliability theory: Models and statistical methods. 5th edition, Wiley, New York, 1994; 158–159.

[59] Kececioglu D. Reliability engineering handbook. PTR Prentice Hall, Englewood Cliffs, NJ, 1991; 2: pp. 363–399.

[60] Pham H. Reliability analysis of a high-voltage power system with dependence failure and imperfect coverage. Reliability Engineering and System Safety 1992; 37: 25–28.

[61] Birolini A. Reliability engineering: Theory and practice. Springer, Berlin, 2004.

[62] Freund JE. A bivariate extension of the exponential distribution. Journal of American Statistical Association. 1961; 56: 971–977.

[63] Pozsgai P, Neher W, Bertsche B, Models to consider load-sharing in reliability calculation and simulation of systems consisting of mechanical components. Proc. IEEE Ann. Reliability and Maintainability Symp., Tampa, Florida, Jan. 2003; 493–499.

[64] Amari SV. Reliability, risk and fault-tolerance of complex systems. PhD Dissertation, Indian Institute of Technology, Kharagpur, 1997.

[65] Amari SV, Misra RB. Closed-form expressions for distribution of sum of exponential random variables. IEEE Trans. on Reliability 1997; 46: 519–522.

[66] Weier DR. Bayes estimation for bivariate survival models based on the exponential distribution. Comm. in Stat.: Theory and Methods 1981; 10: 1415–1427.

[67] Siriteanu C, Blostein SD. Maximal-ratio eigen-combining: a performance analysis. Canadian Journal of Electrical and Computer Engineering 2004; 29: 15–22.

[68] Kim IM. Exact BER Analysis of OSTBCs in spatially correlated MIMO channels. IEEE Trans. on Communications 2006; 54: 1365–1373.

[69] Shao J, Lamberson LR. Modeling a shared-load k-out-of-n:G system. IEEE Trans. on Reliability 1991; 40: 205–209.

[70] Akhtar S. Comment on: Modeling a shared-load k-out-of-n:G system. IEEE Trans. on Reliability 1992; 50: 189.

[71] Newton J. Comment on: Modeling a shared-load k-out-of-n:G system. EEE Trans. on Reliability 1993; 42: 140.

[72] Xie M, Poh KL, Dai YS. Computing system reliability: Models and analysis. Kluwer Academic/Plenum Publishers, Hingham, MA, 2004.

[73] Chan CK. Availability analysis of load-sharing systems. Proc. IEEE Ann. Reliability and Maintainability Symp., Tampa, Florida, Jan. 2003: 551–555.

[74] Lin HH, Chen KH, Wang RT. A multivariate exponential shared-load model. IEEE Trans. on Reliability 1993; 42: 165–171.

[75] Shaked M., Extensions of the Freund distribution with applications in reliability theory. Operations Research 1984; 32: 917–925.

[76] Lu JC. Weibull extensions of the Freund and Marshall–Olkin bivariate exponential models. IEEE Trans. on Reliability 1989; 38(5): 615–619.

[77] Kececioglu D, Jiang S. Reliability of two load-sharing Weibullian units. SAE Technical Papers 1986; No: 861849.

[78] Liu H, Makis V, Jardine AKS. Reliability assessment of systems operating in variable conditions. Proc. ISUMA-NAFIPS 1995; 5–8.

[79] Liu H, Makis V, Jardine AKS. Computation of reliability for systems operating in varying conditions. In Uncertainty modeling and analysis in civil engineering, editor: Ayyub BM, CRC Press, Boca Raton, FL, 1997; 99–120.

[80] Hassett TF, Dietrich DL, Szidarovszky F. Time-varying failure rates in the availability and reliability analysis of repairable systems. IEEE Trans. on Reliability 1995; 44: 155–160.

[81] Press WH, Teukolsky SA, Vetterling WT, Flannery BP. Numerical recipes in C. 2nd edition, Cambridge University Press, 1992.

[82] Dugan JB, Tutorial: Fault-tree analysis of computer-based systems. Proc. Ann. Reliability and Maintainability Symp., Tampa, Florida, Jan. 2003.

[83] Amari SV, Dill G, Howald E. A new approach to solve dynamic fault trees. Proc. Ann. Reliability and Maintainability Symp., Tampa, Florida, Jan. 2003: 374 –379.

21

O(*kn*) Algorithms for Analyzing Repairable and Non-repairable *k*-out-of-*n*:G Systems

Suprasad V. Amari[1], Ming J. Zuo[2], and Glenn Dill[1]

[1] Relex Software Corporation, USA
[2] Department of Mechanical Engineering, University of Alberta, Canada

Abstract: The *k*-out-of-*n*:G system has a wide range of applications in reliability engineering. Several efficient algorithms are available for analyzing the reliability of non-repairable systems. However, such efficient algorithms are not readily available for computing other reliability indices such as the failure (hazard) rate, the probability density function, or the mean time to failure (MTTF). Similarly, the methods for computing the steady-state availability measures, such as failure frequency, mean up-time and mean down-time in a failure-repair cycle, and the mean time between failures (MTBF) of repairable *k*-out-of-*n*:G systems are limited. In this chapter, utilizing the concepts of failure frequency, we present efficient algorithms to compute various reliability and availability indices of *k*-out-of-*n*:G systems. The algorithms are applicable for arbitrary general failure and repair distributions. For repairable systems, we also consider a case where components are kept idle during a system failure (suspended animation). Whenever applicable, we also present simplified results for the exponential case. For the non-identical component case, all of these algorithms have at most $O(kn)$ computational complexity. For the identical component case, the computational complexity reduces to $O(n)$.

21.1 Introduction

In reliability engineering, it is a common practice to use redundancy techniques to improve system reliability and availability. A common form of redundancy is the *k*-out-of-*n*:G (F) structure, which was introduced by Birnbaum *et al*. [8] in 1961. The *k*-out-of-*n*:G (F) system consists of *n* components and functions (fails) if and only if at least *k* of the *n* components function (fail). Therefore, a k-out-of-n:G system is equivalent to $(n-k+1)$-out-of-*n*:F system. In research literature, the term "*k*-out-of-*n* system" is often used to indicate either a *k*-out-of-*n*:G system or a *k*-out-of-*n*:F system (or both). However, in practice, most engineers often use the term *k*-out-of-*n* system to represent the *k*-out-of-*n*:G system and are confused by the additional symbols "G" and "F". This is particularly true in the context of reliability block diagrams or any success oriented models. In this chapter, for simplicity, we often omit "G" and refer to a *k*-out-of-*n*:G system as a *k*-out-of-*n* system. Hence, in the context of this chapter, a *k*-out-of-*n* system functions (fails) if and only if at most $n-k$ (at least $n-k+1$) components fail. Thus, the life of a non-repairable *k*-out-of-*n* system can be characterized

by the $(n-k+1)$th order statistic, which represents the $(n-k+1)$th smallest failure time among n possible failure times.

The k-out-of-n:G redundancy finds a wide range of applications in both industrial and military systems. Examples include the cables in a bridge, a data processing system with multiple video displays, communication systems with multiple transmitters, and the multi-engine system in an airplane. Among applications of the k-out-of-n system, the design of electronic circuits such as very large scale integrated (VLSI) circuits and the automatic repairs of faults in an on-line system, would be the most conspicuous [13]. Several examples of k-out-of-n systems are available in [13, 15]. Both series systems and parallel systems are special cases of the k-out-of-n system. The k-out-of-n system has been investigated extensively in the literature. Various related models have been developed and many formulas have been derived, resulting in a large body of literature. For general results, please refer to Singh and Billinton [25], Ravichandran [19], Misra [16], Trivedi [26], and Kuo and Zuo [13], *etc*. Comparisons of various algorithms for computing the reliability of non-repairable systems are provided by Rushdi [24], Dutuit and Rauzy [11], and Kuo and Zuo [13].

Optimal cost-effective design of non-repairable k-out-of-n systems and subsystems is studied in [2]. Load-sharing k-out-of-n systems are studied in [1, 15]. Recently, Koucky [12] derived the exact formula for the reliability of general k-out-of-n systems whose component failures need not be independent and identically distributed (IID). However, there are relatively few publications on repairable k-out-of-n systems. Even for non-repairable k-out-of-n systems, efficient algorithms are not readily available for computing other reliability indices such as failure (hazard) rate, probability density function (pdf), and mean time to failure (MTTF). In this chapter, we provide efficient algorithms to compute various reliability and availability indices of k-out-of-n systems.

Section 21.2 discusses the background of the problem including the general assumptions and motivation. Section 21.3 presents the algorithms to compute the measures of non-repairable systems. Section 21.4 presents the algorithms to compute the steady-state measures of repairable systems. Section 21.5 presents some simplified results for various special cases, including: (1) exponential failure and repair distributions, (2) MTTF of non-repairable systems, (3) mean time to first failure (MTTFF) of repairable systems, (4) systems with suspended animation, and (5) some simple bounds and approximations. Finally, Section 21.6 presents the conclusions and indication to future research.

21.2 Background

21.2.1 General Assumptions

The general assumptions of the model are:

1. The system consists of n statistically independent components. Hence, the life-times and repair-times of the n components of the k-out-of-n system are s-independent.
2. At least k out of n components must work for the successful operation of the system.
3. The failure and repair time distributions of the components can follow any arbitrary general distribution.
   - For the exponential case, the failure and repair time distributions of all components are exponential.
   - For the identical case, all failure time and all repair time distributions are the same.
   - For non-repairable case, the repair time distributions are not applicable.
4. For a repairable system, a component is assigned a repairman as soon as it fails. A repaired component is as good as new, *i.e.*, the repair is perfect. The repair times of failed components are independent.

In addition to these assumptions, specific assumptions that are applicable to various cases will be introduced later in this chapter.

21.2.2 Availability Measures

One of the important measures of a repairable system is its steady-state availability (A). Another important measure of repairable systems is its steady-state failure frequency (ω), which is the

number of failures per unit time in a long run (as time tends to infinity). It should be noted that the steady-state failure frequency is equivalent to the steady-state repair frequency. Other measures, such as mean failure-repair cycle time [also called mean cycle time (MCT) or mean time between failures (MTBF)], mean working time during a failure-repair cycle [also called mean up-time (MUT) or mean time to failure (MTTF)], mean down-time during a failure-repair cycle [also called mean down-time (MDT) or mean time to repair (MTTR)], expected number of system failures/repairs [NSF/NSR] during a specified interval (T), can easily be found from A *and* ω [9].

$$\begin{aligned} MCT &= MTBF = \frac{1}{\omega} \\ MUT &= MTTF = \frac{A}{\omega} \\ MDT &= MTTR = \frac{U}{\omega} \\ NSF &= NSR = \frac{T}{\omega} \end{aligned} \tag{21.1}$$

In some papers [14], MUT and MDT are also referred as expected up-time (EU) and expected down-time (ED), respectively. It should be obvious from (21.1) that once A and ω are found, all other measures can be computed easily with simple formulae that can be evaluated with constant time complexity, *i.e.*, $O(1)$. Therefore, for the repairable case, we provide algorithms only for computing A and ω.

21.2.3 Motivation

There are several algorithms for computing the reliability of a non-repairable *k*-out-of-*n* system with identical or non-identical components. For details, refer to Misra [16], Rushdi [24], Dutuit and Rauzy [11], and Kuo and Zuo [13]. These algorithms are independent of the failure distribution of the components, but they use the independent assumption among the components' failure behavior. However, there are very few algorithms for computing the availability of a repairable *k*-out-of-*n* system. As long as all components are *s*-independent, *i.e.*, failure and repair processes of a component are *s*-independent of the status of other components, we can compute the system availability using the same algorithms (or functions) that are used to compute system reliability. The system reliability (availability) computation uses component reliabilities (availabilities) as inputs. However, it is easy to compute the component reliability, but not the component availability, particularly when the failure and repair distributions are non-exponential. Therefore, even for the *s*-independent case, efficient algorithms are limited to the case of exponential failure and repair distributions. Fortunately, Ross [21] presented an important finding to overcome this difficulty. As long as all components are *s*-independent, according to Ross [21], we can use the same algorithms to compute several steady-state measures of the system including availability and failure frequency using the same algorithms that are used for non-repairable cases. This means that efficient algorithms are available not only for the steady-state availability but also for various other important measures of repairable systems. We believe that most researchers have over looked this important finding. In this chapter, using these basic concepts, we provide efficient algorithms to compute various steady-state availability measures. In most cases, we use or modify the algorithms available for a non-repairable *k*-out-of-*n* system to compute the availability of repairable a *k*-out-of-*n* system. Further, we also use the concepts of failure frequency (used to analyze repairable systems) in computing the failure rate and pdf of non-repairable systems.

21.3 Non-repairable *k*-out-of-*n* Systems

In this section, we assume that the system consists of n independent components. Initially (at time t = 0), all components are working and are all new. It should be noted that the "all new condition" is not required if we know the conditional reliability. The system functions properly as long as there are at least k working components. The failure time of each component can follow any arbitrary distribution. We considered two cases:

- Identical components: all components are identical and follow the same failure distribution.
- Non-identical components: all or some of the components are non-identical and may follow different failure distributions.

21.3.1 Identical Components

Let $p(t)$, $q(t)$, $\lambda(t)$, and $f(t)$ be the reliability, unreliability, failure (hazard) rate, and pdf of each component at time t. For simplicity, we omit t when it is obvious. For any distribution, the following relationships are valid:

$$q(t) = 1 - p(t); \quad f_c(t) = \lambda(t) \cdot p(t). \quad (21.2)$$

It is well-known that the reliability of a k-out-of-n system can be found using binomial distribution.

$$R = \sum_{i=k}^{n} \binom{n}{i} p^i \cdot q^{n-i} = \sum_{i=0}^{n-k} \binom{n}{i} p^{n-i} \cdot q^i. \quad (21.3)$$

The R in (21.3) can be evaluated with $O(n)$ computational complexity as in the following algorithm.

Algorithm 1: Reliability with Identical Components

$x = p^n = \exp\{n \cdot \ln(p)\}$;
for $i = 1$ to $(n-k)$ do
$\quad x = x \cdot y \cdot \dfrac{n-i+1}{i}; \quad \mathrm{Re}l = \mathrm{Re}l + x$
done

At the end of the algorithm, the results for R will be accumulated in Rel. In fact, the computational time of this algorithm depends on both k and n and is proportional to $(n–k)$. Hence, the computational complexity can be considered as $O(n–k)$. If $k < n/2$, in order to reduce computational time, we can compute system reliability from system unreliability.

$$Q = \sum_{i=n-k+1}^{n} \binom{n}{i} q^i \cdot p^{n-1} = \sum_{i=0}^{k-1} \binom{n}{i} p^i \cdot q^{n-i} \quad (21.4)$$
$$R = 1 - Q$$

We can modify Algorithm 1 slightly to compute Q and R in $O(k)$ computational complexity. Therefore, in general, the computational time of R is proportional to $\min\{k, n–k\}$, which is less than $O(n)$. Similar improvements are also applicable for all algorithms discussed in this chapter. However, those improvements are obvious to most reliability analysts; hence, those are not discussed unless special attention to them is required.

The well-known expression for the pdf of the system is:

$$f(t) = \frac{dQ(t)}{dt} = \frac{d[1 - R(t)]}{dt} = \frac{-dR(t)}{dt} \quad (21.5)$$

It is not straightforward to get the closed-form solution for the right-hand side expression in (21.5). However, we can find a closed-form solution to f using the failure frequency concepts applicable for Markov chains. Specifically, the k–out-of-n system fails at time t when the system is in a state where exactly k components are working and one of those k working components fails at time t. Hence, we have:

$$f(t) = p_k(t) \cdot [k \cdot \lambda(t)]$$
$$p_k(t) = \binom{n}{k} p^k \cdot q^{n-k} \quad (21.6)$$

P_k can be calculated using Algorithm 1 with $O(n–k)$ computational complexity. Specifically, the final results accumulated in the variable x in Algorithm 1 is equivalent to P_k (Rel is not required for computing P_k). Therefore, we can find the pdf of a k-out-of-n system with linear time complexity algorithms. Once we know R and f, we can easily find the failure rate of the system: $h = f/R$.

$$h(t) = \frac{f(t)}{R(t)} = \frac{\binom{n}{k}[p(t)]^k \cdot [q(t)]^{n-k}[k \cdot \lambda(t)]}{\sum_{i=k}^{n} \binom{n}{i}[p(t)]^i \cdot [q(t)]^{n-i}} \quad (21.7)$$

Using Algorithm 1 (using only a single pass), we can compute the failure rate with the linear time complexity.

21.3.2 Non-identical Components

Let $p_i(t)$, $q_i(t)$, $\lambda_i(t)$, and $f_i(t)$ be the reliability, unreliability, failure (hazard) rate, and pdf of

component *i* at time *t*. As in the identical component case, irrespective of the failure distribution, the following relationships are valid:

$$q_i(t) = 1 - p_i(t); \quad f_i(t) = \lambda_i(t) \cdot p_i(t) \tag{21.8}$$

In this case, we first select an existing algorithm for computing system reliability with non-identical components. Later, we modify this algorithm without increasing its computational complexity to compute the pdf of the system. Finally, we calculate the failure rate of the system from the calculated system reliability and pdf.

There are several algorithms to compute the reliability of a *k*-out-of-*n* system with non-identical components [13]. In this chapter, we consider a well-known algorithm that was originally proposed by Barlow and Heidtmann [7] and Rushdi [23, 24]. We also utilize the iterative implementation provided in [11]. This algorithm has $O(n \cdot (n-k+1))$ computational complexity and requires less memory than other algorithms [13].

The algorithm is based on the following recursive relationship. Let $H(r,m)$ be the probability of at least *r* components out of the first *m* components are good. Then, we have:

$$\begin{aligned} R &= H(k,n) \\ H(r,m) &= p_m \cdot H(r-1,m-1) + q_m \cdot H(r,m-1) \\ &\qquad \text{for } 1 \le r \le m \\ &= 1 \quad \text{for } r = 0, m \ge 0 \\ &= 0 \quad \text{for } r = m+1 \end{aligned} \tag{21.9}$$

Although $H(r,m)$ is a two-dimensional array, at any given time, we need to store only a few of these values. In the following iterative algorithm, only $k+1$ values of *H* are stored in the one-dimensional array *P*.

Algorithm 2: Reliability with Non-identical Components

$P(0) = 1$; for $i = 1$ to k do $P[i] = 0$; done
for $i = 1$ to n do
  for $j = k$ downto 1 do
    $P[j] = p_i \cdot P[j-1] + q_i \cdot P[j]$
  done
done

At the end of the algorithm, for $1 \le j \le k$, the reliability results for a j-out-of-n system will be accumulated in $P[j]$. Hence, the reliability of a k-out-of-n system is equivalent to $P[k]$.

In order to compute the pdf, we use the concepts of failure frequency [3, 9]. In fact, as mentioned in [4, 5], for non-repairable systems, failure frequency is equivalent to its pdf, *i.e.*, $\omega = f$. There are several algorithms for computing the failure frequency. In this chapter, we use a factorial algorithm that calculates the failure frequency (pdf). Therefore, applying the factorial algorithm to the reliability recursion used in (21.9), we find a recursive relationship for the failure frequency (21.10).

$$\begin{aligned} f &= F(k,n) \\ F(r,m) &= p_m \cdot F(r-1,m-1) + f_m \cdot H(r-1,m-1) \\ &+ q_m \cdot F(r,m-1) - f_m \cdot H(r,m-1) \text{ for } 1 \le r \le m \\ &= 0 \quad \text{for } r = 0; m \ge 0 \\ &= 1 \quad \text{for } r = m+1 \end{aligned} \tag{21.10}$$

The proof of the above recursion is similar to the proof of the failure frequency calculations used in BDD [9]. Integrating the relationships between $H(r,m)$ and $F(r,m)$ shown in (21.9) and (21.10), we propose the following iterative algorithm to compute system pdf.

Algorithm 3: Pdf with Non-identical Components

$P(0) = 1$; $F(0) = 0$;
for $i = 1$ to k do $P[i] = 0$; $F[i] = 0$; done
for $i = 1$ to n do
  for $j = k$ downto 1 do
    $F[j] = f_i \cdot (P[j-1] - P[j]) + p_i \cdot F[j-1] + q_i \cdot F[j]$
    $P[j] = p_i \cdot P[j-1] + q_i \cdot P[j]$
  done
done

At the end of the algorithm, for $1 \le j \le k$, the pdf results for a *j*-out-of-*n* system will be accumulated in $F[j]$. Hence, the pdf of a *k*-out-of-*n* system is equivalent to $F[k]$. Once we know the pdf and reliability, it is straightforward to calculate the failure rate: $h = f/R = F[k]/P[k]$.

21.4 Repairable *k*-out-of-*n* System

In this section, we consider a *k*-out-of-*n* repairable system with the following additional assumptions.

21.4.1 Additional Assumptions

1. Non-failed components continuously operate irrespective of the system state.
2. For each component, the steady-state availability exists. This assumption is mild and can be ignored if both failure and repair distributions are non-deterministic. Specifically, the assumption is satisfied if either failure or repair distribution is non-lattice [21].

A repairable *k*-out-of-*n* system fails only if the total number of failed components at any instant of time reaches (*n*-*k*+1) or more. Assume that all of the system's components are working at time 0. Thus, the system is in the up state at time 0. As components fail, repair work is performed on the failed components. If the number of components simultaneously in the failed state reaches (*n*–*k*+1), the system makes a transition from the up state to the down state. When the system is down, repair work continues on the failed components, and the system will return to the up state as soon as the number of failed components becomes lower than (*n*–*k*+1). For the exponential case, it is obvious that the behavior of the system constitutes a delayed alternating renewal process. However, even with general failure and repair distributions, using the basic concepts presented in Ross [21], we can compute the steady-state measures using combinatorial algorithms [10].

21.4.2 Identical Components

Let ϕ and θ be the MTTF and MTTR of each component. Then, steady-state availability (a), unavailability (u), and failure frequency (ω_c) are:

$$a = \frac{\phi}{\phi+\theta};\quad u = \frac{\theta}{\phi+\theta} = 1-a;\quad \omega_c = \frac{1}{\phi+\theta} \tag{21.11}$$

The system steady-state availability can be found using binomial distribution.

$$A = \sum_{i=k}^{n}\binom{n}{i}a^i \cdot u^{n-1} = \sum_{i=0}^{n-k}\binom{n}{i}a^{n-1}\cdot u^i \tag{21.12}$$

The A in (21.12) can be evaluated with $O(n)$ computational complexity as in the following algorithm.

Algorithm 4: Availability with Identical Components

$$x = a^n = \exp\{n\cdot\ln(a)\};\quad Avail = x;\quad y = \frac{u}{a}$$

for $i = 1$ to $(n-k)$ do

$$x = x\cdot y\cdot\frac{n-i+1}{i};\quad Avail = Avail + x$$

done

At the end of the algorithm, the results for A will be accumulated in *Avail*. The computational complexity is $O(n–k)$.

Further, the steady-state failure frequency of the system is:

$$\omega = P_k \cdot \left\lfloor k/\phi \right\rfloor$$
$$P_k = \binom{n}{k}a^k\cdot u^{n-k} \tag{21.13}$$

The P_k can be calculated using Algorithm 1 with $O(n–k)$ computational complexity. Specifically, the final result accumulated in the variable x in Algorithm 1 is equivalent to P_k. Therefore, we can find the failure frequency of a *k*-out-of-*n* system with linear time complexity algorithms. Once we know A and ω, we can easily find other measures as shown in (21.1).

21.4.3 Non-identical Components

Let ϕ_i and θ_i be the MTTF and MTTR of component i. Then steady-state availability (a_i), unavailability (u_i), and failure frequency (ω_i) of component i are:

$$a_i = \frac{\phi_i}{\phi_i+\theta_i};\ u_i = \frac{\theta_i}{\phi_i} = 1-a_i;\quad \omega_i = \frac{1}{\phi_i+\theta_i} \tag{21.14}$$

Once we know the steady-state measures for individual components, we can compute the system level measures using the following algorithm.

Algorithm 5: Availability with Non-identical Components

$P(0) = 1;$ for $i = 1$ to k do $P[i] = 0;$ done
for $i = 1$ to n do
  for $j = k$ downto 1 do
    $P[j] = a_i \cdot P[j-1] + u_i \cdot P[j]$
  done
done

At the end of the algorithm, for $1 \le j \le k$, the availability results for a j-out-of-n system will be accumulated in $P[j]$. Hence, the availability of a k–out-of-n system is $P[k]$. This algorithm can also be used to get time-specific availability measures of the system provided that the time-specific availability measures of the components are available. However, computing the time-specific availability measures for components with general distributions is difficult. However, for the exponential case, the measures can be found easily.

$$a_i = \frac{\mu_i}{\lambda_i + \mu_i} + \frac{\lambda_i}{\lambda_i + \mu_i} \exp\{-(\lambda_i + \mu_i)t\}$$
$$u_i = 1 - a_i; \quad \omega_i = a_i \cdot \lambda_i \tag{21.15}$$

The algorithm for computing steady-state availability and failure frequency follows. The same algorithm can also be used to compute the time-specific measures for the exponential case.

Algorithm 6: Steady-state A and ω with Non-identical Components

$P(0) = 1;\ F(0) = 0;$
for $i = 1$ to k do $P[i] = 0;\ F[i] = 0;$ done
for $i = 1$ to n do
  for $j = k$ downto 1 do
    $F[j] = \omega_i \cdot (P[j-1] - P[j])$
      $+ a_i \cdot F[j-1] + u_i \cdot F[j]$
    $P[j] = a_i \cdot P[j-1] + u_i \cdot P[j]$
  done
done

At the end of the algorithm, for $1 \le j \le k$, the results for ω and A of a j-out-of-n system will be accumulated in $F[j]$ and $P[j]$, respectively. Hence, the failure frequency of the k-out-of-n system is equivalent to $F[k]$. Once we know A and ω, we can easily find other measures as shown in (21.1).

21.5 Some Special Cases

In this section, we present some results that are specifically applicable for the exponential case.

21.5.1 MTTF

A k-out-of-n system with non-repairable components can fail only once. Therefore, in this case, MTTF is equivalent to MTTFF. The MTTF of any system can be calculated by integrating its reliability over $(0, \infty)$. Hence, we have:

$$\text{MTTF} = \int_0^\infty t \cdot f(t)\,dt = \int_0^\infty R(t)\,dt \tag{21.16}$$

In general, it is difficult to find a computationally efficient closed-form solution for MTTF. It is particularly true for the case of general distributions and non-identical components. However, we can compute MTTF using numerical integration methods [17]. To find MTTF, we should compute $R(t)$ at $t = t_1, t_2, \ldots, t_m$. For any given time t, we can compute $R(t)$ with $O(kn)$ computational complexity. Hence, using the algorithms presented in Section 21.3, we can compute the MTTF with $O(mnk)$ computational complexity, where m is the number of evaluations of $R(t)$. For the identical component case, the complexity reduces to $O(mk)$. To overcome the difficulties with infinite upper limit, we can use the concepts of improper integrals. One such solution is:

$$\text{let } x = e^{-t} \text{ or } t = -\ln(x)$$
$$\text{MTTF} = \int_0^\infty R(t)\,dt = \int_{t=0}^{t=a} R(t)\,dt + \int_{x=0}^{x=e^{-a}} \frac{R(-\ln(x))}{x} dx \tag{21.17}$$

If $a = 1$, we have:

$$\text{MTTF} = \int_{t=0}^{t=1} R(t)\,dt + \int_{x=0}^{x=e^{-1}} \frac{R(-\ln(x))}{x} dx \tag{21.18}$$

In some cases, we can find simple closed-form solutions for MTTF.

1. IID components with exponential failure distribution: $\lambda_i=\lambda$ for all i.

$$\text{MTTF}=\sum_{i=k}^{n}\frac{1}{i\cdot\lambda}=\frac{1}{\lambda}\left[\sum_{i=k}^{n}\frac{1}{i}\right] \tag{21.19}$$

The MTTF in (21.19) can be computed with $O(n–k)$ time complexity. For large n and k, we can compute the MTTF approximation in a constant time using harmonic number approximation.

$$H(n)=\sum_{i=1}^{n}\frac{1}{i}\approx\ln(n)+0.57721$$

$$\text{MTTF}=\frac{1}{\lambda}\left[H(n)-H(k-1)\right]$$

$$\approx\frac{1}{\lambda}\left[\ln(n)-\ln(k-1)\right]=\frac{1}{\lambda}\cdot\ln\left(\frac{n}{k-1}\right) \tag{21.20}$$

2. Some results for IID components with non-exponential failure distribution are presented in [16]. Particularly, closed-form solutions are presented for Weibull and extreme value distributions. Even for the IID case, these formulas are complex, and numerical evaluation of these formulas may not be efficient as compared to the numerical integration used in (21.17). Further, we have:

- If the components follow an increasing failure rate (IFR) distribution, then the system MTTF found with the exponential distribution (21.19), assuming λ is the reciprocal of component MTTF, is the upper bound of the MTTF of the k-out-of-n system.
- Similarly, if the components follow a decreasing failure rate (DFR) distribution, then the system MTTF found with the exponential distribution (21.19), assuming λ is the reciprocal of component MTTF, is the lower bound of the MTTF of the k-out-of-n system.

3. Various MTTF formulas for non-identical components with exponential failure distributions are presented in [16]. For a 2-out-of-3 system, we have:

$$\text{MTTF}=\frac{1}{\lambda_1+\lambda_2}+\frac{1}{\lambda_1+\lambda_3}+\frac{1}{\lambda_2+\lambda_3}-\frac{2}{\lambda_1+\lambda_2+\lambda_3} \tag{21.21}$$

Similarly, we can also find the MTTF using Markov chain solutions.

$$\text{MTTF}=\frac{1}{\lambda_1+\lambda_2+\lambda_3}\left[1+\frac{\lambda_1}{\lambda_2+\lambda_3}+\frac{\lambda_2}{\lambda_1+\lambda_3}+\frac{\lambda_3}{\lambda_1+\lambda_2}\right] \tag{21.22}$$

For large n and small k, *i.e.*, for large n and $n–k$, the direct evaluation of these formulas is very difficult. In fact, computational time increases exponentially, *i.e.*, $O(n^{n-k})$. Therefore, we are not presenting these formulas for general k and n. We recommend numerical integration in (21.17) for computing the MTTF for the non-identical case.

21.5.2 MTTFF

As in the case of any repairable system, the k-out-of-n system with repairable components alternatively visits the up and down states. In a long run, the system reaches a steady-state. The steady-state MTTF, *i.e.*, up-time in a failure-repair cycle, is discussed in Section 21.4. However, in some cases, we are interested in finding the mean time to the first failure (MTTFF). In general, the MTTFF is not equivalent to MTTF. This is because initially all components are considered to be in good condition. In most cases, the first failure time is greater than the steady-state MTTF (also called MUT). Finding the MTTFF for the general case is difficult. For the exponential failure and repair case, the MTTFF can be computed using Markov chains. However, due to the well-known state space explosion problem, this method is computationally expensive for the non-identical case. Therefore, we may wish to find the bounds for MTTFF. When the failure and repair distributions are exponential, we have [5]: MTTFF > MTTF. Therefore, the MTTF calculations presented in (21.1) can be used as an approximation (or a lower

bound) to the MTTFF of the non-identical case. For the identical case, similar to the concepts used in [18], we present an efficient algorithm to compute MTTFF.

The *k*-out-of-*n* has (*n*–*k*+2) states. The state *i* (*i*= 0,···,*n*–*k*+1) has *i* failed components and (*n*–*i*) working components. Let *E(i)* denote the expected time it takes for the system to reach state (*n*–*k*+*1*) from the time it reaches state *i*. Then we have:

$$\begin{aligned}
&\text{MTTFF} = E(0) = \frac{1}{n\cdot\lambda} + E(1)\\
&E(i) = \alpha_i + \beta_i \cdot E(i+1) \quad \text{for } 1 \le i \le n-k\\
&E(n-k+1) = 0\\
&\textit{where}\\
&\alpha_i = \frac{1}{(n-i)\cdot\lambda + i\cdot\mu}\\
&\beta_i = \frac{i\cdot\mu}{(n-i)\cdot\lambda + i\cdot\mu}\\
&\gamma_i = \frac{(n-i)\cdot\lambda}{(n-i)\cdot\lambda + i\cdot\mu}
\end{aligned} \tag{21.23}$$

where α_i, β_i and γ_i are intermediate variables, which are defined as follows:

α_i = expected time per visit spent in state *i*
β_i = Pr{next visit of the system is to state (*i*–1) | system is in state *i*}
γ_i = Pr{ next visit of the system is to state (*i*+1) | system is in state *i*}

From the above recursion, we find that *E*(*i*) depends both on *E*(*i*–1) and *E*(*i*+1). In order to solve this equation, we first remove the dependency of *E*(*i*) on *E*(*i*+1) via back substitution. Hence, using *E*(*n*–*k*+1) = 0, the above recursion can be rewritten as:

$$\begin{aligned}
&E(i) = \frac{x_i + y_i \cdot E(i-1)}{z_i}\\
&z_i = 1 - \frac{\beta_i + 1\cdot\gamma_i}{z_i + 1} \quad \text{for } 1 \le i \le n-k\\
&\text{where } \; x_i = \alpha_i + \frac{x_i + 1\cdot\gamma_i}{z_i + 1}; \quad y_i = \beta_i\\
&x_{n-k} = \alpha_{n-k}; \quad y_{n-k} = \beta_{n-k}; \quad z_{n-k} = 1
\end{aligned} \tag{21.24}$$

The variables x_i, y_i, and z_i define the above recursion, and they themselves can also be found using recursive relations. Finally, the MTTFF of the system is:

$$\text{MTTFF} = E(0) = \frac{z_1}{z_1 - y_1}\left(\frac{1}{n\cdot\lambda}\right) + \frac{x_1}{z_1 - y_1} \tag{21.25}$$

Now we present an iterative algorithm to compute the MTTFF of a *k*-out-of-*n* system with IID components and exponential distributions.

Algorithm 7: MTTFF of a Repairable k-out-of-n System with IID Components and Exponential Distributions

$$\begin{aligned}
&\text{Rate} = k\cdot\lambda + (n-k)\cdot\mu;\\
&x[n-k] = \frac{1}{\text{Rate}};\\
&y[n-k] = (n-k)\cdot\mu\cdot x[n-k];\\
&z[n-k] = 1;\\
&\text{for } i = (n-k-1) \text{ downto } 1 \text{ do}\\
&\quad \text{Rate} = \text{Rate} + \lambda - \mu;\\
&\quad x[i] = \frac{1}{\text{Rate}} + \frac{x[i+1]\cdot(n-1)\cdot\lambda}{\text{Rate}\cdot z[i+1]};\\
&\quad y[i] = \frac{i\cdot\mu}{\text{Rate}};\\
&\quad z[i] = 1 - \frac{y[i+1]\cdot(n-1)\cdot\lambda}{\text{Rate}\cdot z[i+1]};\\
&\text{done}\\
&\text{MTTFF} = \left[\frac{z[1]}{z[1]-y[1]}\right]\left(\frac{1}{n\cdot\lambda}\right) + \frac{x[1]}{z[1]-y[1]};
\end{aligned}$$

The algorithm has linear time complexity, *i.e.*, *O*(*n*–*k*). It should be noted that at any time we need to store only one value of x_i, y_i, and z_i. Hence, to improve the MTTFF algorithm we can eliminate the arrays to reduce the storage requirements.

Algorithm 8: Storage Efficient MTTFF Computation

$$\text{Rate} = k \cdot \lambda + (n-k) \cdot \mu;$$

$$x = \frac{1}{\text{Rate}}; \quad y = (n-k) \cdot \mu \cdot x; \quad z = 1;$$

for $i = (n-k-1)$ downto 1 do

$$\text{Rate} = \text{Rate} + \lambda - \mu;$$

$$x = \frac{1}{\text{Rate}} + \frac{x \cdot (n-1) \cdot \lambda}{\text{Rate} \cdot z};$$

$$z = 1 - \frac{(i+1) \cdot \mu \cdot (n-i) \cdot \lambda}{z};$$

done

$$\text{ymod} = z - \frac{\mu}{\text{Rate}};$$

$$\text{MTTFF} = \frac{z}{y \bmod}\left(\frac{1}{n \cdot \lambda}\right) + \frac{x}{y \bmod};$$

21.5.3 Reliability with Repair

In some cases, we may be interested in finding the reliability and failure rate of a *k*-out-of-*n* system with repairable components. When both failure and repair distributions are exponential, we can find the reliability and failure rate of the system using Markov chain solutions. However, solutions to the Markov chains are computationally expensive. Using the Vesely failure rate [5], we present an efficient approximation to compute the reliability and failure rate of the *k*-out-of-*n* system with repairable components. For exponential failure and repair distributions, the following approximations provide an upper bound on the average failure rate and a lower bound on the system reliability.

$$h(t) \approx \frac{\omega(t)}{A(t)}; \quad R(t) \approx \exp\{-h(\infty) \cdot t\} \qquad (21.26)$$

Using the algorithms presented in Section 21.4, the approximate reliability and failure rate of the system can be found with $O(kn)$ or $O(n)$ algorithms. In [5], it has been shown that the above approximation is efficient as compared to other known approximations.

21.5.4 Suspended Animation

In most practical cases, non-failed components are kept idle to eliminate further damage to the system [14]. This is known as suspended animation (SA) [22]. Suspended animation introduces dependencies among the component states. Angus [6] derived a formula of the steady-state MTBF of the *k*-out-of-*n* system with identical components with exponential failure and repair distributions, assuming that no other failures will occur when the system is down, *i.e.*, to say, all working components are suspended when the system is down. Recently, Li *et al.* [14] presented generalized results for repairable *k*-out-of-*n* system with non-identical components subjected to exponential failure and repair distributions, assuming that no other failures will occur when the number of failures in the system reaches *d*, where $d \geq n-k+1$. Although the formulas in [14] are general and correct, a direct evaluation of these formulas takes a longer time to compute the results. In the worst case, the computational time increases exponentially with the number of components *(n)*. Therefore, in this chapter, we simplify the results presented in [14] and propose an efficient algorithm.

Additional Assumptions:

1. All non-failed components are kept idle once the number of failures reaches a certain limit.
   - Non-failed components are not suspended immediately after the system failure, but after reaching a certain level of failures (say $d \geq n-k+1$ failures). A special case of this model includes $d = n-k+1$, where all non-failed components are suspended immediately after reaching a system failure, i.e,. no failure occurs when the system is down.
2. Both failure and repair distributions of the components are exponential.
3. The components can be identical or non-identical, but are *s*-independent. The only dependency among the component states is due to the suspended animation.

The steady-state availability (A_{sa}) and failure frequency (ω_{sa}) of the *k*-out-of-*n* system subjected to suspended animation can be expressed as [14] follows.

$$A_{sa} = \frac{A(k)}{A(n-d)}; \quad \omega_{sa} = \frac{\omega(k)}{A(n-d)} \qquad (21.27)$$

where $A(k)$ and $v(k)$ are the steady-state availability and failure frequency of the *k*-out-of-*n* system without considering the suspended animation. Similarly, $A(n–d)$ is the steady-state availability of the (*n*–*d*)-out-of-*n* system without suspended animation. Using the algorithms presented in Section 21.4, we compute $A(k)$, $A(n–d)$, and $\omega(k)$, with $O(kn)$ time complexity (using only a single pass). Therefore, we can compute A_{sa} and ω_{sa} with $O(kn)$ time complexity algorithms. For identical cases, the complexity reduces to $O(n)$ or better. Once we know A_{sa} and ω_{sa}, all other measures, including MTBF, MUT, and MDT, can easily be found from (21.1).

21.6 Conclusions and Future Work

In this chapter, we presented efficient algorithms for computing various indices of repairable and non-repairable *k*-out-of-*n* systems. The algorithms presented are not limited to exponential failure and repair distributions. Hence, they can be applied to a wide range of failure and repair distributions, including frequently used distributions such as Weibull, Raleigh, gamma, Erlang, and extreme value. In addition to exact results, we also presented some computationally efficient approximations and bounds. The bounds are particularly important to finding the MTTFF, failure rate, and reliability of *k*-out-of-*n* systems with repairable components. We also discussed the case of suspended animation and its steady-state availability measures. All algorithms presented in this chapter can be computed with $O(kn)$ time complexity. For the identical component case, the time complexity reduces to $O(n)$. All algorithms presented in this chapter, except the suspended animation case, are implemented in Relex RBD [20]. We are currently working on some generalizations to suspended animation that include general failure and repair distributions and general renewal processes (imperfect maintenance).

References

[1] Amari SV, Misra KB, Pham H. Reliability analysis of tampered failure rate load-sharing *k*-out-of-*n:*G systems. Proc. 12th ISSAT Int. Conf. on Reliability and Quality in Design 2006; 30–35.

[2] Amari SV, Pham H, Dill G. Optimal design of *k*-out-of-*n*:G subsystems subjected to imperfect fault-coverage. IEEE Trans. on Reliability 2004; 53: 567–575.

[3] Amari SV. Generic rules to evaluate system-failure frequency. IEEE Trans. on Reliability 2000; 49: 85–87.

[4] Amari SV. Addendum to: Generic rules to evaluate system-failure frequency. IEEE Trans. on Reliability 2002; 51: 378–379.

[5] Amari SV, Akers JB. Reliability analysis of large fault trees using the Vesely failure rate. Proc. of IEEE Annual Reliability and Maintainability Symp., Los Angeles, CA, Jan. 2004; 391–396.

[6] Angus JE. On computing MTBF for a *k*-out-of-*n*:G repairable system. IEEE Trans. on Reliability 1988; 37: 312–3131.

[7] Barlow RE, Heidtmann KD. Computing *k*-out-of-*n* system reliability. IEEE Trans. on Reliability 1984; R-33: 322–323.

[8] Birnbaum ZW, Esary JD, Saunders SC. Multi-component systems and structures and their reliability. Technometrics 1961; 3: 55–77.

[9] Chang Y, Amari SV, Kuo S. Computing system failure frequencies and reliability importance measures using OBDD. IEEE Trans. on Computers 2003; 53: 54–68.

[10] Dharmaraja S, Amari SV. A method for exact MTBF evaluation of repairable systems. Proc. 10th International Conf. on Reliability and Quality in Design, ISSAT, Las Vegas, Aug. 2004; 241–245.

[11] Dutuit Y, Rauzy A. New insights in the assessment of *k*-out-of-*n* and related systems. Reliability Engineering and System Safety 2001; 72: 303–314.

[12] Koucky M. Exact reliability formula and bounds for general *k*-out-of-*n* systems. Reliability Engineering and System Safety 2003; 82: 287–300.

[13] Kuo W, Zuo MJ. Optimal reliability modeling, Chapter 7. Wiley, New York, 2003; 258–264.

[14] Li X, Zuo MJ, Yam RCM. Reliability analysis of a repairable *k*-out-of-*n* system with some components being suspended when the system is down. Reliability Engineering and System Safety 2006; 91: 305–310.

[15] Liu H. Reliability of a load-sharing *k*-out-of-*n*:G system: non-iid components with arbitrary distributions. IEEE Trans. on Reliability 1998; 47: 279–284.

[16] Misra KB. Reliability analysis and prediction: A methodology oriented treatment. Elsevier, Amsterdam, 1992.

[17] Press WH, Teukolsky SA, Vetterling WT, Flannery BP. Numerical recipes in C. Second edition, Cambridge University Press, 1992.

[18] Rangarajan S, Huang Y, Tripathi SK. Computing reliability intervals for *k*-resilient protocols. IEEE Trans. on Computers 1995; 44: 462–466.

[19] Ravichandran N. Stochastic Methods in Reliability Theory. John Wiley, New York, 1990.

[20] Relex RBD, http://www.relex.com/products/rbd.asp.

[21] Ross SM. On the calculation of asymptotic system reliability characteristics. In: Barlow RE. Fussell JB, Singpunvalla ND, editors. Reliability and fault tree analysis. SIAM, 1975; 331–350.

[22] Ross SM. Introduction to probability models. 8th edition; Academic Press, New York, 2003.

[23] Rushdi AM. Utilization of symmetric switching functions in the computation of *k*-out-of-*n* system reliability. Microelectronics and Reliability 1986; 26: 973–987.

[24] Rushdi AM. Reliability of *k*-out-of-*n* systems. In: Misra KB, editor. New trends in system reliability evaluation. Elsevier, Amsterdam, 1993; 16: 185–227.

[25] Singh C, Billinton R. System reliability modelling and evaluation. Hutchinson, London, 1977.

[26] Trivedi KS, Probability and statistics with reliability, queuing, and computer science applications. John Wiley, New York, 2001.

22

Imperfect Coverage Models: Status and Trends

Suprasad V. Amari[1], Albert F. Myers[2], Antoine Rauzy[3], and Kishor S. Trivedi[4]

[1] Relex Software Corporation, USA
[2] Northrop Grumman Corporation, USA
[3] Institut de Mathématiques de Luminy, France
[4] Duke University, USA

Abstract: Fault tolerance has been an essential architectural attribute for achieving high reliability in many critical applications of digital systems. Automatic fault detection, location, isolation, recovery, and reconfiguration mechanisms play a crucial role in implementing fault tolerance because a not-covered fault may lead to a system or subsystem failure even when adequate redundancy exists. The probability of successfully recovering from a fault given that the fault has occurred is known as the coverage factor or coverage and this is used to account for the efficiency of fault-tolerant mechanisms. If the fault and error handling mechanisms cannot successfully cover all faults in the system, then the coverage factor becomes less than unity and the system is said to have imperfect coverage. The models that consider the effects of imperfect fault coverage are known as imperfect fault coverage models or simply imperfect coverage models, fault coverage models, or coverage models. For systems with imperfect fault coverage, an excessive level of redundancy may even reduce the system reliability. Therefore, an accurate analysis must account for not only the system structure but also the system fault and error handling behavior, which is often called coverage behavior. The appropriate coverage modeling approach depends on the type of fault tolerant techniques used. In this chapter, we present the status and trends of imperfect coverage models, and associated reliability analysis techniques. We also present the historical developments, modeling approaches, reliability algorithms, optimal design policies, and available software tools.

22.1 Introduction

A system is called fault tolerant if it can tolerate most of the faults that can occur in the system. Therefore, a fault tolerant system functions successfully even in the presence of these faults [54]. In many critical applications of digital systems, fault tolerance has been an essential architectural attribute for achieving high reliability [2]. Fault tolerant designs are particularly important for computer and communication systems that are used in life-critical applications such as flight control, space missions, and data storage systems [9, 46, 54]. Fault tolerance is generally achieved by using redundancy concepts that utilize such techniques as error correcting

codes (ECCs), built-in tests (BITs), replication, and fault masking [54]. Automatic recovery and reconfiguration mechanisms, including fault detection, location, and isolation, play a crucial role in implementing fault tolerance because a not-covered fault may lead to a system or subsystem failure even when adequate redundancy exists [7]. This is because if a faulty unit is not reconfigured out of the system, it can produce incorrect results that contaminate the non-faulty units. For example:

- In computing systems, an undetected fault may affect the subsequent calculations and operations and then operate on incorrect data, possibly leading to overall system failure [63].
- An undetected leak carrying dangerous fluid may lead to a catastrophic failure. Similarly, an undetected fire in a component may affect the whole system. In computing systems, a virus-infected file may corrupt the whole system.

Similar effects can also be found in load-sharing systems [1], power distribution systems [2], communication and transmission systems [33, 37], and data storage systems [40]. Therefore, it is important to consider the effects of not-covered faults on the functionality, safety, and security of fault-tolerant systems.

Systems subject to imperfect fault coverage may fail prior to the exhaustion of spares due to not-covered component failures [24]. In addition, an excessive level of redundancy may reduce the system reliability [4, 30, 60]. Therefore, an accurate reliability analysis of these systems is important. This analysis must consider the fault and error handling behavior in addition to the system structure and its provision of redundancy [10, 24, 29, 59, 61].

The appropriate coverage modeling approach depends on the type of fault tolerant techniques used and the details available on the error handling mechanism. The models can be broadly classified as: (1) component level fault models, and (2) system level reliability/dependability models. The component level fault models are used to describe the behavior of the system in response to a fault in each component. These models are further classified as single-fault models and multi-fault models. The system level reliability models are used to describe the behavior of the entire system, which includes the effects of component level faults on the system structure and its provision for redundancy.

Section 22.2 discusses a brief history of solution methods and related software tools. Section 22.3 presents a general description of component level fault models, which are also known as fault/error handling models (FEHM). Section 22.4 presents specific details of various single-fault coverage models. Similarly, Section 22.5 presents the details of various multi-fault models. Section 22.6 discusses the Markov models for evaluating the system reliability. Sections 22.7 and 22.8 present the combinatorial solutions to compute the system reliability measures using single-fault models and multi-fault models respectively. Section 22.9 briefly describes the policies for optimal design of systems subjected to imperfect fault coverage. Finally, Section 22.10 presents the conclusions and future work.

22.2 A Brief History of Solution Techniques

The seminal paper by Bouricius *et al*. [12] (1969) first defined coverage, also called the coverage factor (CF), as a conditional probability to account for the efficiency of fault-tolerant mechanisms.

$$\text{Coverage} = \Pr\{\text{system recovery} \mid \text{fault occurs}\} \tag{22.1}$$

This concept has been rapidly and widely recognized as a major concern in dependability evaluation studies. Since then a vast amount of work has been devoted to refining the notion of coverage [8, 13] to the identification or estimation of relevant parameters [20] and associated component-level and system-level reliability models [9, 59]. As a result, several modeling tools and techniques have been developed [27, 31].

22.2.1 Early Combinatorial Approaches

Early approaches to reliability analysis of fault tolerant systems were based on a combinatorial method first discussed by Mathur and Avizienis [41], where the reconfiguration mechanism was assumed to be perfect. Bouricius *et al*. [12] extended this model to allow the reconfiguration mechanism to have an imperfect coverage. As an embodiment of this notion, the CARE program was developed at JPL as a computer-aided reliability evaluation package [56].

22.2.2 State-Space Models

In the early approaches, fault coverage was assumed to be a single number, whereas in practice, the times to detect isolate, and recover from a fault are non-zero random variables. Furthermore, these quantities depend on the current state of the system. As a result, combinatorial models, such as static fault trees and reliability block diagrams (RBDs), cannot be used to accurately model the system behavior. Further, combinatorial models cannot adequately model the sequence-dependent failure mechanisms associated with spares management, changing working conditions, and so on. Demands for increased accuracy in reliability estimation quickly forced the development of more elaborate system models without the vastly simplifying independence assumptions [27].

For this reason, many modelers turned to Markov chains for reliability assessment of fault tolerant systems. Markov chains are extremely flexible and they can capture the fault coverage mechanism quite well. As a result, reliability analysis tools, such as ARIES [48] and CAST [19], arose based on Markovian methods, thereby allowing the important first-order dependence.

22.2.3 Behavioral Decomposition

In addition to computational complexity, a major disadvantage of Markov chains (state-space models) is that it is difficult to determine the correct Markov model for a given system. This is because the modeler must specify each operational configuration of the system explicitly and determine the rate at which the system changes from one state to another. However, the relative advantages of combinatorial models (fault trees and RBDs) and Markov models have been exploited by using two key techniques: a) behavioral decomposition [58], and b) automatic conversion of a combinatorial model to an equivalent Markov model [10, 14, 59]. These methods were used in CARE III [56] and are enhanced in HARP [9, 10, 29].

HARP (hybrid automated reliability predictor) offers two classes of fault/error handling models (FEHMs): single-fault models and multi-fault models. In the single-fault model, the uncovered (not-covered) failure may lead to the entire system failure. Hence, this event is called a single-point failure. The HARP multi-fault model is limited to near-coincident (critical-pair) failures where the total system failure occurs as a result of two coexisting (not simultaneously occurring) faults. The near-coincident failure condition occurs when the system has already experienced one fault and is in the process of recovering from it when a second statistically independent fault occurs in another unit that is critically coupled to the unit experiencing the first fault. However, if a second fault occurs during recovery in a unit that is not critically coupled, the second fault is not accounted for in the coverage computation. This second fault is accounted for in the redundancy exhaustion model. An example of critically coupled units is a flight control system in a fly-by-wire aircraft. Two units in a voting triad perform a computation required for survival of the system. While HARP is capable of modeling systems that can tolerate only one critical fault, XHARP [28] removes the critical pair restriction. XHARP is capable of supporting exact multi-fault modeling.

22.2.4 The DDP Algorithm

Although the decomposition technique used in HARP reduces the computational time and the state space, Markov chains are still used for reliability evaluation. Using a combinatorial

solution, imperfect coverage in a combinatorial model of VAXcluster systems was first introduced in [30]. Later, a similar concept for general configurations is proposed in the DDP (Doyle, Dugan, and Patterson) algorithm [22]. According to the DDP algorithm as long as the system failure logic is represented using a combinatorial model (static fault tree or RBD), the inclusion of uncovered (not-covered) single-point failures does not require a complex Markov chain-based solution. Instead, the DDP algorithm combines aspects of behavioral decomposition, sum-of-disjoint products (SDP), and multi-state solution methods.

22.2.5 Simple and Efficient Algorithm (SEA)

SEA [5] further develops and then generalizes the DDP algorithm by eliminating the need for cut-set solution methods and multi-state solution methods. The advantage of SEA is that it can be used with any combinatorial solution technique that ignores fault coverage, such as grouped variable inversion techniques, modular fault tree techniques, solutions of reliability block diagrams (array structures), and the latest algorithms including binary decision diagrams (BDD) [16, 51]. A reliability engineer can use, without modification, any software package that employs a combinatorial model that does not consider imperfect fault coverage, and by simply altering the input and output, produce the reliability of a system with imperfect fault coverage.

Two main advantages of SEA are that: (1) it can convert a fault coverage model into an equivalent perfect coverage model in a linear time, and (2) it can produce simple closed-form solutions for all well-structured systems. As a result, the computational complexity of an imperfect fault-coverage model is reduced to its equivalent perfect fault-coverage model, which in turn proves that it is difficult to find a better algorithm than SEA (if the uncovered failure is caused by single-point failures). The closed-form solutions help one to study the system in detail and find efficient algorithms for finding optimal system designs [4]. The basic idea of SEA has gained the attention of several research groups, and it has been extended and applied for a wide range of systems, applications, and techniques [16, 18, 64, 66, 67]. Most of these research works are included in the Galileo fault tree analysis package [25].

22.2.6 Multi-fault Models

The SEA and DDP algorithms and their extensions only consider single-point uncovered failures (caused by single-fault models), where the coverage probability at a component failure is solely dependent on the properties of the failed component. Little progress has been made in analyzing multi-fault models. HARP and XHARP use Markov chains for solving multi-fault models. Amari [1] proposed a simple combinatorial model to compute the reliability of k-out-of-n systems with identical components subjected to multi-fault (concurrent faults) coverage models. Recently, Myers [44] once again emphasized the need for these multi-fault models, also called fault level coverage (FLC) models, and proposed a combinatorial solution to evaluate the reliability of these systems. It should be noted that the element level coverage (ELC) models in [44] are equivalent to the single-fault coverage models in HARP [9].

Recently, several refinements and approximations to the Myers method have been proposed [6, 45, 46]. Some of these methods are incorporated in the reliability analysis tool Aralia [53]. Further, the concept of multi-fault coverage models are also extended to the multi-state systems and performance dependent coverage models [35–37].

22.3 Fault and Error Handling Models

In order to accurately model the reliability of fault-tolerant systems, it is important to know how the system behaves in response to a fault. The models that describe the system behavior in response to a fault are known as fault/error handling models (FEHM) or the coverage models. In order to describe these models, we borrow some terminology from [8, 23].

A system failure occurs when the delivered service deviates from the specified service. An error is that part of the system state which is liable to lead to failure; the cause of an error is a fault. A fault can be a programmer's error, a short circuit, electromagnetic perturbation, *etc*. Upon occurrence, a fault creates a latent error, which becomes effective when it is activated. When the error affects the delivered service, a failure occurs.

The time constants associated with cycling of the error between the effective and latent states determine if the error is considered permanent, intermittent, or transient. If an error, once activated, remains effective for a long time relative to the time needed to detect and handle it, it may be considered permanent. If the error cycles relatively quickly between the active and latent states, it may be considered intermittent. If the error, once activated, becomes latent and remains latent for a long time, it may be considered a transient. For details on the classification of faults, refer to [23].

The recovery mechanisms periodically monitor the components for the identification of faults and errors. When the faults and errors are identified, depending on the type and status of the fault, the recovery process initiates the sequence of actions that include fault location, isolation, and restoration. The detailed description of this recovery process is specified using an appropriate FEHM. The general behavior of FEHM is described in Figure 22.1. The entry point to the model signifies the occurrence of the fault, and the four exits signify the four possible outcomes.

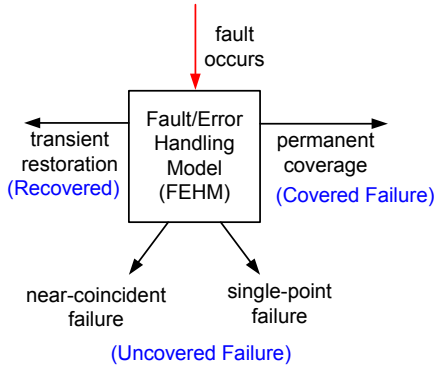


Figure 22.1. General structure of FEHM

If the offending fault is transient, and it can be handled without discarding the component, a transient restoration takes place, and the component returns to its normal working state. If the fault is determined to be permanent, and the offending component is discarded, a permanent fault recovery takes place, and the component is considered to be in the covered failure mode (safe failure mode). If the recovery mechanism is unable to detect, locate, or isolate the fault, the fault may lead to a coverage failure. If the fault by itself causes the system to fail, a single-point failure is said to take place. However, depending on the type of fault-tolerant mechanisms used, some systems can tolerate multiple undetected or non-isolated (non-removed) faults. If the number of such concurrent faults that interfere with the identification and recovery process of each other exceeds the tolerable limit of the system within an identification and recovery window (or simply called recovery window), the system fails in a multi-fault uncovered mode (not-covered mode). If the system can tolerate only one non-isolated fault at a time, the occurrence of a second fault that interferes with the recovery process of the first fault can cause an uncovered failure, which is called a near-coincident failure.

Once the fault occurs, it leads to one of the four possible outcomes or consequences:

- Transient restoration (R)
- Permanent coverage (C)
- Single-point failure (S)
- Near-coincident failure (N)

In the context of FEHM, these consequences are also called exits. In order to analyze the overall system reliability, it is important to calculate these exit probabilities: P_r, P_c, P_s, and P_n [23, 58]. The exit probabilities depend on the fault occurrence rate (λ) and effectiveness of actions that are performed after the occurrence of the fault. Assume that p_r, p_c, p_s, and p_n are the conditional probabilities of exits R, C, S, and N, respectively given that the fault has occurred. These exits are mutually exclusive. Hence, we have:

$$p_r + p_c + p_s + p_n = 1. \qquad (22.2)$$

It should be noted that both the transient restoration (R) and permanent coverage (C) are considered to be the successful actions of the fault-handling mechanisms. Hence, from the definition of coverage factor (CF) in (22.1), we have:

$$CF = p_r + p_c = 1 - (p_s + p_n). \qquad (22.3)$$

Hence, in general, we have: $CF \neq p_c$. However, in order to simplify the analysis, we may ignore the events of fault activations that lead to the R exit. This is because the overall system state is unchanged with these events. Therefore, the effective failure rate of the system becomes $\lambda_{\text{eff}} = (1 - p_r)\lambda$. If we consider only the events that are accounted for the effective fault occurrence rate, the new exit probabilities become: $p_c' = p_c/(1-p_r)$, $p_n' = p_n/(1-p_r)$, and $p_s' = p_s/(1-p_r)$. Hence, in this case, we have: $CF = p_c'$.

Most published papers assume that the conditional exit probabilities are independent of the fault occurrence rate (λ). Therefore, the exit probabilities over a mission time t can be calculated by multiplying these conditional probabilities with the fault occurrence probability: $q = 1 - \exp(-\lambda_{\text{eff}} t)$. Hence, we have: $P_c = q.p_c'$, $P_s = q.p_s'$, and $P_n = q.p_n'$. However, the independence assumption is not valid when near-coincident (or coexisting) failures are present. This is because the occurrence of a near-coincident failure depends on the occurrence rate of another fault in a related component that interfaces with the identification and recovery process of the first fault.

In the majority of research papers on imperfect fault coverage models, the near-coincident faults are not considered [2, 4, 5, 16, 43, 49, 57, 64]. In this case, we have: $p_n = 0$. This assumption is valid only if identification and recovery of a faulty component is independent of the status and information available at any other component. In such cases, the identification and recovery process of a faulty component typically utilizes its built-in test (BIT) capability. Hence, the coverage factor can be considered as a property of that component (element). Therefore, Myers [44] called these models element-level coverage (ELC) models. Because the recovery processes of faults are independent of each other, in HARP these models are known as single-fault coverage models or simply single-fault models. It should be noted that the system subject to single-fault coverage models can perform identification and recovery of multiple faults simultaneously. However, all these recovery processes are assumed to perform independently.

When the identification and recovery process of multiple faults interfere with each other, these models are called multi-fault coverage models or simply multi-fault models [9]. The recovery capabilities of multi-fault models within a recovery and reconfiguration window depend on: (1) the number of known or isolated faults before the recovery window, and (2) the number of new faults occurred in a specific group of components within the recovery window. In these models, the status of each component is compared with the status of other components using predetermined rules (majority voting or mid-value-select voting) to identify the failed components. In some cases, it is possible to correct the faulty components using the information gathered from the existing good components. Examples of this kind include recovery processes used in computer storage and communication applications [54]. Because the recovery capability of a multi-fault coverage model depends on the number of faulty (good) components in a specific group of components, Myers [44] called these models fault-level coverage (FLC) models. The corresponding groups of components are known as FLC groups [6].

When the number of good components within an FLC group is reduced to two, we cannot use majority voting or mid-value-select voting schemes. In this case, the faults in the components may be determined using built-in-tests (BIT). Considering this situation, Myers [44] also proposed a special case of FLC model called the one-on-one level coverage (OLC) model. In this model, the coverage factor is assumed to be unity when the number of good components in a specific FLC group is greater than 2. The rational behind this assumption is that when mid-value-select voting is used, it is almost certain to identify or correct all faulty components as long as the number of good components at the beginning of each recovery window is greater than 2.

At the first glance, we may incorrectly think that single-fault coverage models are efficient as

compared to multi-fault coverage models because the recovery of single-fault models is independent of the co-existing faults in multiple components. As a contradiction to the above intuition, the multi-fault models are efficient, because the identification and recovery of a fault in a component is performed not only using the information of the faulty component but also from the information available in the other good components. In addition to this, the recovery window is generally very small and the probability of multiple fault occurrences within a recovery window is very small. At the same time, in order to accurately analyze the ultra-high reliability systems, we should not ignore the probabilities of multiple faults that defeat the fault-tolerant mechanisms.

22.4 Single-fault Models

In the previous section, we considered a high-level view of FEHM model. In this section, we consider other details that are important to calculate the exit probabilities associated with the FEHM model that are subsequently used to calcuate the coverage probabilities and the overall system reliability measures [53, 57, 58]. Particularly, in this section, we describe the details of various single-fault coverage models proposed in the literature, starting with simplest phase-type models and proceding to complex ones. An appropriate model may depend on the available details on the system behavior. For a system that is still in the design phase, the details of the error handling mechanism may not be known. In such a case, the modeler would be best served by the simple coverage model. As the design progresses, the simple coverage model can be refined. Dugan and Trevedi [23] proposed a methodolgy that allows successive replacement of one coverage model with another within the overall system dependability model, also called the system-level reliability model. In addition to this, the separable method proposed in [5], separates the component-level coverage model (FEHM) from the system-level reliability model and proposes a simple and efficient algorithm (SEA).

As shown in the general structure of FEHM in Figure 22.1, these models have single entry and multiple exits. In addition to this, the FEHM box may contain some internal states. Depending on the details available, the interaction between the states can be modeled using discrete-time Markov models, continuous-time Markov models, semi-Markov models, or non-homogeneous Markov models [57].

22.4.1 Phase Type Discrete Time Models

These models assume that the recovery process takes place in phases and the time spent in each phase is negligible (or not considered). Hence, the FEHM can be represented using discrete-time Markov chains (DTMC). When we consider only the permanent errors, a three phase FEHM with detection, location, and recovery might appear as in Figure 22.2 [57, p. 269]. Each of the three FEHM phases is associated with a probability of success. Hence, the overall probability of successful system recovery is given by the product of success of individual phases (c_d, c_l, and c_r).

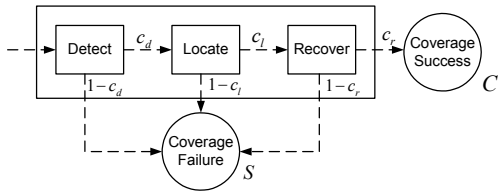


Figure 22.2. Phases of error handling

22.4.2 General Discrete Time Models

In the general discrete models, the recovery process is not restricted to phase type (sequential stages) actions and it may contain loops or backward transitions. Therefore, a state in the FEHM can be revisited. These models are applicable to specify transient restorations, transitions between latent and active fault states, and intermittent errors. Let $P = [p_{ij}]$ be the transition probability matrix of the DTMC. Here, p_{ij} is the probability that the next state will be state j given that the current state is i. Let r_{ij} be the probability of reaching an exit state j from an error

handling state i and let the matrix $R = [r_{ij}]$. Then the matrix of eventual exit probabilities given an entry state is $([I - P]^{-1}R)$ [23].

22.4.3 The CAST Recovery Model

This model is proposed in [19] and it is a DTMC model with a backward transition. This model combines the notion of transient restoration with a permanent recovery model into a single model as shown in Figure 22.3.

The entry to model represents an activation of an error (or a fault) with a total rate of λ (permanent rate) + τ (transient rate). They are detected with probability u.

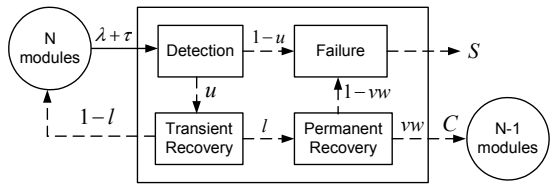


Figure 22.3. CAST recovery model

It conservatively assumes that the failure to detect the error leads to system failure. After detection, transient recovery is attempted and it is successful with probability 1-l (the component returns to its normal working condition). If transient recovery is unsuccessful, a permanent recovery is initiated where the cause of error (fault) is identified with probability v. Once the cause is identified, the system recovers with probability w. The successful permanent recovery removes the faulty component from the system. The unsuccessful permanent recovery leads to system coverage failure (also called uncovered system failure).

22.4.4 CTMC Models

These models assume that the details of FEHM can be represented using continuous-time Markov chains (CTMC). Let the transition matrix $Q = [q_{ij}]$ where q_{ij} is the rate of transition to state j given that the current state is the state i. Let r_{ij} be the rate of transition to an exit state j from an error handling state i and let the matrix $R = [r_{ij}]$. Then the matrix of eventual exit probabilities given an entry state is given by $([- Q]^{-1}R)$ [11, 23, 57]. Several CTMC type FEHM are proposed in the literature. These details are given in the following sections. The dotted lines in these diagrams indicate instantaneous transitions. If there are mutiple outward dotted transitions from a sigle state, then discrete probabilities are used to specify the next state of the FEHM model.

22.4.5 The CARE III Basic Model

This model is proposed in [56] and it is a CTMC model. The model is shown in Figure 22.4. In this model, state A is entered on activation of the fault. The fault is detected with constant rate δ (state D). Once detected the system removes the faulty unit and continues processing (state P). Before detection, the fault can produce an error with constant rate ρ (state E) or can become latent with rate α (state B). The latent fault once again becomes active with rate β. In state E, the error can be detected with probability q and if so the presence of the fault is recognized and recovery can still occur (with rate ε).

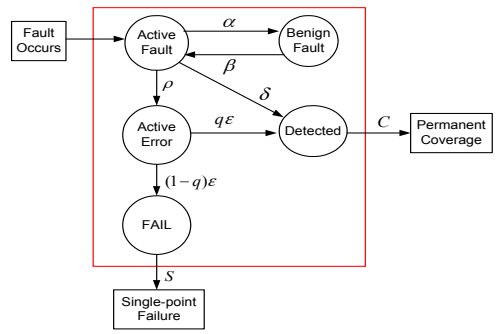


Figure 22.4. CARE III basic model

This model can be used to represent either permanent faults (always effective) or intermittent faults. The permanent faults are represented in this model by setting α and β to zero. To represent intermittent faults both α and β should be positive.

In this model, the probability of taking exit C (reaching state D) is equivalent to the coverage factor. Because state A is the initial state of the model, coverage is equivalent to the exit

probability from state A to the state D. Hence, we have [57]:

$$c = \frac{\delta}{\delta+\rho} + \frac{q\rho}{\delta+\rho} = \frac{\delta+q\rho}{\delta+\rho}. \qquad (22.4)$$

It should be noted that the coverage factor of this model is independent of the parameters: α, β, and ε. As shown [23, 58], in order to compute the system reliability, we need to calculate only the coverage factor from the FEHM. Therefore, the model can be simplified by removing "benign fault state" and setting $\varepsilon = 1$.

22.4.6 The CARE III Transient Fault Model

The CARE III transient model is a generalization to the CARE III basic model and it allows specifying the effects of transient restoration. This model can be used to model transient, intermittent, or permanent faults. In the active state, a fault is both detectable (with rate δ) and capable of producing an error (with rate ρ). Once an error is produced, if it is not detected, it propagates to the erroneous output (with rate ε) and causes system failure. If the fault (error) is detected (with probability q), the faulty element is removed from service with probability P_A when the fault is active or P_B when the fault is benign. With the complementary probabilities, *i.e.*, 1-P_A or 1−P_B, the element is returned to service following the detection of the fault. The model can be specialized to permanent, transient, or intermittent cases. For the permanent model, $\alpha = \beta = 0$, and $P_B = 0$. For the transient model, α is positive and $\beta = 0$. For the intermittent model, both α and β are positive, these rates are fast in relation to the overall model (fault occurrence rates).

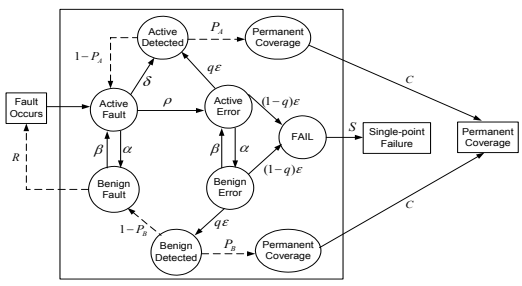


Figure 22.5. CARE III transient model

22.4.7 ARIES Models

The ARIES coverage model was proposed by Makam and Avizienis [48] and it allows the transient restoration. This is a phased recovery model that allows the user to specify how many phases comprise the recovery process. The duration of each phase is constant. The model has three possible eventual exits: system crash (exit S), normal processing (exit R), and permanent fault recovery (exit C). In each phase of the recovery, the system attempts the recovery. If successful, the system returns to the normal processing state without discarding any components. If the recovery in a particular phase is unsuccessful, the next phase attempts to locate and recover from the fault. If all phases are ineffective, the fault is assumed to be permanent. Hence, the component is discarded and system continues its functions with one fewer component provided that redundancy of the system is not exhausted.

22.4.8 HARP Models

HARP supports several single fault models. They include:

1. The no coverage model: This model is used to specify perfect coverage.
2. The value model: In this model, without specifying the detailed behavior of FEHM, the user can specify the probabilities of taking the exits (R, S, and C) directly.
3. The ARIES model.
4. The CARE III model.

In addition to this, HARP also supports the following models.

5. The ESPN model.
6. The probabilities and moments model.
7. The probabilities and distribution model.
8. The probabilities and empirical data model.

The probabilities and distribution model in HARP can be considered as a generalization to the limited

recovery model discussed in [23]. The limited recovery model is applicable for real-time systems, where there may be a time limit within which recovery actions must be completed in order to be considered successful. Assume that the time to perform recovery is exponentially distributed with rate parameter δ, and that recovery is always successful. In the case where there is no limit on the recovery time, the coverage probability is unity. If there is a time limit T on the recovery process, then the coverage probability is given by: $c = \Pr\{\text{recovery time} \leq T\} = 1\text{-}\exp\{\text{-}\delta T\}$. For a more general case, see [57, Section 5.4].

22.5 Multi-fault Models

The need for the multi-fault models arose due to the complex interactions between recovery procedures of multiple faults. In fact, for fly-by-wire aircraft designs such as SIFT and FTMP, it was claimed that all single-point failures were eliminated. Hence, it was thought that near-coincident faults will be the major cause of system failure. The detailed modeling of multiple faults can be computationally expensive and tedious to specify [14, 57]. In addition, the modeling requires the user to input data that are typically unavailable. Therefore, the developers of HARP and other researchers proposed some simple specifications of these models. Although the disadvantage is a reduction in accuracy, published work has demonstrated that the error due to the use of simple models is typically acceptable [9, 42].

22.5.1 HARP Models

HARP supports three simple multi-fault coverage models to automatically incorporate the effects of coexisting faults. All these models are restricted to near-coincident faults.

1. The ALL-inclusive near-Coincident model: In this model, the recovery of a fault is performed as per the single-fault model specified for the individual components. During this recovery process if any other component fails, the system is considered to be failed in the uncovered mode (not-covered mode). In order to include this effect, HARP adds a dummy state between two original states (state i and state j) of the generated Markov model.
2. The SAME-type near-coincident model: This is similar to the ALL-inclusive model, except that the system fails in the uncovered mode only if a similar component fails during the recovery process of the first failure. This model is similar to the model used in [6, 44].
3. USER-defined near-coincident model: This model allows the user to specify, for each component, which other components can interfere with the fault recovery. For example, suppose we have a system consisting of three processors (P1, P2, and P3), a voter V, and a bus B. Suppose further that the processors are connected in a ring network so that processor P1 detects errors and performs recovery for processor P2, processor P2 likewise monitors processor P3, and P3 monitors P1. Thus the failure in processor P1 can interfere with recovery in P2. Similarly, a failure on processor P2 can interfere with recovery in processor P3. Because the processors are connected by the data bus, a bus failure can interfere with recovery on any of the processors. The bus does not relay on any other component for recovery. The voter is self-checking; no faults interfere with recovery from voter faults.

In addition to this, HARP also supports manual specification of exact near-coincident faults.

22.5.2 Exclusive Near-coincident Models

In some cases, we may wish to consider the uncovered (not-covered) failures that are only caused by the occurrence of coexisting faults. In this case, we are ignoring the possibility of single-point failures. This means that the recovery process is perfect as long as there are no coexisting faults within a recovery window. The following approaches can be used to model only near-coincident failures.

1. Exponentially distributed recovery time: In this model, the recovery of a fault is considered to be perfect as long as there is no second fault within a recovery window. The recovery time (window) follows exponential distribution with rate δ. In order to calculate the coverage factors, consider a 1-out-of-3 system subjected to near-coincident faults. The coverage factor at the first fault is calculated as the probability to complete the recovery of that fault before the occurrence of the second fault, which can occur with rate 2λ. Hence, the coverage at the first fault is $c_1 = \delta/(\delta+2\lambda)$. Refer to Fig. 22.6. Similarly, the coverage at the second fault is $c_2 = \delta/(\delta+\lambda)$. This model is discussed in [23, 38, 57].

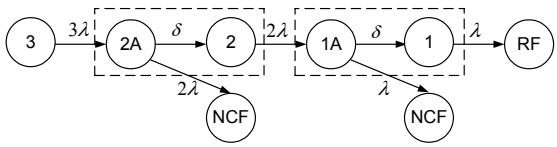


Figure 22.6. Near-coincident model

2. Fixed recovery time: This is the same as the previous model, except that the recovery window time is fixed. Let τ be the recovery window time. During the first failure, any one of the remaining (n-1) components can fail during τ and can cause the system failure. Extending the same logic for other cases, we have:

$$c_i = \exp[-(n-i)\lambda\tau]. \qquad (22.5)$$

   This is exactly the same model used in [1, 44] except for the last two faults where the coverage is calculated using single-fault models associated with built-in-test capabilities.
3. General recovery time: The above models can also be generalized for the general recovery time distribution. Refer to [56, 57] for details. A special case of this model is a phased recovery process discussed below.
4. Phased recovery process: This model is used in CARE [56]. In this model, the recovery of a fault follows a phase-type distribution. For example, consider a 1-out-of-3 system with two phases of recovery for each fault. The Markov model for this system is shown in Figure 22.7. Hence, the coverage factor at the first fault is $c_1 = [\delta/(\delta+2\lambda)]^2$. Similarly, the coverage at the second fault is $c_2 = [\delta/(\delta+\lambda)]^2$.

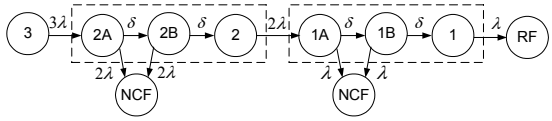


Figure 22.7. Phased recovery near-coincident model

22.5.3 Extended Models

Some generalizations to near-coincident fault models are proposed in [28] and the approach used to analyze these models is called extended behavioral decomposition. In this section, we discuss a specific near-coincident model considered in [28]. In this model, the recovery process attempts to fix the problems in each module (or similar components) at a time. It is assumed that as long as the recovery process is involved in fixing the problems in a specific module, the second or subsequent faults in that module does not lead to the near-coincident failure, but leads to the permanent coverage. However, during a recovery process in a particular module, if another fault occurs in some other module, the recovery process cannot handle that situation and leads to the near-coincident failure.

22.6 Markov Models for System Reliability

Sections 22.4 and 22.5 presented various single-fault and multi-fault models. Now we discuss how to integrate these coverage models into the overall system reliability analysis. For example, consider a 1-out-of-3 system. With perfect coverage, the Markov model of the system is shown in Figure 22.8.

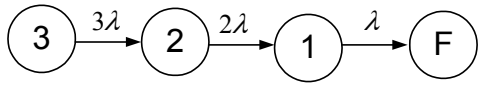


Figure 22.8. A 1-out-of-3 system with perfect coverage

In order to demonstrate the integration of coverage models into the system reliability model, we consider CARE III basic single-fault model. The coverage model will be initiated immediately after occurrence of a fault. Therefore, the coverage model is incorporated after each failure transition in the original Markov model. Hence, the overall system reliability model becomes as shown in Figure 22.9.

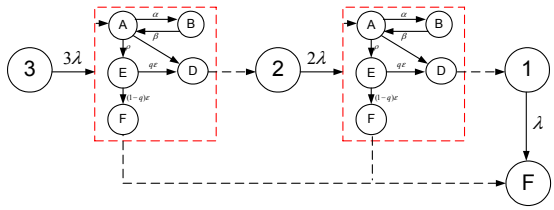


Figure 22.9. 1-out-of-3 system with CARE III basic single-fault model

We can also incorporate the effects of near-coincident faults in the overall system reliability model. For this purpose, assume that any additional failure during the recovery process leads to the near-coincident system failure. Hence, we add a near-coincident failure transition from each state of the recovery process. The procedure is the same for any combination of single-fault and near-coincident models.

The main problem with this approach is stiffness of the resulting Markov chain that contains both fast transition rates (recovery process) and slow transition rates (failure rates). Typically, the mean transition times in the recovery model are in seconds and the mean failure times are in hours. Hence, the difference in the transition rates is in the order of magnitude of 10^6. The numerical solutions of stiff Markov models are very difficult compared to non-stiff Markov models [11, 38, 39, 57]. Another disadvantage of this approach is the state space explosion of the Markov model due to the additional states that describe the details associated with recovery processes. In addition to these difficulties, this approach is inapplicable if the random variables of interest are non-exponentially distributed.

In order to overcome these difficulties, behavioral decomposition has been proposed [58]. This method is based on the fact that time constants of fault-handling processes are several orders of magnitude smaller than those of fault-occurrence events. It is therefore possible to analyze separately the fault-handling behavior of the system (the coverage model) and later incorporate the results of the coverage model, together with the fault-occurrence behavior, in an overall system reliability model. The fast transitions in the fault-handling model are replaced with instantaneous jump transitions. In this method, we first calculate the exit probabilities associated with FEHM [11]. For example, if we consider the CARE III basic single-fault model, we have two exits: C and S. The exit probabilities are:

$$c = \frac{\delta + q\rho}{\delta + \rho}; \qquad s = 1 - c = \frac{(1-q)\rho}{\delta + \rho}. \quad (22.6)$$

Using these exit probabilities as the instantaneous transition probabilities, we can reduce the Markov chain as shown in Figure 22.10.

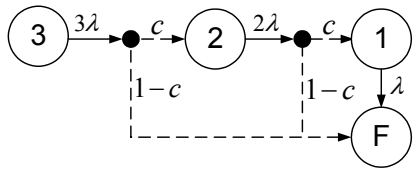


Figure 22.10. 1-out-of-3 system with instantaneous coverage probabilities

Now using the instantaneous jump theorem [28, 58], we can combine the transitions as shown in Figure 22.11.

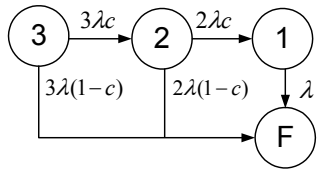


Figure 22.11. Simplified 1-out-of-3 system model with behavioral decomposition

The resulting Markov chain contains the same number of states as in the perfect coverage model

(see Figure 22.8). If we want to distinguish the failures as redundancy exhaustion failures (covered failures) and fault-handling failures (uncovered failures), we can split the failure state accordingly. Similarly, we can also use the behavioral decomposition for analyzing the near-coincident failures [56].

It is important to note that, as shown in [42, 55], the behavioral decomposition always produces conservative results for system reliability, which is a desired property in reliability analysis. In addition to this, the error in the approximation is negligible for any practical purpose. Therefore, this method is used in several software packages including CARE, HARP, and SHARPE [9, 27].

22.7 The Combinatorial Method for System Reliability with Single-fault Models

The decomposition method discussed in Section 22.6 reduces the state-space of a system subjected to imperfect fault coverage to that of a perfect coverage case. However, we still need to use the Markov chains for analyzing the imperfect coverage models even when there are no additional dependencies among the components except the dependencies introduced by the fault-handling processes. Therefore, irrespective of system redundancy mechanisms, the systems subjected to imperfect coverage need to be solved using Markov chains. The main disadvantage of Markov chains is its state-space explosion. Even for a moderate size practical system, the state-space of the Markov chain becomes huge. In order to overcome these difficulties, various approximations and bounds for Markov chains are proposed [15, 42, 57]. In addition to this, some special techniques have been developed to solve the Markov chains associated with the coverage models. They include automatic generation of Markov chains from combinatorial models and solving the Markov chains incrementally while generating them [1, 14, 24].

A major break-through in analyzing the imperfect coverage model came with the publication of the DDP algorithm [22]. According to [22], the system reliability can be computed using combinatorial solution methods when the following conditions are met.

- Component failures (fault occurrence) are statistically independent.
- If manual repair or restoration is applicable, then the restoration process of each component is independent.
- The fault-handling process of each component is independent of the states of other components, *i.e.*, faults do not interfere with each other. This means that there are no near-coincident or multi-fault failures.
- The system failure or success logic is represented using a combinatorial model when we ignore the failures associated with the fault-handling process. This means that when the coverage is perfect, we should be able to represent the system using traditional combinatorial models.

Because there are no near-coincident failures, each component is in one of the following states.

- Good: component is not failed, *i.e.*, working normally.
- Covered failure: component failure is correctly handled, *i.e.*, permanent coverage.
- Uncovered failure (not-covered failure): component failure is not correctly handled, *i.e.*, single-point failure.

Figure 22.12 shows the event space (and corresponding probability) representation of each component.

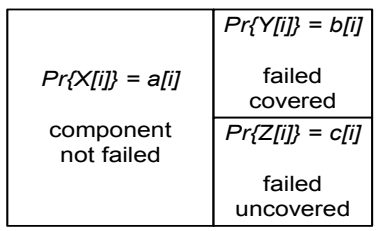


Figure 22.12. Event and probability space of a component

22.7.1 Calculation of Component-state Probabilities

In this method, we first calculate the state probabilities for each component. When there is no manual restoration after a permanent coverage, the state probabilities are calculated from the component reliability and fault coverage probabilities. Refer to [16] for calculating the state probabilities when there are manual restorations. Let $F_i(t)$ be the fault occurrence time distribution that ignores the events associated with transient restoration. It is nothing but component unreliability q_i. Hence, the component reliability is $p_i = 1-q_i = 1-F_i(t)$. Let c_i be the coverage factor of the component. Hence, we have:

$$a[i] = p_i; b[i] = c_i q_i; c[i] = (1-c_i)q_i . \quad (22.7)$$

As discussed in Section 22.3, we can also calculate these probabilities using the exit probabilities associated with FEHM. These calculations are demonstrated using the exponential failure distribution for fault occurrence times. Let λ_i be the combined failure rate (occurrence rate) of transient & permanent faults in component i. Let c_i, s_i, and r_i be the exit probabilities of FEHM corresponding to C, S, and R exits. The effective failure rate of component i is:

$$\gamma_i = (1-r_i)\lambda_i = (c_i + s_i)\lambda_i . \quad (22.8)$$

The failure rates $c_i\lambda_i$, $s_i\lambda_i$ lead to $Y[i]$, $Z[i]$ respectively. From Markov chains, we have:

$$\begin{aligned} a[i] &= \exp(-\gamma_i t) \\ b[i] &= \frac{c_i}{c_i + s_i}[1-\exp(-\gamma_i t)] \\ c[i] &= \frac{s_i}{c_i + s_i}[1-\exp(-\gamma_i t)] \end{aligned} \quad (22.9)$$

This type of equation is used in [24]. However, if $\lambda_i t$ is very small, it is reasonable to assume that at the most one fault can occur in a component during time t. Hence,

$$\begin{aligned} a[i] &= r_i[1-\exp(-\gamma_i t)] + \exp(-\gamma_i t) \\ b[i] &= c_i[1-\exp(-\lambda_i t)] \\ c[i] &= s_i[1-\exp(-\lambda_i t)] \end{aligned} \quad (22.10)$$

This type of equation is used in [22]. If $\lambda_i t \ll 1$, then $\exp(-\lambda_i t) \approx 1-\lambda_i t$, and (22.9) and (22.10) lead to the same results as in (22.11).

$$\begin{aligned} a[i] &= 1-(s_i + c_i)\lambda_i t \\ b[i] &= c_i \lambda_i t \\ c[i] &= s_i \lambda_i t \end{aligned} \quad (22.11)$$

22.7.2 The DDP Algorithm

The system fails in an uncovered mode due to the uncovered failure of any component. Hence, $Z[i]$ is a cut set of the system. Because this cut set contains only one variable (component state), it is also called singleton cut set. If system contains n components, then we have n singleton cut sets corresponding to an uncovered failure of each component.

$$C_i = Z[i] . \quad (22.12)$$

In addition to this, from the system failure logic, we can find the cut sets that represent the exhaustion of redundancy (covered failures). Let there are m such cut sets. These cut sets are represented using the combined events of $Y[i]$ states of different components. We label these cut sets as $C_{n+1},\ldots, C_{n+m}$. Hence, we have a total of $p = n+m$ cut sets. The system unreliability (U) is the probability of union of all these cut sets. Hence, we have:

$$U = \Pr\left\{\bigcup_{i=1}^{p} C_i\right\} \quad (22.13)$$

We cannot add the probability of each cut set to find the unreliability. This is because the cut sets are not disjoint except when $n = 1$. Therefore, [22] proposed a sum of disjoint products (SDP) algorithm to compute the system reliability. The SDP algorithm uses the following identity:

$$\begin{aligned} \bigcup_{i=1}^{p} C_i = C_1 \cup (\neg C_1 C_2) \cup (\neg C_1 \neg C_2 C_3) \cup \\ \ldots \cup (\neg C_1 \neg C_2 \neg C_3 \ldots \neg C_{p-1} C_p) \end{aligned} \quad (22.14)$$

to produce a set of disjoint events whose probabilities can be summed. Here, $\neg C_i$ represents the

negation of C_i and $\neg C_i C_j$ represents intersection of $\neg C_i$ and C_j. Hence, $\neg C_i C_j = (\neg C_i) \cap (C_j)$.

Now the task is reduced to find the probability of each product term in the SDP form. However, we should take a special care while expanding these terms, because each component in the system has three mutually exclusive states, *i.e.*, these are multi-state components. As in the traditional multi-state system (MSS) reliability analysis, we represent each state of the system with a Boolean variable. For example, $Y[i]$ is used to represent the covered failure of component i. The $Y[i]$ is true if the component i is failed in a covered mode; otherwise, it is false. Hence, $Y[i]$ is false if component i is either working ($X[i]$ is true) or failed in an uncovered mode ($Z[i]$ is true). Because the component states are mutually exclusive, exactly one of these variables ($X[i]$, $Y[i]$, and $Z[i]$) is true at a time. Therefore, the SDP terms that contain multiple terms corresponding to a component need to be eliminated. Hence, we use the following identities for simplifying the SDP terms.

$$\begin{aligned} \neg X[i] &= Y[i] \cup Z[i] \\ \neg Y[i] &= X[i] \cup Z[i] \\ \neg Z[i] &= X[i] \cup Y[i] \end{aligned} \tag{22.15}$$

and

$$\begin{aligned} X[i] \cap Y[i] &= \phi \\ X[i] \cap Z[i] &= \phi \\ Y[i] \cap Z[i] &= \phi \\ X[i] \cap Y[i] \cap Z[i] &= \phi \end{aligned} \tag{22.16}$$

To demonstrate this method, we consider a three-unit redundant system that is operational as long as at least one unit is operational, provided that no uncovered failures have occurred. The singleton cut sets that represent uncovered component failures are:

$$\begin{aligned} C_1 &= Z[1] \\ C_2 &= Z[2] \\ C_3 &= Z[3] \end{aligned} \tag{22.17}$$

The system fails in the covered mode if all components fail in the covered mode. Hence, the cut set that represents the redundancy exhaustion is:

$$C_4 = Y[1]Y[2]Y[3] \tag{22.18}$$

Therefore, the system unreliability is:

$$\begin{aligned} U = \Pr\left\{\bigcup_{i=1}^{4} C_i\right\} &= \Pr\{C_1\} + \Pr\{\neg C_1 C_2\} + \\ &\Pr\{\neg C_1 \neg C_2 C_3\} + \Pr\{\neg C_1 \neg C_2 \neg C_3 C_4\} \end{aligned} \tag{22.19}$$

Further, we have:

$$\begin{aligned} &\Pr\{C_1\} = \Pr\{Z[1]\} = c[1] \\ &\Pr\{\neg C_1 C_2\} = \Pr\{(\neg Z[1]) Z[2]\} \\ &= \Pr\{(X[1] \cup Y[1]) Z[2]\} \\ &= \Pr\{X[1] Z[2]\} + \Pr\{Y[1] Z[2]\} \\ &= a[1]c[2] + b[1]c[2] \end{aligned} \tag{22.20}$$

Similarly, we can find that:

$$\begin{aligned} &\Pr\{\neg C_1 \neg C_2 C_3\} = a[1]a[2]c[3] + a[1]b[2]c[3] + \\ &a[2]b[1]c[3] + a[2]b[2]c[3] \\ &\Pr\{\neg C_1 \neg C_2 \neg C_3 C_4\} = b[1]b[2]b[3] \end{aligned} \tag{22.21}$$

Using this approach, we can find the probability of each term in (22.19). The sum of all these probabilities is equivalent to the system reliability.

Although the DDP algorithm reduced the solution complexity from Markov chain based solutions to combinatorial solutions, it is still not suitable for solving large systems. This is because the solution uses cut-set based techniques where finding the cut-sets of a large system itself is a hard problem [43]. Further, expanding the SDP terms needs a complex procedure required for multi-state systems. In addition to this each SDP term contains n variables where the n is the number of components in the system. In order to overcome some of these difficulties, Doyle *et al*., and Zang *et al*. [21, 69] used a latest data-structure called binary decision diagram (BDD). However, unlike in the standard BDD, the variables used in the proposed BDD solution are not independent due to the dependencies among the component states, *i.e.*, the states of a component are mutually exclusive. Hence, the size of the resulting BDD increases, which nullifies the advantages of the BDD technique. Recently, Zing and Dugan [65] proposed a ternary decision diagram (TDD), which is a special type of multi-valued decision diagram (MDD). In the TDD method, a variable can take

three values (branches) that represent the three mutually exclusive states of the component: $X[i]$, $Y[i]$, and $Z[i]$. The advantage of this method is that the TDD contains the same number of nodes as the BDD that is used for the perfect fault coverage case. However, the number of branches in the TDD increases to 3/2 times to that of the BDD for the perfect coverage case. It should be noted that the number of nodes in a BDD is always greater than the number of variables. In most cases, the number of nodes is much greater than the number of variables. Using, the SEA algorithm [5], we can reduce the number of branches to that of the perfect coverage case. However, the TDD approach proposed in [68] solves the phased-mission systems effectively.

22.7.3 SEA

Amari [1] has identified that several computations in the DDP algorithm can be simplified. In addition to this, the system failure state can be divided into mutually exclusive states: system covered failure state and system uncovered failure state. The uncovered failure of the system occurs if at least one component is failed in the uncovered mode. The probability of this state can be calculated using a simple product over all components. This calculation can be performed in a linear-time with respect to the system size. The system fails in the covered mode, if no component fails in the uncovered mode and the system reaches the exhaustion of redundancy. Alternatively, it happens when the system failure condition is reached without the presence of uncovered failures. It is observed that the probability of this failure can be calculated using the same formula as for the perfect coverage case, except that we should use conditional component reliabilities (given that no uncovered failure has occurred) in the place of component reliabilities. The conditional reliability of all components can be computed in a linear-time with respect to the system size. Hence, the computational time to find the reliability of a system with imperfect coverage is almost equivalent to that of perfect coverage case where the effects of imperfect coverage are ignored.

Using the above separable method, [1, 5] proposed an algorithm called simple and efficient algorithm (SEA). The following proof of this algorithm is given in [1, p. 208]. Define the events:

- E: system failure
- E_1: at least one component in the system has failed in an uncovered mode.
- E_2: no component has failed in an uncovered mode.
- $Z[i]$: component i has failed in the uncovered mode (not-covered mode).

Here, E_1 and E_2 are mutually exclusive and exhaustive (complete) events. Further, we have:

$$E_1 = \bigcup_{i=1}^{n} Z[i]$$
$$E_2 = \bigcap_{i=1}^{n} \neg Z[i] \tag{22.22}$$

According to the total probability theorem [43, 57], the system unreliability can be expressed as:

$$U = \Pr\{E\}$$
$$= \Pr\{E \mid E_1\} \cdot \Pr\{E_1\} + \Pr\{E \mid E_2\} \cdot \Pr\{E_2\} \tag{22.23}$$

The system is failed if at least one component is failed in the uncovered mode. Hence, $Pr\{E|E_1\} = 1$. Because the components are independent, we have:

$$\Pr\{E_1\} = \Pr\left\{\bigcup_{i=1}^{n} Z[i]\right\} = 1 - \prod_{i=1}^{n} (1 - c[i])$$
$$\Pr\{E_2\} = 1 - \Pr\{E_1\} = \prod_{i=1}^{n} (1 - c[i]) \equiv P_u \tag{22.24}$$

The probability, $Pr\{E|E_2\}$, is calculated based on the condition that no uncovered failure has occurred in the system. Because all components are independent, it is equivalent to the unreliability of the same system computed using the conditional component reliabilities ($R[i]$) and unreliabilities ($Q[i]$) obtained using the condition that no uncovered fault has occurred in any component. Hence, we have: $R[i] = a[i]/(a[i]+b[i])$ and $Q[i] = b[i]/(a[i]+b[i])$. The conditional reliability (R_c) or unreliability (Q_c) can be calculated using any method that is applicable for the perfect coverage

case. Finally, the system reliability and unreliability are:

$$U = 1.(1 - P_u) + Q_c \cdot P_u$$
$$R = 1 - U = P_u \cdot R_c \quad (22.25)$$

Therefore, the algorithm to compute system reliability and unreliability is as follows:

SEA algorithm

1. Find P_u.

$$P_u = \prod_{i=1}^{n} (a[i] + b[i]) \quad (22.26)$$

where *a[i]+b[i] = 1-c[i]*.

2. Find the modified reliability and unreliability of each component.

$$R[i] = \frac{a[i]}{a[i] + b[i]}$$
$$Q[i] = \frac{b[i]}{a[i] + b[i]} \quad (22.27)$$

3. Using $Q[i]$ and/or $R[i]$ from step 2, find the reliability (R_c) or unreliability (Q_c) of the corresponding perfect coverage system by any method.
   a. Binary decision diagram (BDD) [51].
   b. Sum of disjoint products (SDP) [41].
   c. Any other method, *e.g.*, path-sets, cut-sets, binomial theorem, inclusion-exclusion method, modular fault-tree approach, pivotal decomposition, and simulation [43].
4. Find the reliability or unreliability of the imperfect coverage system as:

$$U = 1 - P_u + P_u \cdot Q_c = 1 - P_u \cdot R_c$$
$$R = 1 - U = P_u \cdot R_c \quad (22.28)$$

In other words, the SEA approach defines a method for adjusting the inputs and outputs for a given software package (or a method) to accommodate the additional information about fault coverage probabilities. No programming (or algorithm) changes to the reliability analysis package are necessary to implement this approach. Figure 22.13 demonstrates how the SEA approach wraps around any traditional fault tree analysis software package.

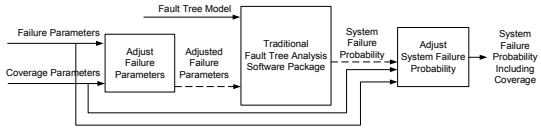


Figure 22.13. Integration of SEA with a traditional FTA package

In order to demonstrate this method, consider the three unit redundant system discussed in Section 22.7.2. We have:

$$P_u = (1 - c[1])(1 - c[2])(1 - c[3])$$
$$Q[1] = b[1]/(a[1] + b[1])$$
$$Q[2] = b[2]/(a[2] + b[2])$$
$$Q[3] = b[3]/(a[3] + b[3]) \quad (22.29)$$
$$Q_c = Q[1]Q[2]Q[3]$$
$$R_c = 1 - Q_c$$

Finally, the system reliability is: $R = P_u.R_c$. With some simple mathematical manipulations, the reliability can be expressed as:

$$R = \prod_{i=1}^{3} (a[i] + b[i]) - \prod_{i=1}^{3} b[i] \quad (22.30)$$

Similarly, we find the closed-form expressions for all systems whenever the closed-form expression for the corresponding perfect coverage case exists. Amari *et al*. [4] provided the closed-form expressions for several standard systems such series, parallel, parallel-series, series-parallel, *k*-out-of-*n*, and majority voting system. Using these closed-form expressions, [4] has provided efficient algorithms to find the optimal system configurations that maximize the overall system reliability.

22.7.4 Some Generalizations

22.7.4.1 Propagtion of Uncovered Failures

The SEA algorithm assumes that an uncovered failure of any component leads to the overall system failure. In other words, the effects of uncovered failures are global. However, this may not be the case in some situations. The uncovered

failure in a component may leads to the failure of a module (or subsystem) that contains the component, *i.e.*, the effects of uncovered failures are local to that module. As a result, the module failure may not always lead to the overall system failure and it depends on the states of other modules in the system. In such cases, the reliability of each module is calculated using the SEA algorithm (step 1) and overall system reliability is calculated using the reliabilities of individual modules (step 2) [1]. While calculating the overall system reliability (step 2), we assume perfect coverage. Hence, there is no need to apply the separable approach once again.

The above concept is generalized to the modular imperfect coverage case [66] where the uncovered failure of a component is limited to its local module with a certain probability p and may propagate to the next higher level with probability $q = 1-p$. Another way of modeling the same situation is that an uncovered failure of a component may cause immediate failure up to a certain higher level (hierarchies) according to a probability distribution. The latter approach requires more parameters as compared to the former. However, it provides a more detailed modeling capability. The solution to this problem is provided by recursively applying the concepts of separable method (SEA) from the lower level module to the higher level module.

Zing and Dugan [64] extended the concept of modular imperfect coverage to the phased-mission systems (PMS), where an uncovered component failure in a specific phase may be local to that phase (leads to phase failure) or global to the entire mission (leads to overall mission failure) with certain probabilities. It should be noted that we can only distinguish these local and global uncovered failure effects, when the phases are not in series. Therefore, [64] also proposed the concept of a non-series type phased mission system, which is a generalization to the traditional phased-mission system. Extending the same concept, the phased-mission system can be modeled as a multi-state system, where the state of the system is determined based on the specific combination of successful phases. The solution to this problem is obtained by applying the separable method twice.

22.7.4.2 Dependencies in Component Failures

Both the SEA and DDP algorithms assume that the failure or success logic of the system is combinatorial and the failures of components are statistically independent. These assumptions are too restrictive; particularly, they are not valid when there are induced failures, standby components, load-sharing components, priorities in repairs, limited repair resources, and sequential failures. If there is at least once such dependency, we cannot apply the SEA approach directly. Hence, we should once again go back to the complex Markov solutions.

Dugan [25] presented an effective solution to this problem when the system failure behavior is modeled using fault trees. It is assumed that the sequence dependencies are modeled using dynamic gates. Hence, using modularization techniques, the fault tree is partitioned into static modules and dynamic modules. The static modules are solved using combinatorial methods where we can apply the SEA algorithm to compute modules covered and uncovered failure probabilities. The dynamic modules are solved using Markov chains or simulation. Once we know the covered and uncovered probabilities for each module, we can once again use the SEA algorithm to compute the overall system reliability.

The same concept is further extended to the phased-mission systems, where the static phases are solved using combinatorial methods and the dynamic phases are solved using Markov chains. For details, refer to [64, 67].

22.7.4.3 Multi-state Systems and Components

The majority of published works on imperfect coverage assumes that both the system and its components have only two states if the effects of coverage are ignored. However, with the addition of imperfect coverage, the failure state of the system and its components are once again divided into: covered failure and uncovered failure. Only in this way, the system and its components have multiple states, *i.e.*, three states with single-fault coverage models. In this situation, using SEA we can convert the problem into an equivalent perfect

coverage problem having binary states. However, the binary models are not appropriate in several applications. This is because the system performance may decrease over time due to its component failure, but might not have reached a total failed state. In such cases, if the failure and repair follow exponential distributions, we can use Markov reward processes. To some extent, we can also use semi-Markov or non-homogeneous Markov reward models to handle the general distributions. However, with this approach we need to use the complex Markov chain based solutions that are efficient only for moderate size systems. Of course, using some approximations or bounds we can solve the large problems to some extent [15, 51].

Another approach to this problem is multi-state system (MSS) modeling. It should be noted that the Markov chain approach itself is a multi-state approach. However, in most cases, we can decompose the problem such that individual components, subsystems, or modules (or super-components) can be modeled using state-space methods (Markov chains). Further, the overall system performance or behavior can be expressed using combinatorial models as a combination of different component states. The MSS approach can be used to model degradation, dependencies associated with cold or warm spares, load-sharing components, *etc*. Now if we add the effects of coverage to the individual components of the original model, then the components and systems in the MSS model will have an additional state that represents the uncovered failure. The MSS model that includes the effects of coverage can be solved using several existing methods such as explicit enumeration, disjointing method based on critical state vectors (multi-state cut sets), binary decision diagrams with restrictions on variables, *etc*. [32, 43]. However, as in the case of the DDP algorithm for binary state systems, this method has some limitations. Due to the presence of uncovered failures, we cannot use the modularization methods. The state-space of the system increases quickly even though only one additional state is added to each component. With the addition of an uncovered failure to each component, when disjointing method is used, each product term contains the states from all components. For example, the above difficulties can easily be realized while solving the multi-state k-out-of-n system subjected to imperfect coverage. Therefore, the direct application of MSS solution methods is inefficient.

In order to overcome the above difficulties, Chang *et al*. [17, 18] extended the separable approach used in SEA to the case of multi-state components where the implicit assumption is that the system is subjected to single-fault coverage models. Consider that a multi-state component has $m + 1$ states: 0, 1,…,m. Where 0 indicates uncovered failure state, and 1,…,m indicates other m performance levels that include covered failure states. Let $p[i]$ be the unconditional probability of state i. The conditional probability that the component is in state i given that no uncovered failure has occurred in that component is:

$$P_c[i] = \frac{p[i]}{1 - p[0]} \quad . \tag{22.31}$$

Once we know these probabilities, we can apply any method that is applicable for solving MSS systems subjected to perfect coverage. Chang *et al*. [17, 18] used binary decision diagrams (BDD) with restrictions on variables. Then the overall system reliability is calculated using the total probability theorem [57]. Although the BDD method is efficient in general, it may not be the case for each and every system. Particularly, several other efficient methods are readily available for well structured systems.

Levitin [33] proposed a direct recursive method based on universal generating functions for solving modular systems represented using multi-state reliability block diagrams. In this method, as in [1, 66] the effects of coverage can be local (to subsystems) or global (system level).

22.8 Combinatorial Method for System Reliability with Multi-fault Models

In this section, we discuss the combinatorial solutions for solving multi-fault coverage models. We first consider k-out-of-n systems with identical

components and then generalize these results for the non-identical component case. Later we discuss modular systems consisting of independent *k*-out-of-*n* subsystems subjected to multi-fault models. Finally, we present the methods for computing general configurations.

22.8.1 *k*-out-of-*n* Systems with Identical Components

In this section, we describe the method provided in [1, 44] for analyzing *k*-out-of-*n* systems subjected to multi-fault models. The method assumes that the coverage probabilities are calculated using near-coincident failures. Assume that p is the reliability of each component and c_i is the coverage probability at the ith failure. If the coverage probabilities are calculated based on fixed recovery window, from (22.5) we have:

$$c_i = \exp[-(n-i)\lambda\tau]\,. \tag{22.32}$$

Because the system fails after $(n-k+1)$ failures (irrespective of fault coverage), c_i for $i \geq (n-k+1)$ are not applicable and can be considered as zero. Myers [44] used a slightly different approach to calculate the coverage probabilities where the mid-value-select voting scheme is used to find the failed components. It is assumed that as long as there are more than two good components in the system, the mid-value-select scheme covers all failures if there is no additional component failure within the recovery window. If there are only two components in the system, then the components' failures cannot be covered using the mid-value-select voting scheme. In such cases, the coverage of a component is based on built-in-tests. Hence, c_{n-1} is calculated using single-fault models associated with the built-in-tests. If there is only one component in the system, failure of that component leads to overall system failure for any value of k. Hence, c_n can be considered as zero. Of course, this value does not impact the reliability of a *k*-out-of-*n* system.

The above calculations can be generalized to the case where built-in-tests are performed at each failure instance in addition to the mid-value-select voting scheme. Let c be the coverage associated with the built-in-test of a component. Then the effective, coverage factor at the ith failure is:

$$c_i = 1-(1-c)(1-\exp[-(n-i)\lambda\tau]) \approx c+\exp[-(n-i)\lambda\tau \tag{22.33}$$

First consider the perfect coverage case, where the reliability of *k*-out-of-*n* system is [32]:

$$R = \sum_{i=0}^{n-k} P_i\,, \tag{22.34}$$

where P_i is the probability of exactly i components have failed. For the identical component case, P_i can be calculated using the binomial distribution.

$$P_i = \binom{n}{i} p^i q^{n-i}\,, \tag{22.35}$$

where $q = 1 - p$ = unreliability of each component. In the imperfect coverage case, we should multiply P_i with the cumulative coverage probability associated with the first i failures. The cumulative coverage up to the first i failures is:

$$r_i = \prod_{j=0}^{i} c_i\,. \tag{22.36}$$

Note that by definition, we have: $c_0 = r_0 = 1$. Therefore, system reliability is:

$$R = \sum_{i=0}^{n-k} r_i P_i\,. \tag{22.37}$$

The reliability in (22.37) can be computed using a linear-time algorithm.

Algorithm 1: Reliability with Identical Components

$x = p^n = \exp\{n \cdot \ln(p)\}$; y = q/p
for $i = 1$ to $(n-k)$ do
$x = c_i \cdot x \cdot y \cdot \dfrac{n-i+1}{i}$; $\mathrm{Re}\,l = \mathrm{Re}\,l + x$
done

At the end of the algorithm, the results for reliability will be accumulated in Rel.

22.8.2 *k*-out-of-*n* Systems with Non-identical Components

In this case, we assume that the components are non-identical. Let p_i be the reliability of component

i. In this case, the exact calculation of coverage probabilities c_i depends on a set of components that already failed. For example, the coverage probability at component *k* is calculated based on the effective failure rate (λ_{eff}) within the recovery window. The effective failure rate is the sum of failure rates of all non-failed components. If components *i* and *j* have already failed, then the coverage at component *k* failure is calculated by summing the failure rates of all components except the components *i, j, k*. Hence, the coverage probability is: $\exp(-\tau.\lambda_{\text{eff}})$. This approach is used in HARP [9]. However, such a calculation increases the computational time exponentially. Therefore, using the average failure rate approximation, the coverage probability calculations can be simplified to produce acceptable results. Using this approximation, we calculate the average failure rate of all *n* components first and then use (22.32) to compute the coverage probability at each failure.

Once we know component reliabilities and coverage probabilities, it is straightforward to extend the method discussed in Section 22.8.1 to the non-identical component case. The only difference is that P_i should be computed using an appropriate formula. For simplicity, consider a 2-out-of-3 system. We have:

$$R = P_0 + r_1 P_1 + r_2 P_2 . \qquad (22.38)$$

The probabilities for P_i can be calculated in several ways. For example, we show two different forms of equations:

FORM 1: truth-table

$$\begin{aligned} P_0 &= p_1 p_2 p_3 \\ P_1 &= q_1 p_2 p_3 + p_1 q_2 p_3 + p_1 p_2 q_3 \\ P_2 &= p_1 q_2 q_3 + q_1 p_2 q_3 + q_1 q_2 p_3 \end{aligned} \qquad (22.39)$$

FORM 2: inclusion-exclusion using path-sets

$$\begin{aligned} P_0 &= p_1 p_2 p_3 \\ P_1 &= p_1 p_2 + p_2 p_3 + p_1 p_3 - 3 p_1 p_2 p_3 \\ P_2 &= q_1 q_2 + q_2 q_3 + q_1 q_3 - 3 q_1 q_2 q_3 \end{aligned} \qquad (22.40)$$

Myers and Rauzy [45, 46] proposed an efficient $O(n(n\text{-}k))$ algorithm to compute the reliability of *k*-out-of-*n* systems with non-identical components subjected FLC models (multi-fault models). This algorithm slightly modifies the perfect coverage case algorithm discussed in [26].

Algorithm 2: Reliability with Non-identical Components

$R = 0; P[1] = 1;$ for $i = 2$ to $n - k + 1$ do $P[i] = 0;$ done
for $i = 1$ to n do
  for $j = n - k$ downto 1 do
    $P[j+1] = p_i \cdot P[j+1] + c_j \cdot q_i \cdot P[j]$
    if $(i == n)$ then $R = R + P[j+1]$
  done
  $P[1] = p_i \cdot P[1]$
done
$\text{Re}l = R + P[1]$

At the end of the algorithm, the results for system reliability will be accumulated in Re*l*.

22.8.3 Modular Systems

This section considers general configuration systems with embedded *k*-out-of-*n* subsystems subjected to multi-fault models. In other words, the system consists of several *k*-out-of-*n* type subsystems arranged in either a series-parallel or non-series-non-parallel structure. Each subsystem consists of identical or non-identical components, and these components form an FLC group. This means that the coverage probabilities of the components in a subsystem depend only on the number of good components in that subsystem.

As in Section 22.7.4.1 [1, 66], we consider two cases for the effects of uncovered failure: (1) local to each subsystem, and (2) global to system level. In the first case, we can calculate the reliability of each subsystem as mentioned in Sections 22.8.1 and 22.8.2. Using these subsystem reliabilities, we can compute the overall system reliability using an appropriate combinatorial method. In the second case, we can apply the separable method used in SEA. In order to apply this method, we should first calculate the reliability of each subsystem as mentioned in Sections 22.8.1 and 22.8.2. In

addition to this we should also calculate the covered and uncovered failure probabilities for each subsystem.

The uncovered failure of subsystem j can be calculated as:

$$U_j = \sum_{i=0}^{n(j)} [1 - c_i(j)] r_{i-1}(j) P_i(j), \qquad 22.41)$$

where c, r, P have the same meaning as in Sections 22.8.1 and 22.8.2. The uncovered failure probability can also be calculated by slightly modifying the reliability algorithms presented in Sections 22.8.1 and 22.8.2. The covered failure probability of subsystem j can be calculated as:

$$V_j = 1 - R_j - U_j. \qquad (22.42)$$

Once we know reliability, covered failure probability, and uncovered failure probability for each subsystem, we can use the SEA algorithm to compute the overall system reliability as in the case of ELC models.

22.8.4 General System Configurations

This section considers general configuration systems where the components in any FLC group can appear anywhere in the system, *i.e.*, they need not to belong to a specific k-out-of-n type subsystem.

22.8.4.1 System Description and Assumptions

The solution methods are proposed considering the following assumptions, which are applicable for most cases.

- The system consists of several s-independent components. The only dependency among the component failures is due to the uncovered failures caused by imperfect fault coverage mechanisms.
- The uncovered (not-covered) failure of any component causes immediate system failure, even in the presence of adequate redundancy. Note that, as discussed in the previous section, it is easy to relax this assumption.
- The system consists of several groups of components called FLC groups. Say there are m FLC groups. Each component belongs to one and only one FLC group. Note that if needed all components with perfect coverage can be grouped into a special FLC group where coverage is unity.
- The *fault-coverage* = Pr{system can recover | a fault occurs} depends on the number of faulty components in the FLC group corresponding to the faulty component.
- An s-coherent combinatorial model (fault tree, RBD, digraph, or network) can be used to represent the combinations of covered component failures that lead to system failure (or success).
- Fault occurrence probabilities are given either (a) as fixed probabilities (for a given mission time), or (b) in terms of a lifetime distribution. They are s-independent of the system state.

22.8.4.2 The Sum of Disjoint Product Approach

In this method, we represent the system structure using a sum of disjoint products (SDP) form. For example, consider the truth table method, which is a special type of SDP method. In this method, each product term contains a specific combination of states (good or failed) of all components. For each product term, we can find the number of failed components that belongs to each FLC group and then find the corresponding coverage probability. Then we can find the contribution of each product term to the overall system reliability by multiplying the corresponding component reliabilities, unreliabilities, and coverage probabilities. The sum of product contributions over all products gives the overall system reliability.

The truth table approach can be improved by grouping the product terms that belongs to specific number of failed components in each FLC group. Although this procedure produces correct results, it is computationally inefficient. Therefore, this method can only be applied for very small problems.

22.8.4.3 The Implicit Common-cause Failure Method

This method is proposed in [6] and it uses SEA-based calculations [5] and common-cause failure analysis concepts [62]. The basic idea of this method is that the conditional reliability of the system given that no uncovered failure in the system can be computed using implicit common-cause failure analysis. To apply implicit common-cause analysis, we should know the joint probabilities of events that belong to an *s*-dependent group (FLC group). The procedure is explained through a simple example of 2-out-of-3 system with non-identical components subjected to imperfect fault coverage. To apply this method, we should first compute the uncovered failure probability (U) of each FLC group using (22.41). Let x_i be the probability that only the ith component in the FLC group has failed in covered mode given that there is no uncovered failure in the FLC group. Similarly, x_{ij} represents the probability that only the ith and jth components have failed. Hence, we have:

$$\begin{aligned} x_1 &= r_1 q_1 p_2 p_3 /(1-U) \\ x_{12} &= r_2 q_1 q_2 p_3 /(1-U) \\ x_{123} &= r_3 q_1 q_2 q_3 /(1-U) \end{aligned} \tag{22.43}$$

Similarly, we can compute (1) x_2 and x_3, and (2) x_{13} and x_{23}. Let y_{ij} be the probability that at least components i and j have failed in the covered mode, and there are no uncovered failures in the FLC group. Hence, we have:

$$\begin{aligned} y_1 &= x_1 + x_{12} + x_{13} + x_{123} \\ y_{12} &= x_{12} + x_{123} \\ y_{123} &= x_{123} \end{aligned} \tag{22.44}$$

Similarly, we can compute (1) y_2 and y_3, and (2) y_{13} and y_{23}. Once we know these x and y values, it is straightforward to compute the system reliability. Most algorithms use the y values. For example, the conditional unreliability of a 2-out-of-3 system is:

$$Q^c = y_{12} + y_{13} + y_{23} - y_{123}. \tag{22.45}$$

Finally, the overall system reliability is: $(1-U)(1-Q^c)$. The method for general system configuration follows:

- For each FLC group j, find the uncovered failure probability, (U_j).
- Using U_j, for each FLC group, find the x and y values required for the common-cause analysis.
- Using these x and y values, compute the system conditional reliability, R_c.
- Compute the C = Pr{no uncovered failure in the system}.

$$C = \prod_{i=1}^{m} (1 - U_j), \tag{22.46}$$

  where m is the number of FLC groups in the system.
- Finally, the overall system reliability is:

$$R = C.R_c. \tag{22.47}$$

Although this method is slightly better than the SDP method discussed in Section 22.8.4.2, it is still computationally expensive for the general system configurations. In order to overcome this difficulty, reference [6] proposed a simple approximation.

22.8.4.4 The Approximation Method

The basic idea of this approximation is that "the conditional reliability of the system given that no uncovered failure in the system (R_c)" is almost equivalent to the "unconditional reliability of the system with perfect coverage (R_p)" [6]. In fact, $R_c \geq R_p$. Hence, this algorithm produces provably conservative results for the system reliability. The algorithm is follows :

- For each FLC group in the system, find the uncovered failure probability.
- Compute C = Pr{no uncovered failure in the system}.
- Using component reliabilities, compute the system reliability, R_p, using any combinatorial algorithm. This means that we compute the system reliability ignoring

effects of coverage, *i.e.*, assuming perfect coverage.

- Finally, the overall system reliability is:

$$R = C.R_p . \tag{22.48}$$

The computational time of this algorithm is equivalent to that of the perfect coverage case and the error in this approximation is very small and can be ingnored for any practical purposes [6].

22.8.4.5 Binary Decision Diagrams

Recently, Myers and Rauzy [45, 46] proposed an efficient method using binary decision diagrams (BDD) for computing the reliability of systems subjected to imperfect coverage. In this section, we describe this method for solving complex systems subjected to FLC models. The basic idea of this method is that the system is successful only if there are no uncovered failures in any FLC group and the number of working components in the system satisfies its structue function for success. Hence, we have:

$$R = \Pr\{X_0 \cap X_1 \cap ... \cap X_m\} , \tag{22.49}$$

where X_0 represents the Boolean function for system success when the coverage is perfect. X_i, i=1,…,m, represents the Boolean function for "no uncovered failures" in FLC group i. In order to find the intersection in (22.49) and its probability, Myers and Rauzy [46] used binary decision diagrams. In this method, we should first find the BDD for each X_i, I = 0,1,…,m. Then find the BDD for overall system success using AND operations.

Generating the BDD for X_0, *i.e.*, without considering the effects of coverage (perfect coverage) is discussed in several publications [51]. The remaining step is finding the BDD for X_i, i=1,…,m, that represents the "no uncovered failures" in FLC group i in terms of variables that represent component success, component failure, and success of coverage mechansims. Myers and Rauzy [46] proposed an efficient BDD representation for each FLC group. For example, consider an FLC group consisting of four components. Then the BDD for this FLC group can be represented as in Figure 22.14.

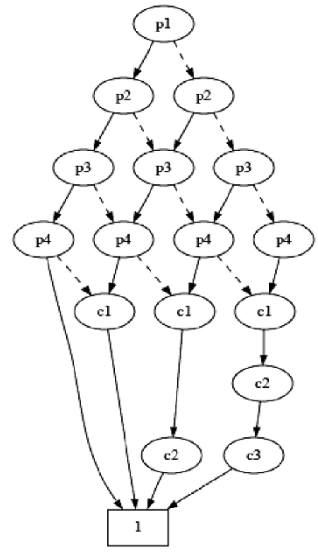


Figure 22.14. BDD for a 4-unit system subject to FLC models

In this BDD, the branches that lead to node 0 (uncovered failure) are removed to simplify the BDD representation. Once we generate the BDDs for all X_i, we can find the BDD for system success using standard BDD operations [51]. The calculation of system reliability is straightforward from the BDD representation of the system success and these details are available in several sources [16, 51].

The above method can be generalized to the case of induced failures, where failure of a component forces some other components to fail. For example, consider the quad power computer with cross channel data link (CCDL) discussed in [6, 44]. It has four computers (C1, C2, C3, and C4) and four sensors (S1, S2, S3, and S4). In this system, S1 is considered to be available only if C1 is available. Similarly, S2, S3, and S4 are considered to be failed if C2, C3, and C4 are respectively failed. Hence, while generating the BDD for the FLC group corresponding to sensors (S1, S2, S3, and S4), we should also consider the states of computers (C1, C2, C3, and C4). Hence, the BDD for sensors FLC success contains a total of 11 variables: 4 for computers, 4 for sensors, and 3 for sensor coverages.

22.8.5 Some Generalizations

All multi-fault coverage (FLC) models considered so far assume that the system and its components have binary states if the effect of coverage is ingored. Reference [36] generalized the concept of FLC to multi-state systems consisting of binary components with different performance and reliability characteristics. However, Levitin and Amari [36] assumed that the system is represented using modular reliability block diagrams where each FLC group represents a *k*-out-of-*n* subsystem. Similarly, Levitin and Amari [37] generalized this concept to performace based coverage, where the coverage factor of each FLC group depends on its performance instead of the number of failed components. Levitin and Amari [35] extended the concepts of FLC for the modular imperfect coverage case [66], where uncovered failures progatage from a lower system level to higher system level.

22.9 Optimal System Designs

Amari *et al.* [4] have proved that reliability of any system subjected to imperfect fault-coverage, particularly with single-fault models, decreases after a certain level of active redundancy. Therefore, there exists an optimal level of redundancy that maximizes the overall system reliability. These results coincide with the observations made in [23]. Specifically, Dugan and Trevedi have shown that both reliability and mean time to failure (MTTF) of parallel systems subjected to imperfect fault-coverage decreases with the increase in number of parallel components after reaching a certain limit. Initially, these observations seem counterintuitive. However, as explained in [23], the systems subjected to imperfect fault-coverage can fail in two modes: covered failure and uncovered (not-covered) failure. Irrespective of the system structure function, the system behaves like a series system for the uncovered failure mode, which is a dominant failure mode for the systems with a large number of components. Therefore, the system reliability decreases with an increase of redundant components after a certain limit. Several researchers have shown similar results for some special cases of *k*-out-of-*n* systems that include triple modular redundancy with spares [49], *k*-resilient protocols [50], multiprocessor systems [60], and gracefully degradable systems [47]. Amari *et al.* [4] provided closed-form solutions for optimal redundancy that maximize the reliability of various standard system models that include parallel systems, series-parallel systems, parallel-series systems, *N*-tuple modular systems, and *k*-out-of-*n* systems. Similarly, using the concepts of SEA [5], the cost-effective design policies for parallel systems subjected to imperfect fault-coverage are provided [3]. Later Amari *et al.* [2] extended these results for complex systems composed of *k*-out-of-*n* subsystems and provided easy to evaluate lower and upper bounds for optimal redundancy levels for both reliability optimization and cost minimization problems.

In all the previous studies, the aim is to (1) show the negative effects of imperfect fault-coverage, (2) emphasize the need for accurate analysis of the coverage factor, and (3) emphasize the use of optimal redundancy (thereby discouraging the use of too much redundancy). In addition to this, Amari [1] also discusses some alternative means for the provision of redundancy that include adding the spares in periodic intervals, use of standby redundancy, and adding the redundancy only when a certain predefined number of components have failed. Amari [1] studied the effects of imperfect fault-coverage on the cold standby redundancy policies. It shows that, unlike in active redundancy, the reliability of a cold standby system always increases with the additional redundancy. However, unlike in the perfect coverage models, there exists a maximum achievable reliability limit for the standby systems subjected to imperfect fault-coverage. A closed-form solution to the maximum achievable reliability limit is provided. Further, an algorithm is provided to find the optimal cost-effective redundancy level that strikes a balance between system failure cost and the cost of spares [1].

Levitin [34] considered the optimal redunancy problem of multi-state systems subjected to single-fault coverage models. The solution to this

problem is provided using the universal generating function method and genetic algorithms.

Almost all papers that consider optimal redundancy problems assume that the system is subjected to single-fault models. Not much work has been done on the multi-fault coverage models. Similarly, there is a need to develop optimal design policies for multi-state systems, phased-mission systems, and common-cause failure models subjected to imperfect coverage.

22.10 Conclusions and Future Work

Coverage is an important concept and it is used to assess the effectiveness of tolerant mechanisms. In this chapter, we discussed various coverage models for both single-fault models and multi-fault models. These models can be used to model both single-point failures and near-coincident failures. We also discussed the status and trends in analyzing the systems subjected to imperfect fault coverage models. Particularly, we emphasized the use of behavioural decomposition, Markov chain based solutions, combinatorial methods based on a separable method, and binary decision diagrams. Recently, several generalizations to imperfect coverage models are proposed that include the integration of coverage models into multi-state systems, phased-mission systems, hierachiel systems, dynamic fault trees, reliability block diagrams, and common-cause failure models.

The reliability of systems subjected to imperfect coverage models decreases after a certain level of redundancy. Therefore, there exists an optimal redundancy that maximizes the system reliability. Further, it is important to investigate the sparing policies that are specific to imperfect coverage cases.

In the past few years, multi-fault coverage models have gained a lot of research interest. New solution methods and generalizations are proposed by several researchers. At the same time, there is still a lot of scope for further research. Particularly, there is a need for integrating multi-fault coverage models into multi-state models, phased-mission systems, dependent failures, common-cause failures, *etc*. In addition to this, the methods for finding the optimal redundancy of systems subjected to multi-fault models are still limited.

References

[1] Amari SV. Reliability, risk and fault-tolerance of complex systems. PhD Dissertation, Indian Institute of Technology, Kharagpur, 1997.

[2] Amari SV, Pham H, Dill G. Optimal design of *k*-out-of-*n*:G subsystems subjected to imperfect fault-coverage. IEEE Trans. on Reliability 2004; 53:567−575.

[3] Amari SV, McLaughlin L, Yadlapati B. Optimal cost-effective design of parallel systems subject to imperfect fault-coverage. Proc. IEEE Ann. Reliability and Maintainability Symp., Tampa, Florida Jan. 2003; 29−34.

[4] Amari SV, Dugan JB, Misra RB. Optimal reliability of systems subject to imperfect fault-coverage. IEEE Trans. on Reliability 1999; 48: 275–284.

[5] Amari SV, Dugan JB, Misra RB. A separable method for incorporating imperfect fault-coverage into combinatorial models. IEEE Trans. on Reliability 1999; 48: 267–274.

[6] Amari SV, Myers A, Rauzy A. An efficient algorithm to analyze new imperfect fault coverage models. Proc. Ann. Reliability and Maintainability Symp. Orlando, FL. Jan. 2007;420−426.

[7] Arnold TF. The concept of coverage and its effect on the reliability model of a repairable system. IEEE Trans. on Computers 1973; C-22:325–339.

[8] Avizienis A, Laprie JC, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. on Dependable and Secure Computing 200; 1:11−33.

[9] Bavuso SJ *et. al*., HiRel: Hybrid automated reliability predictor tool system (Version 7.0), NASA TP 3452, 1994.

[10] Bavuso SJ, Dugan JB, Trivedi KS, Rothmann EM, Smith WE. Analysis of typical fault-tolerant architectures using HARP. IEEE Trans. on Reliability 1987; R-36:176−185.

[11] Bobbio A. Trivedi KS. An aggregation technique for the transient analysis of stiff Markov chains. IEEE Trans. on Computers 1986; 35:803−814.

[12] Bouricius WG, Carter WC, Schneider PR. Reliability modeling techniques for self-repairing computer systems. 24th Ann. ACM National Conf. 1969; 295−309.

[13] Bouricius WG, Carter WC, Jessep DC, Schneider PR, Wadia AB. Reliability modeling for fault-

tolerant computers. IEEE Trans. on Computers 1971; C-20:1306−1311.

[14] Boyd MA, Veeraraghavan M, Dugan JB, Trivedi KS. An approach to solving large reliability models. Proc. of IEEE/AIAA 8th Embedded Digital Avionics Conf. 1988; 243−250.

[15] Butler RW, Hayhurst KJ, Johnson SC. A note about HARP's state trimming method. NASA/TM-1998-208427, 1998.

[16] Chang YR, Amari SV, Kuo S. Computing system failure frequencies and reliability importance measures using OBDD. IEEE Trans. on Computers 2003; 53: 54−68.

[17] Chang YS, Amari V, Kuo SY. Reliability evaluation of multi-state systems subject to imperfect coverage using OBDD. Proc. Pacific Rim Int. Symp. Dependable Computing (PRDC), Tsukuba, Japan, Dec. 16-18, 2002;193−200.

[18] Chang YR, Amari SV, Kuo SY. OBDD-based evaluation of reliability and importance measures for multistate systems subject to imperfect fault coverage. IEEE Trans. on Dependable and Secure Computing 2005; 2:336−347.

[19] Conn RB, Merryman PM, Whitelaw KL. CAST—A complementary analytic-simulative technique for modeling fault-tolerant computing systems. Proc. AIAA Computer Aero. Conf. 1977; 6.1−6.27.

[20] Cukier M, Powell D, Arlat J. Coverage estimation methods for stratified fault-injection. IEEE Trans. on Computers 1999; 48:707−723.

[21] Doyle SA, Dugan JB, Boyd M. Combinatorial-models and coverage: a binary decision diagram (BDD) approach. Proc. Ann. Reliability and Maintainability Symp., Washington D.C., Jan. 16-19, 1995; 82−89.

[22] Doyle SA, Dugan JB, Patterson-Hine FA. A combinatorial approach to modeling imperfect coverage. IEEE Trans. on Reliability 1995; 44:87−94.

[23] Dugan JB, Trivedi KS. Coverage modeling for dependability analysis of fault-tolerant systems. IEEE Trans. on Computers 1989; 38:775−787.

[24] Dugan JB. Fault trees and imperfect coverage. IEEE Trans. on Reliability 1989; 38:177−185.

[25] Dugan JB. Fault-tree analysis of computer-based systems. Tutorial Notes, RAMS, Reliability and Maintainability Symp., Los Angeles, CA, Jan. 26-29, 2004.

[26] Dutuit Y, Rauzy A. New insights in the assessment of *k*-out-of-*n* and related systems. Reliability Engineering and System Safety 2001; 72:303−314.

[27] Geist R, Trivedi KS. Reliability estimation of fault-tolerant systems: Tools and techniques. IEEE Computer, Special Issue on Fault-tolerant Computing 1990; 23: 52−61.

[28] Geist R. Extended behavioral decomposition for estimating ultrahigh reliability. IEEE Trans. on Reliability 1991; 40:22−28.

[29] Geist R, Smotherman M, Trivedi KS, Dugan JB. The reliability of life-critical computer systems. , Acta Informatica 1986; 23:621−642.

[30] Ibe OC, Howe RC, Trivedi KS. Approximate availability analysis of VAXcluster systems. IEEE Trans. on Reliability 1989; 38:146−152.

[31] Johnson AM Jr., Malek M. Survey of software tools for evaluating reliability, availability, and serviceability. ACM Computing Surveys 1988; 20:227−269.

[32] Kuo W, Zuo MJ. Optimal reliability modeling. Wiley, New York, 2003.

[33] Levitin G. Block diagram method for analyzing multi-state systems with uncovered failures. Reliability Engineering and System Safety 2007; 92:727−734.

[34] Levitin G. Optimal structure of multi-state systems with uncovered failures. IEEE Trans. on Reliability, March 2007; 57(1): 140-148.

[35] Levitin G, Amari SV. Reliability analysis of fault tolerant systems with multi-fault coverage. International Journal of Performability Engineering, 2007; 3(4): 441-451.

[36] Levitin G, Amari SV. Multi-state Systems with multi-fault coverage. Reliability Engineering and System Safety, in press, 2008.

[37] Levitin G, Amari SV. Multi-state Systems with static performance dependent coverage. Proc. Institution of Mechanical Engineers, Part O, Journal of Risk and Reliability, accepted for publication, to appear in 2008.

[38] Lindemann C, Malhotra M, Trivedi KS. Numerical methods for reliability evaluation of Markov closed fault-tolerant systems. IEEE Trans. on Reliability 1995; 44:694−704.

[39] Malhotra M, Muppula J, Trivedi KS. Stiffness-tolerant methods for transient analysis of stiff Markov chains. Microelectronics and Reliability 1994; 34:1825−1841.

[40] Malhotra M, Trivedi KS. Data integrity analysis of disk array systems with analytic modeling of coverage. Performance Evaluation 1995; 22:111–133.

[41] Mathur FP, Avizienis A. Reliability analysis and architecture of a hybrid-redundant digital system: Generalized triple modular redundancy with repair. Proc. AFIPS SJCC 1970; 36:375−383.

[42] McGough J, Smotherman M, Trivedi KS. The conservativeness of reliability estimates based on instantaneous coverage. IEEE Trans. on Computers 1985; 34: 602−609.

[43] Misra KB. Reliability analysis and prediction: A methodology oriented treatment. Elsevier, Amsterdam, 1992.

[44] Myers AF. *k*-out-of-*n*:G system reliability with imperfect fault coverage. IEEE Trans. on Reliability, Sept. 2007; 56(3): 464-473.

[45] Myers AF, Rauzy A. Assessment of redundant systems with imperfect coverage by means of binary decision diagrams. Reliability Engineering and System Safety. July 2008; 93(7): 1025-1035.

[46] Myers AF, Rauzy A. Efficient reliability assessment of redundant systems subject to imperfect fault coverage using binary decision diagrams. Accepted to appear in IEEE Trans. on Reliability, DOI: 10.1109/TR 2008. 916884.

[47] Najjar WA, Gaudiot J. Scalability analysis in gracefully-degradable large systems. IEEE Trans. on Reliability 1991; 40: 89−197.

[48] Ng YW, Avizienis A. ARIES: An automated reliability estimation system. Proc. Ann. Reliability and Maintainability Symp. Philadelphia, PA; Jan. 18-20, 1977; 108−113.

[49] Pham H. Optimal cost-effective design of triple modular redundancy with spares systems. IEEE Trans. on Reliability 1993; 42:369−374.

[50] Rangarajan S, Huang Y, Tripathi SK. Computing reliability intervals for k-resilient protocols. IEEE Trans. on Computers 1995; 44:462−466.

[51] Rauzy A. new algorithms for fault tree analysis. Reliability Engineering and System Safety 1993; 40:203−211.

[52] Rauzy A. Aralia user's manual. ARBoost Technologies 2006.

[53] Sahner RA, Trivedi KS. Puliafito A. Performance and reliability analysis of computer systems. Kluwer, Dordrecht, 1996.

[54] Shooman ML. Reliability of computer systems and networks: Fault tolerance, analysis, and design. Wiley, New York, 2002.

[55] Smotherman M, Geist RM, Trivedi KS. Provably conservative approximations to complex reliability models. IEEE Trans. on Computers 1986; C-35: 333−338.

[56] Trivedi KS, Geist RM. A tutorial on the CARE III approach to reliability modeling. NASA Contractor Report, 1981; 3488.

[57] Trivedi KS. Probability and statistics with reliability, queuing, and computer science applications. Wile, New York, 2001.

[58] Trivedi KS, Geist R. Decomposition in reliability analysis of fault tolerant systems. IEEE Trans. on Reliability 1983; R-32:463−468.

[59] Trivedi KS, Dugan JB, Geist R, Smotherman M. Modeling imperfect coverage in fault-tolerant systems. Fault-Tolerant Computing Symp. (FTCS) IEEE Computer Society, 1984; 77−82.

[60] Trivedi KS, Sathaye AS, Ibe OC, Howe RC. Should I add a processor? 23rd Annual Hawaii International Conference on System Sciences. IEEE Computer Society Press; Jan. 1990:214−221.

[61] Trivedi KS, Dugan JB, Geist R, Smotherman M. Hybrid reliability modeling of fault-tolerant computer systems. Computers and Electrical Engineering, 1984; 11:87−108.

[62] Vaurio JK. Treatment of general dependencies in system fault-tree and risk analysis. IEEE Trans. on Reliability 2002; 51:278−287.

[63] Vesely W. *et al*. Fault tree handbook with aerospace applications, Version 1.1, NASA Publication, Aug. 2002.

[64] Xing L, Dugan JB. Analysis of generalized phased-mission systems reliability, performance, and sensitivity. IEEE Trans. on Reliability 2002; 199−211.

[65] Xing L, Dugan JB. Dependability analysis using multiple-valued decision diagrams. 6th Int'l. Conf. Problems in Safety Assessment and Management (PSAM6) 2002.

[66] Xing L, Dugan JB. Dependability analysis of hierarchical systems with modular imperfect coverage. Proc. 19th Int. System Safety Conf. (ISSC) 2001; 347−356.

[67] Xing L. Reliability importance analysis of generalized phased-mission systems. International Journal of Performability Engineering 2007; 3:303−318.

[68] Xing L, Dugan JB. A separable ternary decision diagram based analysis of generalized phased-mission reliability. IEEE Trans. on Reliability 2004; 53: 174−184.

[69] Zang X, Sun H, Trivedi KS. Dependability analysis of distributed computer systems with imperfect coverage. Proc. 29th Ann. Int. Symp. Fault-Tolerant Computing (FTCS-29); IEEE Computer Society, IEEE Press, Madison, WI, 1999: 330−337.

23

Reliability of Phased-mission Systems

Liudong Xing[1] and Suprasad V. Amari[2]

[1] Department of Electrical and Computer Engineering, University of Massachusetts – Dartmouth, USA
[2] Relex Software Corporation, Greensburg, USA

Abstract: In this chapter, a state-of-the-art review of various analytical modeling techniques for reliability analysis of phased-mission systems (PMS) is presented. The analysis approaches can be broadly classified into three categories: combinatorial, state-space oriented, and modular. The combinatorial approaches are computationally efficient for analyzing static PMS. A combinatorial binary decision diagram based method is discussed in detail. Methods to consider imperfect fault coverage and common-cause failures in the reliability analysis of PMS will also be presented.

23.1 Introduction

The operation of missions encountered in aerospace, nuclear power, and many other applications often involves several different tasks or phases that must be accomplished in sequence. Systems used in these missions are usually called phased-mission systems (PMS). A classic example is an aircraft flight that involves take-off, ascent, level-flight, descent, and landing phases. During each mission phase, the system has to accomplish a specified task and may be subject to different stresses as well as different dependability requirements. Thus, system configuration, success criteria, and component failure behavior may change from phase to phase [1]. This dynamic behavior usually requires a distinct model for each phase of the mission in the reliability analysis. Further complicating the analysis are statistical-dependencies across the phases for a given component. For example, the state of a component at the beginning of a new phase is identical to its state at the end of the previous phase in a non-repairable PMS [2]. The consideration of these dynamics and dependencies poses unique challenges to existing analysis methods.

Considerable research efforts have been expended in the reliability analysis of PMS over the past three decades. Generally, there are two classes of approaches to the evaluation of PMS: analytical modeling [1–5] and simulation [6, 7]. Simulation typically offers greater generality in system representation, but it is often more expensive in computational requirements [5]. On the other hand, analytical modeling techniques can incorporate a desirable combination of flexibility in representation as well as ease of solution. The analytical modeling approaches can be further categorized into three classes: state space oriented models [3, 5, 8–10], combinatorial methods [1, 2, 4, 11, 12], and a phase modular solution [13–16] that combines the former two methods as appropriate. The state space oriented approaches,

which are based on Markov chains and/or Petri nets, are flexible and powerful in modeling complex dependencies among system components. However, they suffer from state explosion when modeling large-scale systems. With an effort to deal with the state explosion problem of the state space oriented approaches, some researchers proposed combinatorial methods, which exploit Boolean algebra and various forms of decision diagrams to achieve low computational complexity and less storage space consumption.

This chapter will give a state-of-the-art review of the various analytical modeling methods. It then focuses on a combinatorial binary decision diagrams based method for the reliability analysis of a class of generalized PMS (GPMS). Traditionally in a PMS, the mission is assumed to fail if the system fails during any one phase [17]. GPMS extends this phase-OR failure requirement to the more general combinatorial phase requirement (CPR) [1]. The outcome of the GPMS may also exhibit multiple performance levels between binary outcome (success or failure). Methods to consider imperfect fault coverage and common-cause failures in the reliability analysis of GPMS will also be discussed in this chapter.

23.2 Types of Phased-mission Systems

PMS can be categorized in several ways:

- *Static versus dynamic PMS:* If the structure of the reliability model for any phase of PMS is combinatorial, *i.e.*, the failure of the mission in any phase depends only on the combinations of component failure events, the PMS is said to be static. If the order in which the component failure events occur affects the outcome, *i.e.*, the failure of the mission in any one phase depends on both the combinations of the component failure events and sequence of occurrence of input events, the PMS is said to be dynamic. Systems involving functional dependencies and/or spares management are also dynamic. In Section 23.3, various approaches to the analysis of static and dynamic PMS will be presented.
- *Repairable versus non-repairable PMS:* In a non-repairable PMS, once a component has failed in one phase, it remains failed in all later phases. In a repairable system, the state of the system depends on the failure characteristics of its components as well as the maintenance plans that are conducted on the system. Maintenance can be classified into three categories according to the reason why it is conducted [13]: 1) *failure-driven maintenance* occurs when maintaining a system upon the occurrence of a component failure; 2) *time-driven maintenance* is performed on a pre-determined schedule; and 3) *condition-driven maintenance* is performed based on the observed condition of a system, for example, a component is repairable whenever the component fails and the system does not fail; no repair is possible upon the system failure. Meshkat [13] investigated these maintenance plans and analysis of PMS with certain kinds of time-driven maintenance. Xing [18] studied the dependability modeling and analysis of PMS with the failure-driven maintenance and the scheduled maintenance. This chapter will focus on the reliability modeling and analysis of non-repairable PMS.
- *Coherent versus non-coherent PMS:* In a coherent PMS, each component contributes to the system state, and the system state worsens (at lease does not improve) with an additional component failure [19]. On the other hand, the structure function of a noncoherent system does not increase monotonically with the additional number of functioning components. Specifically, a noncoherent system can transit from a failed state to a good state by the failure of a component, or transit from a good state to a failed state by the repair of a component. In other words, both component failures and repairs can contribute to the system failure in a noncoherent system. The failure behavior of a noncoherent PMS can be described using noncoherent fault trees, which are characterized by inverse gates (for example, NOT and exclusive-OR gates) besides logic gates used in coherent fault trees. This chapter will focus on coherent PMS.

- *Series/phase-OR PMS versus combinatorial phase requirements (CPR):* In a series PMS, the entire mission fails if the system fails during any one phase [17]. For a PMS with CPR, its failure criterion can be expressed as a logical combination of phase failures in terms of phase-AND, phase-*K*-out-of-*N*, and phase-OR. Thus, a phase failure does not necessarily lead to a mission failure; it may just produce degraded performance of the mission [1].
- *Sequential versus dynamic choice of mission phases:* In a sequential PMS, the sequence of phases traversed by the system to accomplish its goals is always constituted by a single path from the first phase to the last one. Most of existing PMS analysis techniques focuses on the sequential PMS. There are indeed examples of PMS for which the sequence of phases is better represented by a more generic direct acyclic graph [9]. In this scenario, at the end of a phase, the next phase may be selected according to a probability distribution, or depending on the current internal state of the PMS. Methods for considering the probabilistic choice of mission phases were presented in [8, 9]. A brief discussion on these methods is also given in Section 23.3.2.2.

23.3 Analytical Modeling Techniques

Three classes of analytical approaches to the reliability analysis of coherent PMS are described in this section. Section 23.3.1 presents the combinatorial approaches to the analysis of static PMS. Section 23.3.2 presents the state space oriented methods. Section 23.3.3 presents the phase modular approach, which provides a combination of combinatorial solution for static phase modules and Markov chain solution for dynamic phase modules.

23.3.1 Combinatorial Approaches

Combinatorial methods for analyzing PMS assume that all components fail/behave *s*-independently within each phase. However, they deal with the *s*-dependence across phases for a given component.

23.3.1.1 The Mini-component Technique

Esary and Ziehms [4] proposed to deal with the *s*-dependence across phases by replacing the component in each phase with a system of components (called *mini-components*), performing *s*-independently and in series. For example, a component *A* in phase *j* of a non-repairable PMS is replaced by a set of *s*-independent mini-components $\{a_i\}_{i=1}^{j}$ in series. The relation between a component and its mini-components is: $A_j = a_1 \bullet a_2 \bullet \ldots \bullet a_j$, meaning that *A* is operational in phase *j* (represented by $A_j = 1$ or $\overline{A}_j = 0$) if and only if it has functioned in all the previous phases.

Figure 23.1 shows the reliability block diagram (RBD) and fault tree (FT) format of the mini-component solution. Esary and Ziehms [4] showed that reliability of the resulted new system after the above transformation is the same as the reliability of the original PMS. Most importantly, the evaluation of the new system can proceed without considering the *s*-dependence across phases for a given component.

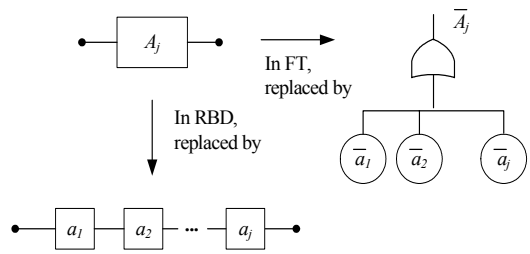


Figure 23.1. Mini-component method

Let *A(t)* be the state indicator variable of component *A*, and $q_{a_i}(t)$ be the failure function of mini-component a_i for component *A* in phase *i*, which conditionally depends on the survival of phase (*i*-1). The relationship between *A(t)* and $q_{a_i}(t)$ is:

$$q_{a_i}(t) = \begin{cases} \Pr(A(t) = 0) & i = 1, \\ \Pr(A(t + T_{i-1}) = 0 \mid A(T_{i-1}) = 1) & 1 < i \le j, t \le T_i. \end{cases} \quad (23.1)$$

In the system-level reliability analysis, $q_{a_i}(t)$ is given as the system input in the form of a

conditional failure distribution conditioned on the success of a_{i-1}.

Consider an example PMS with three components (A, B, and C) used in three non-overlapping consecutive phases (adapted from [3]). Figure 23.2 shows the failure criteria in each phase of the PMS in fault trees. In Phase 1, the system fails if all the three components fail. In Phase 2, the system fails if A fails or both B and C fail. In Phase 3, the system fails if any of the three components fails.

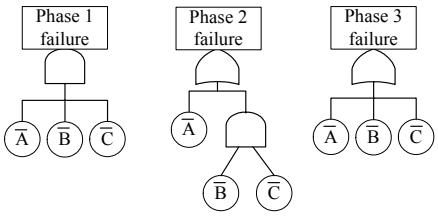


Figure 23.2. Fault tree model of a three-phase PMS

Figure 23.3 shows the equivalent system fault tree model in the mini-component method. Clearly the difficulty with this method is that the size of the problem becomes very large as the number of phases increases, for which a solution can be computationally very expensive.

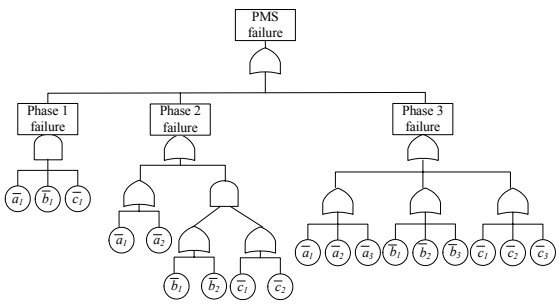


Figure 23.3. Equivalent mini-component system

23.3.1.2 The Boolean Algebraic Method

Another solution to the phased mission problem is to connect multiple phase models in series. Figure 23.4 shows the equivalent system at the end of mission in the Boolean algebraic method for the example PMS in Figure 23.2.

Based on the relation between a component and its mini-components, the failure function for component A in phase j can be calculated from $q_{a_i}(t)$ as (23.2):

$$F_{A_j}(t) = \begin{cases} q_{a_j}(t) & j = 1, \\ [1 - \prod_{i=1}^{j-1}(1 - q_{a_i}(T_i))] + [\prod_{i=1}^{j-1}(1 - q_{a_i}(T_i))] \bullet q_{a_j}(t) & j > 1 \end{cases} \quad (23.2)$$

where time t is measured from the beginning of phase j so that $0 \le t \le T_j$. T_j is the duration of phase j. The first term in (23.2) when $j > 1$ represents the probability that component A has already failed in the previous phases (1, 2, …, j-1). The second term denotes the probability distribution of lifetime of A in phase j.

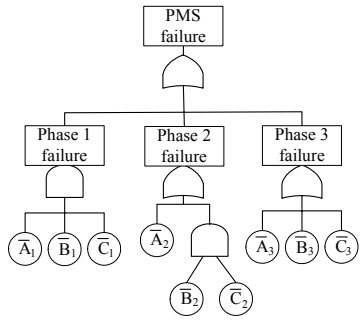


Figure 23.4. Example PMS in the Boolean algebra method

Because s-dependence exists among the same component in different phases, special treatment is needed for combination terms containing more than one A_i, $1 \le i \le m$, where m represents the total number of phases in the PMS. A set of Boolean algebraic rules called phase algebra rules was proposed to deal with the dependence (Table 23.1) [11, 20].

Table 23.1. Rules of phase algebra *($i < j$)*

$A_i \bullet A_j \to A_j$	$\overline{A}_i + \overline{A}_j \to \overline{A}_j$
$\overline{A}_i \bullet \overline{A}_j \to \overline{A}_i$	$A_i + A_j \to A_i$
$\overline{A}_i \bullet A_j \to 0$	$A_i + \overline{A}_j \to 1$

The phase algebra rules can be proved using the relation between the component and its mini-components ($A_j = a_1 \bullet a_2 \bullet \ldots \bullet a_j$) [2]:

- "$A_i \bullet A_j \to A_j$": the event "*A* is operational in phase *i* and the later phase *j*" is equivalent to the event "*A* is operational in the later phase *j*".

$$A_i \bullet A_j = (a_1 \bullet a_2 \bullet ... a_i)(a_1 \bullet a_2 \bullet ... a_j)$$
$$= a_1 \bullet a_2 \bullet ... a_j = A_j$$

- "$\overline{A}_i \bullet \overline{A}_j \to \overline{A}_i$": the event "*A* has failed in phase *i* and the later phase *j*" is equivalent to the event "*A* has failed in phase *i*".

$$\overline{A}_i \bullet \overline{A}_j = (a_1 \bullet a_2 \bullet ... a_i) \bullet \overline{(a_1 \bullet a_2 \bullet ... a_j)}$$
$$= \overline{a_1 \bullet a_2 \bullet ... a_i + a_1 \bullet a_2 \bullet ... a_j}$$
$$= \overline{a_1 \bullet a_2 \bullet ... a_i} = \overline{A}_i$$

- "$\overline{A}_i \bullet A_j \to 0$": the event "*A* has failed in phase *i*, but is operational in the later phase *j*" does not exist for a non-repairable PMS.

$$\overline{A}_i \bullet A_j = (\overline{a_1 \bullet a_2 \bullet ... a_i})(a_1 \bullet a_2 \bullet ... a_j)$$
$$= (\overline{a}_1 + \overline{a}_2 + ... + \overline{a}_i)(a_1 \bullet a_2 \bullet ... a_j) = 0$$

The three rules in the right column of Table 23.1 are just the complementary form of the rules in the left column, which have been proved in the above. Phase algebra rules do not account for $A_i \bullet \overline{A}_j$ and $\overline{A}_i + A_j$ combinations [2, 20]. $A_i \bullet \overline{A}_j$ means that *A* is operational until the end of phase *i* and then fails sometime between the end of phase *i* and the end of phase *j*; $\overline{A}_i + A_j$ has no physical meaning without considering repair. These phase algebra rules apply only to variables belonging to the same component.

23.3.1.3 Binary Decision Diagrams

Zang *et al.* [2] proposed a binary decision diagram (BDD) based method for the reliability analysis of static PMS with phase-OR requirement. As the first step of the method, phase algebra rules (Table 23.1) combined with heuristic variable ordering strategies are used to generate the PMS BDD model. Two types of ordering strategies were explored for variables that represent the same component in different phases: *forward* and *backward*. Thus, two types of phase-dependent operations (PDO) were proposed: *forward PDO* in which the variable order is the same as the phase order, and *backward PDO* in which the variable order is the reverse of the phase order. It is shown in [2] that in the PMS BDD generated by the backward PDO, the 0-edge always links two variables belonging to different components and the cancellation of common components can be done automatically during the generation of the BDD without any additional operation. So, the backward PDO is preferred in the PMS analysis.

After generating the PMS BDD, a recursive evaluation of the resulting PMS BDD yields the reliability/unreliability of the PMS. Special treatments are needed in the evaluation to deal with dependence among variables of the same component but different phases. The above BDD-based method [2] will be discussed in detail in Section 23.4.1. BDD-based methods for analyzing generalized PMS subject to imperfect fault coverage, modular imperfect coverage, and common-cause failures will also be discussed in Sections 23.4.2, 23.4.3, and 23.4.4, respectively.

23.3.2 State Space Based Approaches

Traditionally, if the failure criteria in any one phase of the PMS are dynamic, then a state space based approach must be used for the entire PMS. Section 23.3.2.1 presents Markov chains based methods for the reliability analysis of dynamic PMS. Section 23.3.2.2 presents Petri nets based methods for dynamic PMS analysis.

23.3.2.1 Markov Chains

Several different Markov chain based methods are available for the reliability analysis of PMS. The basic idea is to construct a single Markov chain to represent the failure behavior of the entire PMS or several Markov chains, each representing the failure behavior in each phase. These Markov models at once account for dependence among components within a phase as well as dependence across phases for a given component. Solving the Markov chain models yields the probability of the system being in each state. The system unreliability is obtained by summing all the failure state probabilities.

Specifically, Smotherman and Zemoudeh [5] (*SZ approach*) used a single non-homogeneous Markov chain model to perform the reliability analysis of a PMS. In their approach, the behavior of the system in each phase is represented using a different Markov chain, which may contain a different subset of states. The state transitions are described in terms of time dependent rates so as to include phase changes. Thus, state-dependent phase changes, random phase durations, time-varying failure and repair behavior can be easily modeled in the SZ approach.

Consider the example PMS in Figure 23.2. Assume the failure rates of the three components *A*, *B*, and *C* are *a*, *b*, and *c*, respectively. Figure 23.5 shows the Markov chain model of the entire PMS in the SZ approach. In the Markov chain representation, a 3-tuple represents a state indicating the status of the three components. A "1" represents the corresponding component is operational and a "0" represents the corresponding component has failed. For example, state (110) implies that *A* and *B* are operational and *C* has failed. A "F" represents a state in which the system has failed. A transition from one state to another state is associated with the failure rate of the failed component. The transitions $h_i(t)$ in Figure 23.5 represent the failure rates associated with the time at which phase changes occur.

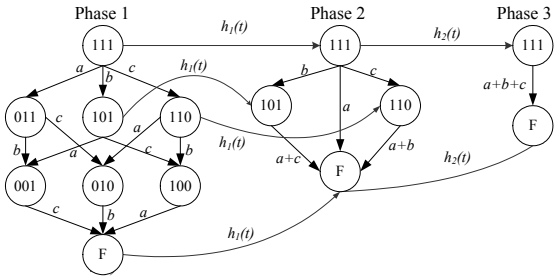


Figure 23.5. Markov chain model in the SZ approach

Since this model includes the configurations for all phases as well as the phase changes, it needs only be solved once. The major drawback of this approach, like the mini-component approach [4], is that a large overall model is needed. The size of the state space is as large as the sum of number of states in each of the individual phases. Since the state space associated with a Markov model of a system is exponential in the number of components in the worst case, the SZ method requires a large amount of storage and computational time to solve the model, thus limiting the type of system that can be analyzed.

Instead of generating and solving an overall Markov chain, Somani *et al*. [21] (*SRA approach*) suggested generating and solving separate Markov chains for individual phases of a PMS. The variation in failure criteria and system configuration from phase to phase is accommodated by providing an efficient mapping procedure at the transition time from one phase to another. While analyzing a phase, only states relevant to that phase are considered. Apparently, each individual Markov chain is much smaller than the overall Markov chain used in the SZ approach [5]. For the example three-phase PMS in Figure 23.2, Markov chains for the three phases are shown in Figure 23.5 (without considering the inter-phase mapping). In the SRA approach, three Markov chains with 8, 4, and 2 states, respectively, need to be solved. The reliability (or unreliability) of the system can be computed from the output of the last phase. While in the SZ approach, a single Markov chain with 12 states (after the three system failure states "F" are merged as one failure state) must be solved. Therefore, using the SRA approach, the computation time for large systems can be reduced significantly without compromising the accuracy of the results. Also, the SRA approach allows the phase duration to be modeled as fixed or random.

As another alternative to the reliability analysis of PMS using Markov models, Dugan [3] (*Dugan approach*) advocated generating a single Markov chain with state space equal to the union of the state spaces of the individual phases from the start. The transition rates are parameterized with phase numbers and the Markov chain is solved *n* times if the PMS has *n* phases. The final state probabilities of one phase become the initial state probabilities of the next phase. One potential source of the problem with the Dugan approach is that once a state is declared to be a system failure state in a phase, it cannot become an up state in a later phase. In practice, it is possible to have some states that are failure states in a phase but are up states in

a later phase. For example, if we swap the failure criteria of phase 1 and phase 3 in Figure 23.2, then the states of (011), (001), (010), and (100) are failure states in both phase 1 and phase 2, but are up states in phase 3. In the Dugan approach, all those states will be treated as forced failure states in phase 3. This problem would cause overestimated system unreliability.

23.3.2.2 Petri Nets

Mura and Bondavalli [9] (*MB approach*) proposed a hierarchical modeling and evaluation approach for analyzing PMS, where missions may evolve dynamically by selecting the next phase to perform according to the state of the system, and the duration of all phases are fixed and known in advance. Their approach combines the Markov analyses and Petri nets through a two-level modeling approach.

Specifically the upper level model in the MB approach is a single discrete-time Markov chain (DTMC), describing the overall behavior of the whole mission without any detail of the internal phase behavior. There are typically two absorbing states: loss of the entire mission and success of the mission. Each non-absorbing states in the DTMC represents a different phase in the mission. This allows simplifying the modeling of variety of mission scenarios by sequencing the phases in proper ways. Moreover, it allows probabilistic or dynamic choice of the mission phases according to the system states, which is not possible in other state space oriented approaches based only on Markov models. The lower level models are built using generalized stochastic Petri nets (GSPN). These lower level models are used to describe the system behavior inside each phase and they are built and solved separately. The separate modeling of each phase allows the reuse of the previously built models when the operation of a phase is repeated during the mission. The major advantages offered by the MB approach include the great flexibility by allowing the dynamic selection of mission phases and reusability of the defined phase models.

Later, Mura and Bondavalli [10] proposed a new methodology based on Markov regenerative stochastic Petri nets (MRSPN), which extended the MB approach by allowing random phase duration. This methodology is incorporated in the DEEM (dependability evaluation of multiple-phased systems) software package [8].

23.3.3 The Phase Modular Approach

Traditional approaches to PMS analysis are either combinatorial (Section 23.3.1) or state space based (Section 23.3.2). The combinatorial approaches are computationally efficient, but are applicable only when every phase of the PMS is static. Markov based approaches can capture the dynamic behavior such as functional dependencies, the sequence of failure events, and spares management. However, the major limitation with Markov methods is that if the failure criterion in only one phase is dynamic, then a Markov approach must be used for every phase. Due to the well-known state explosion problem of Markov approaches, it is often computationally intensive and even infeasible to solve the model.

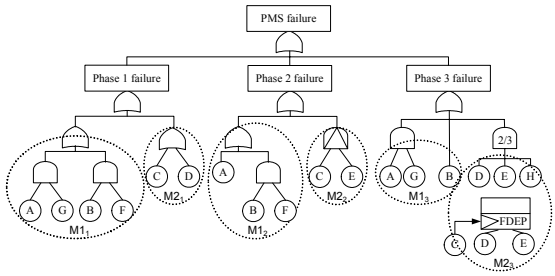


Figure 23.6. PMS fault free with defined modules

To take advantage of both types of solutions while addressing their limitations, a phase-modular fault tree approach employing both BDD and Markov-chain solution methods as appropriate was developed for the reliability analysis of PMS [13–16]. In applying this approach, first the modules of components that remain independent throughout the mission are identified, and then the reliability of each independent module in each phase is found using the appropriate solution technique. Finally, the modules are combined in a system-level BDD to find the system-level reliability. We illustrate the basic elements/steps of the phase-modular

approach using a simple example PMS, which has three phases and eight components (Figure 23.6) [22] as follows:

1) Represent each mission phase with a fault tree, and then link the phase fault trees with a system top event. For this example, the reliability of the PMS is the probability that the mission successfully achieves its objectives in all phases, the phase fault trees are linked using an OR gate to obtain the entire PMS fault tree.
2) Each phase fault tree is then divided into independent subtrees/modules. In Figure 23.6, Phase 1 fault tree has two main modules {A, G, B, F} and {C, D}. Phase 2 fault tree has two modules {A, B, F} and {C, E}. Phase 3 fault tree has three modules {A, G}, {B}, and {C, D, E, H}.
3) Characterize each phase module as static or dynamic. Static fault trees use only OR, AND, and *K*-out-of-*N* gates. Dynamic fault trees have at least one dynamic gate such as priority-AND gate, FDEP gate, or CSP/WSP/HSP gates. In Figure 23.6, both modules in Phase 1 fault tree are static; the module {A, B, F} in Phase 2 fault tree is static and the module {C, E} is dynamic; and Phase 3 fault tree has two static modules, {A, G} and {B}, and one dynamic module, {C, D, E, H}.
4) Identify each phase module as bottom-level (without child modules) or upper-level (with child modules). The module {C, D} in Phase 1 fault tree is a bottom-level module, and the module {A, G, B, F} is an upper-level module since it contains child modules {A, G} and {B, F} linked by an OR gate. The identification of child and parent modules is vital information used in solving for these modules' reliability.
5) Find the system-level independent modules. This identification is accomplished by finding the unions of components in all the phase modules that overlap in at least one component. The example PMS fault tree has two system-level independent modules, {A, B, F, G} and {C, D, E, H}.
6) Identify each system-level module as static or dynamic across the phases. Identification of a component as dynamic in at least one mission phase is sufficient for the identification of the corresponding system-level module as dynamic. In the example PMS, the system-level module {A, B, F, G} is static and {C, D, E, H} is dynamic.
7) Group the phase modules according to the corresponding system-level module. Components of {A, B, F, G} are labeled as $M1_i$ and components of {C, D, E, H} are labeled as $M2_i$, where i = mission phase (Figure 23.6). These are the modules that will be solved for the joint phase module probabilities.
8) Find the joint phase module probabilities for all system-level modules. The BDD method is used for modules that are static across all the phases, and the combined Markov chain method as presented in [13, 15] is used for modules identified as dynamic. Therefore, we can use the BDD method on the system-level module {A, B, F, G}; however, we must use the Markov chain method on the system-level module {C, D, E, H}.
9) Consider each module as a basic event of a static fault tree of the entire system and solve the corresponding fault tree using BDD to find the overall system reliability based on the reliability measures of the modules.

Each module's reliability is solved with a consideration of its own behavior in previous phases. For instance, for finding the reliability of $M1_2$, a combined BDD approach is used for $M1_1$ and $M1_2$; for finding the reliability of $M2_3$, the combined Markov chain approach is used for $M2_1$, $M2_2$, and $M2_3$. We then consider solving the static PMS fault tree with the basic events $M1_1$, $M2_1$, $M1_2$, $M2_2$, $M1_3$, and $M2_3$ using the combined BDD approach and the reliability measures for each individual phase module computed from previous steps. It is important to note that solving this simple PMS fault tree without using the modularization technique would involve solving a Markov chain with approximately 256 states, while the Markov chain involved in this example has a maximum of only 16 states. The phase-modular approach provides exact reliability measures for PMS with dynamic phases in an efficient manner. Readers may refer to [13, 15, 16] for more details about this approach.

23.4 BDD Based PMS Analysis

In this section, the binary decision diagrams (BDD) based approaches to the reliability analysis of PMS, PMS with imperfect fault coverage, and PMS with common-cause failures will be discussed. In the model for the BDD based PMS analysis, the following assumptions are made:

- Component failures are *s*-independent within each phase. Dependencies arise among different phases and different failure modes (when imperfect fault coverage is considered).
- Phase durations are deterministic.
- The system is not maintained during the mission; once a component transfers from the operation mode to a failure mode (either *covered* or *uncovered*), it will remain in that failure mode for the rest of the mission time.
- The system is coherent.

23.4.1 Traditional Phased-mission Systems

Reliability of a traditional phase-OR PMS is the probability that the mission successfully achieves the objective in all phases [17]. In the BDD-based method to the reliability analysis of PMS, three major steps are involved: 1) generating BDD for each phase fault tree, 2) combining single-phase BDD to obtain the entire PMS BDD, and 3) evaluating the PMS BDD to obtain the system reliability. Similar to the generation of BDD for non-PMS, the variable ordering can heavily affect the size of PMS BDD. Currently, there is no exact method of determining the best way of ordering basic events for a given fault tree structure. Fortunately, heuristics can usually be used to find a reasonable variable ordering.

In PMS, two kinds of variables need to be ordered: variables belonging to different components and variables that represent the same component in different phases. For the variables of different components, heuristics are typically used to find an adequate ordering. Several heuristics based on a depth-first search of the fault tree model can be found in [23]. For the variables of the same component in different phases, there are two ways to order them: *forward* and *backward*. In the forward method, the variable order is the same as the phase order, that is, $A_1 \prec A_2 \prec \ldots \prec A_m$, where A_i is the state variable of component A in phase i and m is the number of phases. In the backward method, the variable order is the reverse of the phase order, that is, $A_m \prec A_{m-1} \prec \ldots \prec A_1$.

After assigning each variable an index/order, for generating single-phase BDD in step 1), the traditional BDD operation rules based on Boolean algebra are applied. The reader may wish to review the traditional BDD operation rules in Chapter 38. In step 2), for combining single-phase BDD, dependence among variables of the same component but different phases is dealt with using the phase-dependent operation (PDO) [2]. According to the two ways to order variables of the same component, two types of PDO were developed: forward and backward. Assume component A is used in both phases i and j ($i < j$). A_i and A_j are state variables of A in phase i and phase j, respectively. A_i =0 or $\overline{A}_i$ =1 implies that A has failed in phase i. Using the *ite* format, the sub-BDD rooted at $\overline{A}_i$ and $\overline{A}_j$ respectively can be written as: $G = ite(\overline{A}_i, G_{\overline{A}_i=1}, G_{\overline{A}_i=0}) = ite(\overline{A}_i, G_1, G_2)$ and $H = ite(\overline{A}_j, H_{\overline{A}_j=1}, H_{\overline{A}_j=0}) = ite(\overline{A}_j, H_1, H_2)$. Let $\Diamond$ represent logic operation AND or OR, then we have:

$$G \Diamond H = ite(\overline{A}_i, G_1, G_2) \Diamond ite(\overline{A}_j, H_1, H_2) = \begin{cases} ite(\overline{A}_i, G_1 \Diamond H_1, G_2 \Diamond H) & \text{forward PDO} \\ ite(\overline{A}_j, G \Diamond H_1, G_2 \Diamond H_2) & \text{backward PDO} \end{cases} \quad (23.3)$$

The reader may refer to [2] for the proof of (23.3) using the phase algebra rules in Table 23.1. As discussed in Section 23.3.1.3, the backward PDO is preferred in the PMS analysis because in the PMS BDD generated by the backward PDO, the 0-edge always links two variables of different components and thus less dependence needs to be handled during the model evaluation.

Note that PDO of [2] is only applicable to non-repairable PMS. In addition, they can perform the task of combining BDD of individual phases into the overall PMS BDD correctly only given that the ordering strategies abide the following two rules:

- Orderings adopted in the generation of each single phase BDD are consistent or the same for all the phases.

- Orderings of variables that belong to the same component but to different phases stay together. In practice, this can be achieved by replacing each component indicator variable with a set of variables that represent this component in each phase after ordering components using heuristics.

These two rules are very stringent from the implementation point of view. Xing and Dugan relaxed the constraints by adding a removal procedure in the PMS BDD generation to allow arbitrary ordering strategies. For details, see [24].

After PMS BDD is generated, the final step to accomplish the reliability analysis is to evaluate the resulting PMS BDD. Note that 1-edges in the PMS BDD may link two variables of the same component but different phases. Dependence between these variables must be addressed during the evaluation. As a result, two different evaluation methods are needed for the PMS BDD generation. Specifically, consider the sub-BDD in Figure 23.7: The *ite* format is: $G = ite(x, G_1, G_2) = x \bullet G_1 + \bar{x} \bullet G_2$ $G_1 = ite(y, H_1, H_2) = y \bullet H_1 + \bar{y} \bullet H_2$. Let $p(x)$ be the failure probability of component represented by node x and P(G) be the unreliability with respect to the current sub-BDD rooted at node x. The recursive evaluation algorithm of PMS BDD is as follows:

- For 1-edge or 0-edge linking variables of different components, the evaluation method is the same as the ordinary BDD. For example, if x, y in Figure 23.7 belong to different components, the evaluation method is:

$$P(G)=P(G_1)+[1-p(x)]*[P(G_2)-P(G_1)] \quad (23.4)$$

- For 1-edge linking variables of the same component, for example, if x, y in Figure 23.7 belong to the same component, the evaluation method is:

$$P(G)= P(G_1)+[1-p(x)]* [P(G_2)-P(H_2)] \quad (23.5)$$

The phase algebra rules (Table 23.1) are applied to deal with the dependence between x and y in the derivation of (23.5). Refer to [2] for details of the derivation. Exit conditions of the recursive algorithm are: if G = 0, *i.e.*, the system is operational, then the unreliability P(G) = 0; if G = 1, *i.e.*, the system has failed, then P(G) = 1.

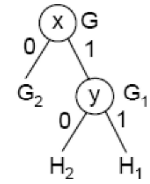


Figure 23.7. A PMS BDD branch

23.4.2 PMS with Imperfect Coverage

PMS, especially those devoted to safety-critical applications, such as aerospace and nuclear power, are typically designed with sufficient redundancies and automatic recovery mechanisms to be tolerant of faults or errors that may occur. However, the recovery mechanisms can fail, such that the system cannot adequately detect, locate, and recover from a fault occurring in the system. This uncovered fault can propagate through the system and may lead to an overall system failure, despite the presence of fault-tolerant mechanisms. As discussed in Chapter 22, the imperfect coverage (IPC) [25, 26] introduces multiple failure modes (*covered failure* and *uncovered failure*) that must be considered for accurate reliability analysis of fault-tolerant PMS. A covered component failure is local to the affected component; it may or may not lead to the system failure depending on the system configuration, failure criteria, and remaining redundancy. An uncovered component failure is globally malicious, and causes the system to crash.

This section presents a BDD-based approach called GPMS-CPR [1] for the reliability analysis of PMS with IPC, while considering the CPR and multiple performance levels for GPMS. The IPC behavior will be modeled using the fault/error handling model (FEHM) described in Figure 22.1. However, the near-coincident failure exit is not considered here. The probabilities of the three mutually exclusive exits R, C, and S in the FEHM are denoted as: r, c, and s, where $r + c + s = 1$.

The basic idea of the GPMS-CPR is to separate all the component uncovered failures from the combinatorics of the solution based on the simple and efficient algorithm (SEA) [1, 27] (Chapter 22) and the mini-component technique (Section 23.3.1.1). SEA represents a separable scheme for

incorporating IPC in the reliability analysis of single-phase systems. It cannot directly apply to PMS with *s*-dependence across phases. The mini-component concept can deal with the across-phase dependence. The basics of GPMS-CPR are to convert the PMS to an equivalent mini-component system so as to remove *s*-dependence, and then apply the SEA approach to address IPC. Figure 23.8 illustrates the GPMS-CPR approach.

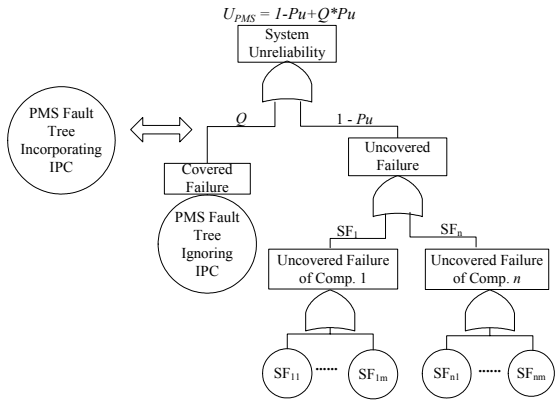


Figure 23.8. The separable GPMS-CPR approach

In Figure 23.8, SF_A denotes an event that component A fails uncovered. SF_A for different components are *s*-independent. SF_{a_i} represents an event that mini-component a_i fails uncovered. Different SF_{a_i} (i = 1,…,m) for the same component are not independent and the dependence must be addressed in the solution. The probability of no mini-component experiencing an uncovered failure (P_u) and the unreliability of the complementary perfect-coverage system (Q) are integrated using the total probability theorem:

$$U_{PMS} = 1 - P_u + Q * P_u \tag{23.6}$$

The derivation of (23.6) is similar to the derivation of the SEA in Chapter 22. Also, refer to [1] for details. The formulation of P_u in (23.6) is:

$$\begin{aligned} P_u &= \Pr(\overline{SF}_1 \cap \overline{SF}_2 \cap \ldots \cap \overline{SF}_n) \\ &= \prod_{A=1}^{n}(1 - \Pr(SF_A)) = \prod_{A=1}^{n}(1 - u[A]) \\ &= \prod_{A=1}^{n}(1 - u[A_m]) \end{aligned} \tag{23.7}$$

where n is the total number of components in the PMS, $u[A]$ is the probability that component A fails uncovered during the whole mission, that is, $u[A_m]$ is the probability that A has failed uncovered before the end of the last phase m. Let NF_{a_i}, CF_{a_i}, and SF_{a_i} denote events that A in phase i, namely, mini-component a_i does not fail, fails covered, and fails uncovered, respectively. The three events are mutually exclusive and complete. Define $n[a_i]$ = $\Pr(NF_{a_i})$, $c[a_i]$ = $\Pr(CF_{a_i})$, and $u[a_i]$ = $\Pr(SF_{a_i})$. According to the FEHM in Figure 22.1, these three probabilities can be calculated as:

$$\begin{aligned} n[a_i] &= 1 - q_{a_i}(t) + r_{a_i} \bullet q_{a_i}(t) \\ c[a_i] &= c_{a_i} \bullet q_{a_i}(t) \\ u[a_i] &= s_{a_i} \bullet q_{a_i}(t) \end{aligned} \tag{23.8}$$

Based on the relationship between a component and its mini-components depicted in Section 23.3.1.1 and on the fact that a component can fail uncovered in one phase only if it has survived all the previous phases, $u[A_j]$ can be calculated as:

$$\begin{aligned} u[A_j] &= \Pr(SF_{A_j}) \\ &= \Pr(A \text{ fails uncovered before the end of phase j}) \\ &= \Pr(\text{any mini - component } a_{i\in\{1\ldots j\}} \text{ fails uncovered}) \\ &= \Pr(SF_{a_1} \cup (NF_{a_1} \cap SF_{a_2}) \cup \ldots \\ &\qquad \cup (NF_{a_1} \cap \ldots \cap NF_{a_{j-1}} \cap SF_{a_j})) \\ &= u[a_1] + n[a_1] \bullet u[a_2] + \ldots \\ &\qquad + n[a_1] \bullet n[a_2] \bullet \ldots \bullet n[a_{j-1}] \bullet u[a_j] \\ &= u[a_1] + \sum_{i=2}^{j}(\prod_{k=1}^{i-1} n[a_k]) \bullet u[a_i] \end{aligned} \tag{23.9}$$

where j = 1, $u[A_1] = u[a_1]$. Similarly, the covered failure probability $c[A_j]$ and non-failure probability $n[A_j]$ can be calculated as in (23.10) and (23.11), respectively, when j = 1, $c[A_1 = c[a_1]$, $n[A_1] = n[a_1]$.

Next, consider the evaluation of perfect-coverage unreliability Q in (23.6). According to the SEA method, Q should be evaluated given that no component experiences an uncovered failure.

$$
\begin{aligned}
&c[A_j] = \Pr(CF_{A_j}) \\
&= \Pr(A \text{ fails covered before the end of phase j}) \\
&= \Pr(\text{any mini - component } a_{i\in\{1...j\}} \text{ fails covered}) \\
&= \Pr(CF_{a_1} \cup (NF_{a_1} \cap CF_{a_2}) \cup ... \\
&\qquad \cup (NF_{a_1} \cap ... \cap NF_{a_{j-1}} \cap CF_{a_j})) \\
&= c[a_1] + n[a_1] \bullet c[a_2] + ... \\
&\qquad + n[a_1] \bullet n[a_2] \bullet ... \bullet n[a_{j-1}] \bullet c[a_j] \\
&= c[a_1] + \sum_{i=2}^{j} (\prod_{k=1}^{i-1} n[a_k]) \bullet c[a_i]
\end{aligned}
\tag{23.10}
$$

$$
\begin{aligned}
&n[A_j] = \Pr(NF_{A_j}) \\
&= \Pr(A \text{ has not failed before the end of phase j}) \\
&= \Pr(\text{all mini - components } a_{i\in\{1...j\}} \text{ are not failed}) \\
&= \Pr(NF_{a_1} \cap ... \cap NF_{a_{j-1}} \cap NF_{a_j})) \\
&= n[a_1] \bullet n[a_2] \bullet ... \bullet n[a_{j-1}] \bullet n[a_j] = \prod_{i=1}^{j} n[a_i]
\end{aligned}
\tag{23.11}
$$

Therefore, before evaluating Q, the failure function of each component A in each phase j needs to be modified as a conditional failure probability, denoted by $F_{A_j}(t)$, conditioned on there being no uncovered failure during the whole mission, that is,

$$
F_{A_j}(t) = \Pr(CF_{A_j} \mid \overline{SF}_A) = \frac{c[A_j]}{1 - u[A]} = \frac{c[A_j]}{1 - u[A_m]} \tag{23.12}
$$

Using these modified component failure functions, Q can be evaluated using the efficient PMS BDD method that does not consider IPC [2] (Section 23.4.1). In summary, GPMS-CPR can be described as the following five-step algorithm:

1) Compute the modified failure probability for each component at the end of each phase using (23.12).
2) Order components using backward PDO and heuristics. Generate BDD for each phase.
3) According to the specified CPR and mission performance criteria, combine the single-phase BDD using phase algebra and backward PDO to obtain the final PMS BDD.
4) Evaluate Q recursively from the final PMS BDD using the algorithm of Section 23.4.1 and using $F_{A_j}(t)$ generated in step (1) as the component failure probability.
5) Evaluate the imperfect coverage probability (1 - P_u). Then integrate it with Q using (23.6) to obtain final GPMS unreliability/performance.

Due to the nature of BDD and the beauty of the SEA method, the GPMS-CPR method has low computational complexity and is easy to implement, as compared to the other potential methods such as Markov chain based methods. The Markov methods can address IPC by expanding the state space and number of transitions, worsening the state explosion problem [28]. In addition, the GPMS-CPR is capable of evaluating a wider range of more practical systems with less restrictive mission requirements, while offering more human-friendly performance indices such as multi-level grading as compared to the previous PMS methods. Next, we consider the analysis of a data gathering PMS using GPMS-CPR.

23.4.2.1 The Data Gathering System and Analysis

A space data gathering system [1], which is loosely based on a practical system in NASA, consists of four types of components that are used in different configurations over three consecutive phases (Figure 23.9):

- A_a, A_b: needed for all phases; one of them must be functional during all the three phases.
- B_a: only needed for phases 1 and 2; it must be functional during these two phases.
- C_a, C_b: work during phases 1 and 3; both must be functional during phase 1, at least one of them must be functional during phase 3.
- D_a, D_b, D_c: work during phases 2 and 3; all of them must be functional during phase 2, at least two of them must be functional during phase 3.

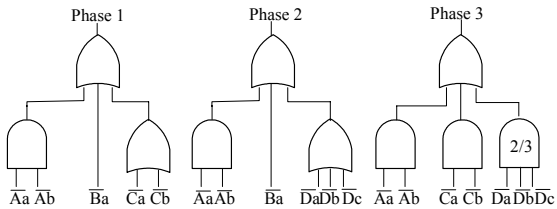


Figure 23.9. Data gathering system configuration

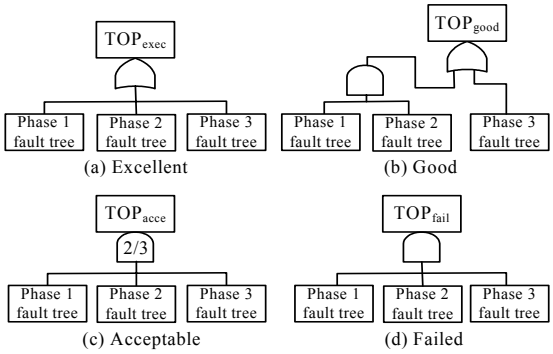


Figure 23.10. Four performance levels in the fault tree

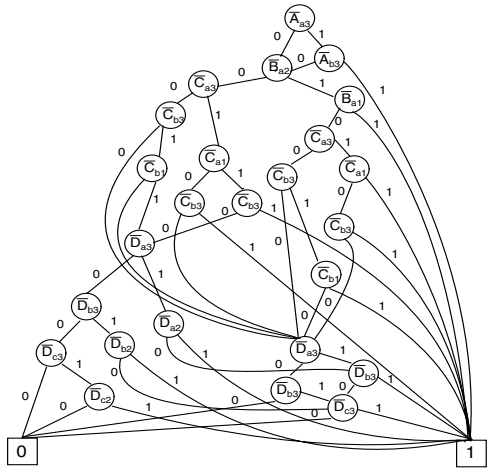


Figure 23.11. PMS BDD for the *good* level

According to the combination of data quality in the three phases, a four-performance-level result for the process can be defined as follows (Figure 23.10):

- *Excellent* level: data collection is successful in all the three phases.
- *Good* level: data collection is successful in phase 1 or 2 and in phase 3.
- *Acceptable* level: data collection is successful in only one of the three phases.
- *Failed* level: data collection fails in all the three phases.

Let P_{level} represent the multi-level reliability of the system, then we have:

$$P_{excellent} = 1 - \Pr(\text{TOP}_{\text{exce}}),$$
$$P_{good} = 1 - \Pr(\text{TOP}_{\text{good}}),$$
$$P_{acceptable} = \Pr(\text{TOP}_{\text{acce}}) - \Pr(\text{TOP}_{\text{fail}}),$$
$$P_{failed} = \Pr(\text{TOP}_{\text{fail}}). \quad (23.13)$$

For illustration purpose, the final PMS BDD for the *good* level is shown in Figure 23.11 [1]. The ordering of $A_a \prec A_b \prec B_a \prec C_a \prec C_b \prec D_a \prec D_b \prec D_c$ for variables of different components and backward ordering for variables of the same component and are used in the BDD generation.

By recursively traversing the PMS BDD of each performance level, the parameter Q in (23.6) is calculated. The U_{PMS}(level) is then found using (23.6). Lastly, the multi-level reliability P_{level} for each level is given as a simple and linear function of U_{PMS}(level) according to the corresponding grade-level performance criteria described in (23.13). Table 23.2 gives the input parameters (including phase duration, failure probabilities or rates, and coverage factors r, c, s) used in the analysis. Table 23.3 presents both the intermediate and final results for the analysis of the data gathering system.

Table 23.2. Input parameters (λ and λ_w are in 10^{-6}/hr; coverage factor r is 0 for all components in all phases)

Basic events	Phase 1 (33 hours)		Phase 2 (100 hours)		Phase 3 (67 hours)	
	p or λ	coverage c	p or λ	coverage c	p or λ	coverage c
A_a, A_b	0.0001	0.99	0.0001	0.99	0.0001	0.99
B_a	λ =1.5	0.97	λ =1.5	0.97	0.0001	0.97
C_a, C_b	0.0025	0.97	λ =1	0.99	λ_{Weibull} =1.6 α_{Weibull} =2	1
D_a, D_b, D_c	0.001	0.99	0.002	0.99	0.0001	0.97

Table 23.3. Analysis results of the data gathering system using GPMS-CPR

Performance level	Excellent	Good	Acceptable	Failed
P_u	0.999734	0.999734	0.999734	0.999734
Q	1.387e-2	1.261e-4	1.2602e-4	2.049e-7
$U_{PMS} = 1 - P_u + Q * P_u$.	0.0141326	3.9193e-4	3.9185e-4	2.6607e-4
Multi-level reliability: P_{level}	0.9858674	0.9996081	1.2578e-4	2.6607e-4

23.4.3 PMS with Modular Imperfect Coverage

In the traditional IPC, an uncovered component failure kills the entire mission. In the GPMS with CPR, however, the extent of the damage from an uncovered component fault can be just a phase loss, instead of the entire mission loss. Xing and Dugan proposed a generalized coverage model, called the modular imperfect coverage model (MIPCM) [29, 30], to exactly describe the behavior of a GPMS with CPR in the presence of a fault. As shown in Figure 23.12, MIPCM is a single entry, multiple exit black box. The model is activated when a fault occurs, and is exited when the fault is successfully handled or when the fault causes either a phase failure or the entire mission failure. The transient restoration exit R and permanent coverage exit C have the same meaning as in the traditional coverage model FEHM.

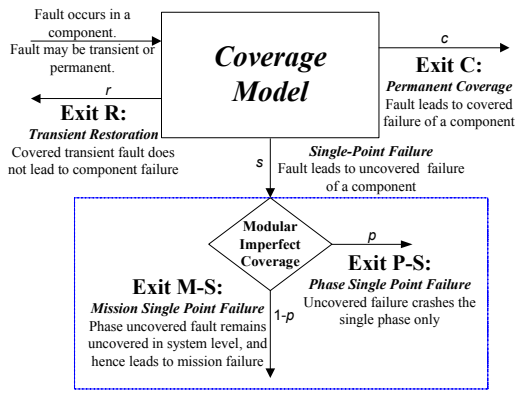


Figure 23.12. General structure of MIPCM

The following details the single-point failure exits. When a single fault (by itself) brings down a phase to which the fault belongs, single-point failure (or uncovered failure) is said to occur. Further, if such phase uncovered fault is covered at the higher system level, the phase single-point failure exit (labeled P-S) is reached, then a phase uncovered component failure occurs. If the phase uncovered fault remains uncovered at the system level, and hence leads to the failure of the entire mission, then the mission single-point failure exit (labeled M-S) is reached, and a mission uncovered failure is said to occur.

The four exits R, C, P-S, and M-S are mutually exclusive and complete. Define [*r, c, s*] to be the probability of taking the [transient restoration, permanent coverage, single-point failure] exit, given that a fault occurs, as in IPCM, and $r + c + s = 1$. Define p as a conditional probability that an uncovered fault fails a single phase, not the mission conditioned on an uncovered fault occurring in that phase. Then $s*p$ will be the probability of taking the P-S exit, and $s*(1-p)$ will be the probability of taking the M-S exit.

As compared with reliability analysis of PMS with traditional IPC, the analysis of GPMS with modular imperfect coverage (MIPC) is a more challenging task because the MIPC introduces more failure modes (covered failure, phase uncovered failure, and mission uncovered failure) and thus more dependencies into the system analysis. Building upon the above MIPCM, Xing and Dugan proposed two types of combinatorial methods for the reliability analysis of GPMS subject to MIPC: multi-state binary decision diagrams (MBDD) based method and ternary decision diagrams (TDD) based method. For each method, new phase algebra rules, new phase dependent operations for combining single-phase models into the overall system model, and new model evaluation algorithms were developed. The reader may refer to [29, 30] for the details of the MBDD-based method and the TDD-based method, respectively.

23.4.4 PMS with Common-cause Failures

Components in PMS can be subject to common-cause failures (CCF) during any phase of the mission. CCF are simultaneous component failures within a system that are a direct result of a common cause (CC) [31], such as extreme environmental conditions, design weaknesses, or human errors. It has been shown in many studies that the presence of CCF tends to increase a system's joint failure probabilities and thus contributes significantly to the overall unreliability of the system [32]. Therefore, it is crucial that CCF be modeled and analyzed appropriately. Considerable research efforts have been expended on the study of CCF for the system reliability analysis; refer to Chapter 38 for a discussion of various approaches, their contributions, and their limitations concerning the analysis of non-PMS. Actually, many of these limitations can also be found in the CCF models developed for PMS [33].

This section will present a separable solution that can address those limitations by allowing multiple CC to affect different subsets of system components and to occur *s*-dependently [34]. This separable approach is based on the efficient decomposition and aggregation (EDA) approach for the CCF analysis of single-phased systems (Chapter 38) and is easy to integrate into the existing PMS analysis methods.

Assume L_i elementary CC exists in each phase i of the PMS and they are denoted as: $CC_{11},.....,CC_{1L_1}$ for phase 1, $CC_{21},.....,CC_{2L_2}$ for phase 2, …, $CC_{m1},.....,CC_{mL_m}$ for the last phase m. Thus, total number of CC in PMS is: $L=\sum_{i=1}^{m}L_i$. According to the EDA approach, a common-cause event (CCE) space is built over a set of collectively exhaustive and mutually exclusive CCE that can occur in the PMS: $\Omega_{CCE}=\{CCE_1,CCE_2,...,CCE_{2^L}\}$. Each CCE in the set is a distinct and disjoint combination of elementary CC in the PMS:

$$CCE_1=\overline{CC_{11}}\cap...\cap\overline{CC_{1L_1}}\cap...\cap\overline{CC_{m1}}\cap...\cap\overline{CC_{mL_m}},$$
$$CCE_2=CC_{11}\cap...\cap\overline{CC_{1L_1}}\cap...\cap\overline{CC_{m1}}\cap...\cap\overline{CC_{mL_m}},$$
$$\cdots\cdots,$$
$$CCE_{2^L}=CC_{11}\cap...\cap CC_{1L_1}\cap...\cap CC_{m1}\cap...\cap CC_{mL_m}.$$

If $\Pr(CCE_j)$ denotes the occurrence probability of CCE_j, then $\sum_{j=1}^{2^L}\Pr(CCE_j)=1$ and $\Pr(CCE_i\cap CCE_j)=P(\phi)=0$ for any $i\neq j$.

As in the EDA approach, to find S_{CCE_j}, a set of components affected by event CCE_i is necessary. Define a common-cause group (CCG) as a set of components that are caused to fail due to the same CC. For non-PMS, S_{CCE_j} is simply the union of CCG whose corresponding CC occur. For example, assume $CCE_i=\overline{CC_1}\cap\overline{CC_2}\cap CC_3$ is a CCE in a non-PMS with three CC, S_{CCE_j} is simply equal to CCG_3 since CC_3 is the only active elementary CC. For a non-maintainable PMS, a component will remain failed in all later phases once it has failed in a phase. Therefore, S_{CCE_j} must be expanded to incorporate the affected components in all subsequent phases. The generation of S_{CCE_j} for PMS will be illustrated later on.

According to the total probability theorem, the unreliability of a PMS with CCF is calculated as:

$$U_{PMS}=\sum_{j=1}^{2^L}[\Pr(PMS\ fails\mid CCE_j)\Pr(CCE_j)] \quad (23.14)$$

$\Pr(PMS\ fails|CCE_j)$ in (23.14) is a conditional probability that the PMS fails conditioned on the occurrence of CCE_j. It is a reduced reliability problem, in which all components in S_{CCE_j} do not appear. Specifically, in the system fault tree model, each basic event appearing in S_{CCE_j} is replaced by a constant logic value "1" (true). After the replacement, a Boolean reduction can be applied to the PMS fault tree to generate a fault tree in which all components in S_{CCE_j} do not appear. Most importantly, the evaluation of the reduced problems can proceed without consideration of CCF. Thereby, the overall solution complexity is reduced.

Consider the *excellent* case of the data gathering PMS in Figure 23.9 with the following CCF scenario. The system is subject to CCF from hurricanes (denoted by CC_{11}) during phase 1, from lightning strikes (CC_{21}) during phase 2, and from floods (CC_{31}) during phase 3. A hurricane of sufficient intensity in phase 1 would cause A_a and C_a to fail, *i.e.*, $CCG_{11}=\{\overline{A_{a1}},\overline{C_{a1}}\}$, where A_{a1} is the

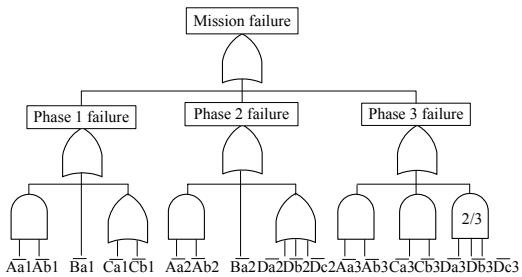
state indicator variable of component A_a in phase 1, and $\overline{A_{a1}}$ denotes the failure of A_a in phase 1. Serious lightning strikes in phase 2 would cause A_a, A_b, and B_a to fail, *i.e.*, $CCG_{21} = \{\overline{A_{a2}}, \overline{A_{b2}}, \overline{B_{a2}}\}$. Serious flooding in phase 3 would cause C_a and D_a to fail, *i.e.*, $CCG_{31} = \{\overline{C_{a3}}, \overline{D_{a3}}\}$. The probability of a hurricane occurring in phase 1 is $P_{CC_{11}} = 0.02$. The probability of a lightning strike occurring in phase 2 is $P_{CC_{21}} = 0.03$. Floods often occur in conjunction with hurricanes, and the *s*-dependence between the two CC can be defined by a set of conditional probabilities: the probability that floods occur in phase 3 conditioned on the occurrence of hurricanes in phase 1 is: $P_{CC_{31}|CC_{11}} = 0.6$. Similarly, $P_{CC_{31}|\overline{CC_{11}}} = 0.03$, $P_{\overline{CC_{31}}|CC_{11}} = 1 - P_{CC_{31}|CC_{11}}$, $P_{\overline{CC_{31}}|\overline{CC_{11}}} = 1 - P_{CC_{31}|\overline{CC_{11}}}$. These probabilities can typically be derived from available weather information.

Because there are three common causes in the example PMS, the CCE space is composed of $2^3 = 8$ CCE, as defined in the first column of Table 23.4. The second and third columns of the table show the set of components affected by each CCE (S_{CCE_j}) and occurrence probability calculation for each CCE based on statistical relation among those three CC, respectively.

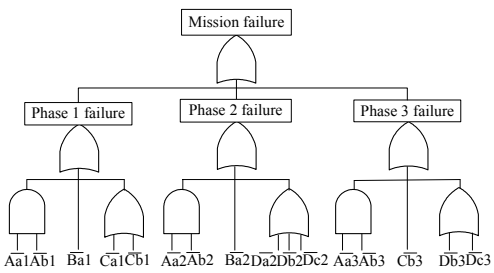
Table 23.4. CCE, affected components, and probabilities

CCE_i	S_{CCE_j}	$\Pr(CCE_i)$
$1: \overline{CC_{11}} \cap \overline{CC_{21}} \cap \overline{CC_{31}}$	ϕ	$P_{\overline{CC_{21}}} P_{\overline{CC_{11}}} P_{\overline{CC_{31}}\|\overline{CC_{11}}} = 0.9221$
$2: \overline{CC_{11}} \cap \overline{CC_{21}} \cap CC_{31}$	$\{\overline{C_{a3}}, \overline{D_{a3}}\}$	$P_{\overline{CC_{21}}} P_{\overline{CC_{11}}} P_{CC_{31}\|\overline{CC_{11}}} = 0.0285$
$3: \overline{CC_{11}} \cap CC_{21} \cap \overline{CC_{31}}$	$\{\overline{A_{a(2-3)}}, \overline{A_{b(2-3)}}, \overline{B_{a(2-3)}}\}$	$P_{CC_{21}} P_{\overline{CC_{11}}} P_{\overline{CC_{31}}\|\overline{CC_{11}}} = 0.0285$
$4: \overline{CC_{11}} \cap CC_{21} \cap CC_{31}$	$\{\overline{A_{a(2-3)}}, \overline{A_{b(2-3)}}, \overline{B_{a(2-3)}}, \overline{C_{a3}}, \overline{D_{a3}}\}$	$P_{CC_{21}} P_{\overline{CC_{11}}} P_{CC_{31}\|\overline{CC_{11}}} = 8.82e-4$
$5: CC_{11} \cap \overline{CC_{21}} \cap \overline{CC_{31}}$	$\{\overline{A_{a(1-3)}}, \overline{C_{a(1-3)}}\}$	$P_{\overline{CC_{21}}} P_{CC_{11}} P_{\overline{CC_{31}}\|CC_{11}} = 0.0078$
$6: CC_{11} \cap \overline{CC_{21}} \cap CC_{31}$	$\{\overline{A_{a(1-3)}}, \overline{C_{a(1-3)}}, \overline{D_{a3}}\}$	$P_{\overline{CC_{21}}} P_{CC_{11}} P_{CC_{31}\|CC_{11}} = 0.0116$
$7: CC_{11} \cap CC_{21} \cap \overline{CC_{31}}$	$\{\overline{A_{a(1-3)}}, \overline{C_{a(1-3)}}, \overline{A_{b(2-3)}}, \overline{B_{a(2-3)}}\}$	$P_{CC_{21}} P_{CC_{11}} P_{\overline{CC_{31}}\|CC_{11}} = 2.4e-4$
$8: CC_{11} \cap CC_{21} \cap CC_{31}$	$\{\overline{A_{a(1-3)}}, \overline{C_{a(1-3)}}, \overline{A_{b(2-3)}}, \overline{B_{a(2-3)}}, \overline{D_{a3}}\}$	$P_{CC_{21}} P_{CC_{11}} P_{CC_{31}\|CC_{11}} = 3.6e-4$

According to (23.14), the problem of evaluating the reliability of the data gathering system with CCF can be subdivided into eight reduced problems that need not consider CCF. Based on system configuration in Figure 23.9 and failure criteria for the *excellence* case described in Figure 23.10 (a), it is easy to derive that: Pr(PMS fails|CCE_j) = *1* for *j* = *3*...*8*. We apply the PMS BDD approach of [2] to evaluate the remaining two reduced problems, Pr(PMS fails|CCE_1) and Pr(PMS fails|CCE_2). Figure 23.13 (a) and (b) show the reduced fault tree models after applying the reduction procedure for removing components of S_{CCE_1} and S_{CCE_2}, respectively. Note that because no component is affected by CCE_1, the reduced fault tree in Figure 23.13(a) is actually the same as the original PMS fault tree (fault trees of the three phases in Figure 23.9 connected via an OR gate) but without considering CCF. Figures 23.14(a) and (b) show the PMS BDD generated from the fault tree models in Figures 23.13(a) and(b), respectively. Finally, results of the eight reduced problems are aggregated using (23.14) to obtain

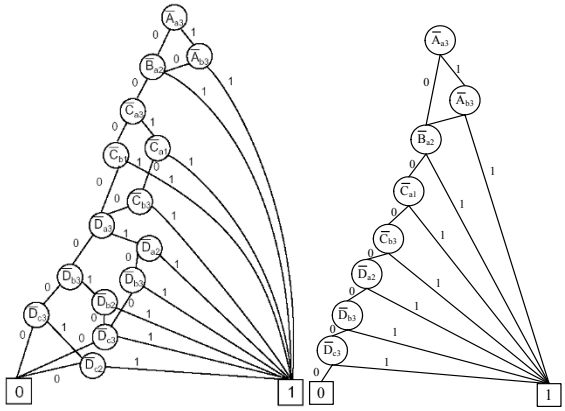


(a) PMS|CCE$_1$



(b) PMS|CCE$_2$

Figure 23.13. Reduced PMS fault trees



(a) PMS BDD|CCE$_1$ (b) PMS BDD|CCE$_2$

Figure 23.14. PMD BDD for reduced fault trees

the unreliability of the data gathering system with the consideration of CCF.

Figure 23.15 shows a conceptual overview of the separable approach for analyzing PMS with CCF. In summary, the methodology is to decompose an original PMS reliability problem with CCF into a number of reduced reliability problems based on the total probability theorem. The set of reduced problems does not have to consider dependence introduced by CCF, and thus can be solved using the efficient PMS BDD method [2]. Finally, the results of all reduced reliability problems are aggregated to obtain the entire PMS reliability considering CCF.

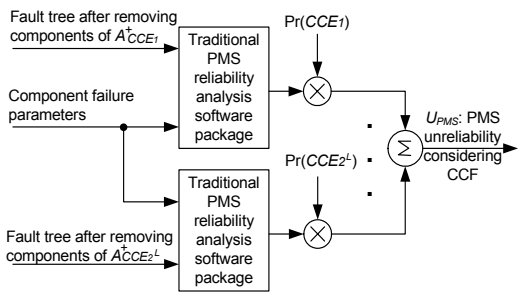


Figure 23.15. A conceptual overview

23.4.4.1 A Case Study: The Mars Orbiter System

To demonstrate this method, we considered a Mars orbiter mission system (originally described in [35]). As shown in the high-level dynamic fault tree (DFT) model of the system (Figure 23.16), this mission system involves launch, cruise, Mars orbit insertion (MOI), commissioning, and orbit phases. The triangles in the DFT are transfer gates to the DFT model for the Subsystem F.

Each mission phase is characterized by at least one major event in which the mission failure can occur. Examples of failure events for this system include the launch event during the launch phase, the deployment of the solar arrays (SA) and high-gain antennas (HGA), and the configuration of the heaters during the cruise phase, the propulsive capture into Mars' orbit during the MOI phase, and the release of an orbiting sample (OS) and the inclusion of a rendezvous and navigation (RAN) platform on the orbiter that might induce additional failure modes during orbit [35]. Table 23.5 gives occurrence probabilities of these failure events.

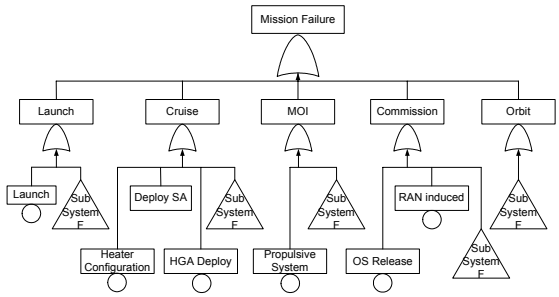


Figure 23.16. High-level DFT model

Table 23.5. Probabilities of failure events

Failure events	Probability
Launch	0.02
SA deployment	0.02
Heater configuration	0.02
HGA deployment	0.02
Propulsive capture	0.03
Orbiting sample release	0.02
RAN-induced failure	0.02

Subsystem F in Figure 23.16 consists of telecommunication, power, propulsion, the command and data handling system (CDS), the attitude control system (ACS), and thermal subsystems, which are connected through an OR gate (Figure 23.17).

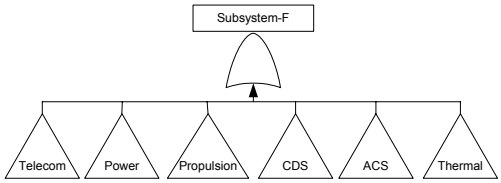


Figure 23.17. Fault tree of subsystem F

As described in [35], these subsystems can be subject to CCF due to two independent CC: CC_1 is a micrometeoroid attack that results in the failure of the entire system, and CC_2 is a solar flare that fails the subsystem's electronics, most notably the CDS in all pre-MOI phases. The orbiter will not be affected by solar flares after the MOI phase due to the increased distance of the orbiter from the sun. Assume that the occurrence probabilities of CC_1 and CC_2 are 0.01 and 0.02, respectively. Table 23.6 specifies the four CCE generated from the two CC, the set of components affected by CCE_i, and occurrence probability of each CCE_i, $\Pr(CCE_i)$.

A review of Table 23.6 implies that the CDS subsystem is the only subsystem affected by both CC_1 and CC_2 and therefore its failure will receive further analysis in this example. Figure 23.18 shows the fault tree model of the CDS subsystem.

Table 23.6. CCE, affected components, and probabilities

CCE_i	S_{CCE_j}	$\Pr(CCE_i)$
$CCE_1 = \overline{CC_1} \cap \overline{CC_2}$	ϕ	9.702e-1
$CCE_2 = CC_1 \cap \overline{CC_2}$	all spacecraft elements	9.980e-3
$CCE_3 = \overline{CC_1} \cap CC_2$	CDS	1.980e-2
$CCE_4 = CC_1 \cap CC_2$	all spacecraft elements	2.000e-4

Table 23.7 gives the failure rates for the CDS components and for the rest of the components (subsystems) of the subsystem F in each phase, as well as the phase duration. According to (23.14), the problem of evaluating the unreliability of the orbiter system with CCF is decomposed into four reduced problems that need not consider CCF. Based on the fault trees in Figures 23.16 through 23.18, we can derive that $\Pr(\text{orbiter fails}| CCE_i) = 1$ for $i = 2$, 3, and 4. Solving the phase-mission fault tree for a mission duration of 97368 hours using the PMS BDD method yields 0.14661 for $\Pr(\text{Orbiter fails}|CCE_1)$. Finally, according to (23.14), the unreliability of the proposed Mar's orbiter system with CCF is 0.172. This result is obtained by aggregating the results of $\Pr(\text{Orbiter fails} | CCE_i)$ and $\Pr(CCE_i)$ given in Table 23.6.

Table 23.7. Failure rates (10^{-7}/hr) of components in CDS and subsystem F

CDS components/ subsystem in F	Launch (504 hrs)	Cruise (5040 hrs)	MOI (144 hrs)	Comm. (4080 hrs)	Orbit (87600 hrs)
EPS-interface	0.05	0.04	0.05	0.05	0.04
Mass memory	0.02	0.01	0.02	0.02	0.01
AC-DC converter	0.02	0.01	0.02	0.02	0.01
CMIC (A and B)	0.03	0.02	0.03	0.03	0.02
FlightProc (A and B)	0.04	0.03	0.04	0.04	0.03
Bus (A and B)	0.02	0.01	0.02	0.02	0.01
IO-card (A and B)	0.02	0.01	0.02	0.02	0.01
PACI-card	0.01	0.005	0.01	0.01	0.005
ULDL-card	0.01	0.005	0.01	0.01	0.005
Telecommunication	0.03	0.2	0.3	0.3	0.2
Power	0.02	0.1	0.2	0.2	0.1
Propulsion	0.3	0.2	0.3	0.3	0.2
ACS	0.04	0.03	0.04	0.04	0.03
Thermal	0.02	0.01	0.02	0.02	0.01

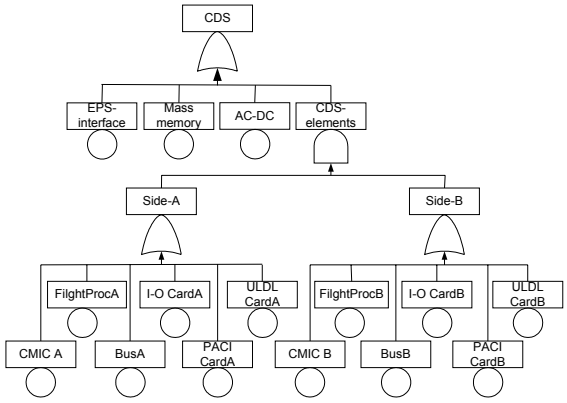


Figure 23.18. DFT model of the CDS

23.5 Conclusions

This chapter presented three classes of analytical approaches to the reliability analysis of PMS, which subject to multiple, consecutive, and non-overlapping phases of operations. The combinatorial approaches are computationally efficient but are limited to the analysis of static PMS only. The state space oriented approaches are powerful in modeling the various dynamic behaviors and dependencies, but are limited to the analysis of small-scale systems due to the state explosion problem. A better solution is the phase modular approach that combines the advantages of both combinatorial analyses and state space oriented analyses. This chapter also discussed the efficient BDD based methods to the analysis of PMS with imperfect coverage or common-cause failures in detail. Since they are combinatorial, the BDD-based methods are applicable to static PMS only. Recently, a separable solution based on the phase modular approach was proposed for the reliability analysis of dynamic PMS subject to CCF. The reader may refer to [22] for details.

References

[1] Xing L, Dugan JB. Analysis of generalized phased-mission systems reliability, performance and sensitivity. IEEE Transactions on Reliability 2002; 51(2): 199–211.

[2] Zang X, Sun H, Trivedi KS. A BDD-based algorithm for reliability analysis of phased-mission systems. IEEE Transactions on Reliability 1999; 48(1): 50−60.

[3] Dugan JB. Automated analysis of phased-mission reliability. IEEE Transactions on Reliability 1991; 40(1): 45−52, 55.

[4] Esary JD, Ziehms H. Reliability analysis of phased missions. In: Barlow RE, Fussell JB, Singpurwalla ND, editors. Reliability and fault tree analysis: Theoretical and applied aspects of system reliability and safety assessment. Philadelphia, PA, SIAM, 1975; 213−236,

[5] Smotherman MK, Zemoudeh K. A non-homogeneous Markov model for phased-mission reliability analysis. IEEE Transactions on Reliability 1989; 38(5): 585−590.

[6] Altschul RE, Nagel PM. The efficient simulation of phased fault trees. Proceedings of IEEE Annual Reliability and Maintainability Symposium, Philadelphia, PA, Jan. 1987; 292−296.

[7] Tillman FA, Lie CH, Hwang CL. Simulation model of mission effectiveness for military systems. IEEE Transactions on Reliability 1978; R-27: 191−194.

[8] Bondavalli A, Chiaradonna S, Di Giandomenico F, Mura I. Dependability modeling and evaluation of multiple-phased systems using DEEM. IEEE Transactions on Reliability 2004; 53(4): 509−522.

[9] Mura I, Bondavalli A. Hierarchical modeling and evaluation of phased-mission systems. IEEE Transactions on Reliability 1999; 48(4): 360−368.

[10] Mura I, Bondavalli A. Markov regenerative stochastic Petri nets to model and evaluate phased mission systems dependability. IEEE Transactions on Computers 2001; 50(12): 1337−1351.

[11] Somani AK, Trivedi KS. Boolean algebraic methods for phased-mission system analysis. Technical Report NAS1-19480, NASA Langley Research Center, Hampton, VA, 1997.

[12] Tang Z, Dugan JB. BDD-based reliability analysis of phased-mission systems with multimode failures. IEEE Transactions on Reliability 2006; 55(2): 350−360.

[13] Meshkat L. Dependency modeling and phase analysis for embedded computer based systems. Ph.D Dissertation, Systems Engineering, University of Virginia, 2000.

[14] Meshkat L, Xing L, Donohue S, Ou Y. An overview of the phase-modular fault tree approach to phased-mission system analysis. Proceedings of the 1st International Conference on Space Mission Challenges for Information Technology, Pasadena, CA, July 2003; 393−398.

[15] Ou Y. Dependability and sensitivity analysis of multi-phase systems using Markov chains. PhD Dissertation, Electrical and Computer Engineering, University of Virginia, 2002; May.
[16] Ou Y, Dugan JB. Modular solution of dynamic multi-phase systems. IEEE Transactions on Reliability 2004; 53(4): 499−508.
[17] Alam M, Al-Saggaf UM. Quantitative reliability evaluation of repairable phased-mission systems using Markov approach. IEEE Transactions on Reliability 1986; R-35(5): 498−503.
[18] Xing L. Dependability modeling and analysis of hierarchical computer-based systems. Ph.D. Dissertation, Electrical and Computer Engineering, University of Virginia, 2002; May.
[19] Andrews JD, Beeson S. Birnbaum's measure of component importance for noncoherent systems. IEEE Transactions on Reliability 2003; 52(2): 213−219.
[20] Somani AK, Trivedi KS. Phased-mission system analysis using Boolean algebraic methods. Proceedings of the ACM Sigmetrics Conference on Measurement and Modeling of Computer Systems 1994; 98−107.
[21] Somani AK, Ritcey JA, Au S. Computationally efficient phased-mission reliability analysis for systems with variable configuration. IEEE Transactions on Reliability 1992; 42: 504−511.
[22] Xing L, Meshkat L, Donohue S. An efficient approach for the reliability analysis of phased-mission systems with dependent failures. Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management, New Orleans, LA, May 14–18, 2006.
[23] Bouissou M, Bruyere F, Rauzy A. BDD based fault-tree processing: a comparison of variable ordering heuristics. Proceedings of ESREL Conference 1997.
[24] Xing L, Dugan JB. Comments on PMS BDD generation in "a BDD-based algorithm for reliability analysis of phased-mission systems". IEEE Transactions on Reliability 2004; 53(2): 169−173.
[25] Doyle SA, Dugan JB, Patterson-Hine A. A combinatorial approach to modeling imperfect coverage. IEEE Transactions on Reliability 1995; 44(1): 87−94.
[26] Dugan JB, Doyle SA. New results in fault-tree analysis. Tutorial notes of the Annual Reliability and Maintainability Symposium, Philadelphia, PA, Jan. 1997.
[27] Amari SV, Dugan JB, Misra RB. A separable method for incorporating imperfect coverage in combinatorial model. IEEE Transactions on Reliability 1999; 48(3): 267−274.
[28] Gulati R, Dugan JB. A modular approach for analyzing static and dynamic fault trees. Proceedings of the Annual Reliability and Maintainability Symposium 1997.
[29] Xing L, Dugan JB. Generalized imperfect coverage phased-mission analysis. Proceedings of the Annual Reliability and Maintainability Symposium 2002; 112−119.
[30] Xing L, Dugan JB. A separable TDD-based analysis of generalized phased-mission reliability. IEEE Transactions on Reliability 2004; 53(2): 174−184.
[31] Rausand M, Hoyland A. System reliability theory: models, statistical methods, and applications (2nd edition). Wiley Inter-Science, New Jersey, 2004.
[32] Vaurio JK. An implicit method for incorporating common-cause failures in system analysis. IEEE Transactions on Reliability 1998; 47(2): 173−180.
[33] Tang Z, Xu H, Dugan JB. Reliability analysis of phased mission systems with common cause failures. Proceedings of the Annual Reliability and Maintainability Symposium, Washington D.C., Jan. 2005; 313−318.
[34] Xing L. Phased-mission reliability and safety in the presence of common-cause failures. Proceedings of the 21st International System Safety Conference, Ottawa, Ontario, Canada 2003.
[35] Xing L, Meshkat L, Donohue S. Reliability analysis of hierarchical computer-based systems subject to common-cause failures. Reliability Engineering and System Safety 2007; 92(3): 351−359.

24

Reliability of Semi-Markov Systems in Discrete Time: Modeling and Estimation

Vlad Stefan Barbu[1] and Nikolaos Limnios[2]

[1]Université de Rouen, Laboratoire de Mathématiques Raphäel Salem, UMR 6085, Avenue de l'Université, BP 12, F76801, Saint-Étienne-du-Rouvray, France
[2]Université de Technologie de Compiègne, Laboratoire de Mathématiques Appliquées de Compiègne, BP 20529, 60205, Compiègne, France

Abstract: This chapter presents the reliability of discrete-time semi-Markov systems. After some basic definitions and notation, we obtain explicit forms for reliability indicators. We propose non-parametric estimators for reliability, availability, failure rate, mean hitting times and we study their asymptotic properties. Finally, we present a three state example with detailed calculations and numerical evaluations.

24.1 Introduction

In the last 50 years, a lot of work has been carried out in the field of probabilistic and statistical methods in reliability. We do not intend to provide here an overview of the field, but only to point out some bibliographical references that are close to the work presented in this chapter. More precisely, we are interested in discrete-time models for reliability and in models based on semi-Markov processes that extend the classical *i.i.d.* or Markovian approaches. The generality is important, because we pass from a geometric distributed sojourn time in the Markov case, to a general distribution on the set of non-negative integers $\mathbb{N}$, like the discrete-time Weibull distribution.

It is worth noticing here that most mathematical models for reliability consider time to be continuous. However, there are real situations when systems have natural discrete lifetimes. We can cite here those systems working on demand, those working on cycles or those monitored only at certain discrete times (once a month, say). In such situations, the lifetimes are expressed in terms of the number of working periods, the number of working cycles or the number of months before failure. In other words, all these lifetimes are intrinsically discrete. However, even in the continuous-time modeling case, we pass to the numerical calculus by first discetizing the concerned model. A good overview of discrete probability distributions used in reliability theory can be found in [1].

Several authors have studied discrete-time models for reliability in a general *i.i.d.* setting (see [1–4]). The discrete-time reliability modeling via homogeneous and non-homogeneous Markov chains can be found in [5, 6]. Statistical estimations and asymptotic properties for

reliability metrics, using discrete-time homogeneous Markov chains, are presented in [7]. The continuous-time semi-Markov model in reliability can be found in [8–10].

As compared to the attention given to the continuous-time semi-Markov processes and related inference problems, the discrete-time semi-Markov processes (DTSMP) are less studied. For an introduction to discrete-time renewal processes, see, for instance, [11]; an introduction to DTSMP can be found in [12–14]. The reliability of discrete-time semi Markov systems is investigated in [14–18] and in [22].

We present here a detailed modeling of reliability, availability, failure rate and mean times, with closed form solutions and statistical estimation based on a censured trajectory in the time interval $[0,M]$. The discrete time modeling presented here is more adapted to applications and is numerically easy to implement using computer software, in order to compute and estimate the above metrics.

The present chapter is structured as follows. In Section 24.2, we define homogeneous discrete-time Markov renewal processes, homogeneous semi-Markov chains and we establish some basic notation. In Section 24.3, we consider a repairable discrete-time semi-Markov system and obtain explicit forms for reliability measures: reliability, availability, failure rate and mean hitting times. Section 24.4 is devoted to the non-parametric estimation. We first obtain estimators for the characteristics of a semi-Markov system. Then, we propose estimators for measures of the reliability and we present their asymptotic properties. We end this chapter by a numerical application.

24.2 The Semi-Markov Setting

In this section we define the discrete-time semi-Markov model, introduce the basic notation and definitions and present some probabilistic results on semi-Markov chains.

Consider a random system with finite state space $E=\{1,\ldots,s\}$. We denote by $\mathcal{M}_E$ the set of matrices on $E\times E$ and by $\mathcal{M}_E(\mathbb{N})$ the set of matrix-valued functions defined on the set of non-negative integers $\mathbb{N}$, with values in $\mathcal{M}_E$. For $A\in\mathcal{M}_E(\mathbb{N})$, we write $A=(A(k);k\in\mathbb{N})$, where, for $k\in\mathbb{N}$ fixed, $A(k)=(A_{ij}(k);k\in E)\in\mathcal{M}_E$. Put $\mathbf{I}_E\in\mathcal{M}_E$ for the identity matrix and $\mathbf{0}_E\in\mathcal{M}_E$ for the null matrix.

We suppose that the evolution in time of the system is described by the following chains (see Figure 24.1.):

- The chain $J=(J_n)_{n\in\mathbb{N}}$ with state space E, where J_n is the system state at the n th jump time.
- The chain $S=(S_n)_{n\in\mathbb{N}}$ with state space $\mathbb{N}$, where S_n is the n th jump time. We suppose that $S_0=0$ and $0<S_1<S_2<\ldots<S_n<S_{n+1}<\ldots$.
- The chain $X=(X_n)_{n\in\mathbb{N}^*}$ with state space $\mathbb{N}^*$, where X_n is the sojourn time in state J_{n-1} before the n th jump. Thus, for all $n\in\mathbb{N}^*$, we have $X_n=S_n-S_{n-1}$.

A fundamental notion for semi-Markov systems is that of semi-Markov kernel in discrete time.

Definition 1: A matrix-valued function $\mathbf{q}\in\mathcal{M}_E(\mathbb{N})$ is said to be *a discrete-time semi-Markov kernel* if it satisfies the following three properties:

1. $0\le q_{ij}(k)\le 1, i,j\in E, k\in\mathbb{N}$;
2. $q_{ij}(0)=0$ and $\sum_{k=0}^{\infty} q_{ij}(k)\le 1, i,j\in E$;
3. $\sum_{k=0}^{\infty}\sum_{j\in E} q_{ij}(k)=1, i\in E$.

Definition 2: The chain $(J,S)=(J_n,S_n)_{n\in\mathbb{N}}$ is said to be *a Markov renewal chain* (MRC) if for all $n\in\mathbb{N}$, for all $i,j\in E$ and for all $k\in\mathbb{N}$ it satisfies almost surely

$$\mathbb{P}(J_{n+1}=j,S_{n+1}-S_{n+1}=k\,|\,J_0,\ldots J_n,S_0,\ldots S_n)$$
$$=\mathbb{P}(J_{n+1}=j,S_{n+1}-S_{n+1}=k\,|\,J_n).$$

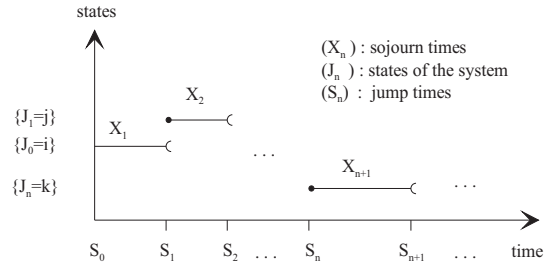


Figure 24.1. A typical sample path of a Markov renewal chain

Moreover, if the previous equation is independent of n, (J,S) is said to be homogeneous and the discrete-time semi-Markov kernel $\mathbf{q}$ is defined by

$$q_{ij}(k) := \mathbb{P}(J_{n+1} = j, X_{n+1} = k \big| J_n = i).$$

Figure 24.1 provides a representation of the evolution of the system.

We also introduce the cumulative semi-Markov kernel as the matrix-valued function $\mathbf{Q} = (\mathbf{Q}(k); k \in \mathbb{N}) \in \mathcal{M}_E(\mathbb{N})$ defined by

$$\begin{aligned} Q_{ij}(k) &:= \mathbb{P}(J_{n+1} = j, X_{n+1} \le k \big| J_n = i) \\ &= \sum_{l=0}^{k} q_{ij}(l), i, j \in E, k \in \mathbb{N}. \end{aligned} \tag{24.1}$$

Note that for (J,S) a Markov renewal chain, we can easily see that $(J_n)_{n\in\mathbb{N}}$ is a Markov chain, called *the embedded Markov chain associated to MRC* (J,S). We denote by $\mathbf{p} = (p_{ij})_{i,j\in E} \in \mathcal{M}_E$ the transition matrix of $(J_n)_{n\in\mathbb{N}}$ defined by

$$p_{ij} = \mathbb{P}(J_{n+1} = j \big| J_n = i), i, j \in E, n \in \mathbb{N}.$$

We also assume that $p_{ii} = 0$, $q_{ii}(k) = 0$, $i \in E$, $k \in \mathbb{N}$, *i.e.,* we do not allow transitions to the same state. Let us define now the conditional sojourn time distributions depending on the next state to be visited and the sojourn time distributions in a given state.

Definition 3: For all $i, j \in E$, let us define:

1. $f_{ij}(\cdot)$, the conditional distribution of $X_{n+1}, n \in \mathbb{N}$,

$$f_{ij}(k) := \mathbb{P}(X_{n+1} = k \big| J_n = i, J_{n+1} = j), k \in \mathbb{N}.$$

2. $F_{ij}(\cdot)$, the conditional cumulative distribution of $X_{n+1}, n \in \mathbf{N}$,

$$\begin{aligned} F_{ij}(k) &:= \mathbb{P}(X_{n+1} \le k \big| J_n = i, J_{n+1} = j) \\ &= \sum_{l=0}^{k} f_{ij}(l), k \in \mathbb{N}. \end{aligned}$$

Obviously, for all $i, j \in E$ and for all $k \in \mathbb{N} \cup \{\infty\}$, we have

$$f_{ij}(k) = \begin{cases} q_{ij}(k) / p_{ij}, \text{ if } p_{ij} \neq 0, \\ \mathbf{1}_{\{k=\infty\}}, \text{ if } p_{ij} = 0. \end{cases}$$

Definition 4: For all $i \in E$, let us define:

1. $h_i(\cdot)$, the sojourn time distribution in state i:

$$h_i(k) := \mathbb{P}(X_{n+1} = k \big| J_n = i) = \sum_{j\in E} q_{ij}(k), k \in \mathbb{N}.$$

2. $H_i(\cdot)$, the sojourn time cumulative distribution function in state i:

$$H_i(k) := \mathbb{P}(X_{n+1} \le k \big| J_n = i) = \sum_{l=0}^{k} h_i(l), k \in \mathbb{N}.$$

We consider that in each state i the chain stays at least one time unit, *i.e.*, for any state j we have

$$f_{ij}(0) = q_{ij}(0) = h_i(0) = 0.$$

Let us also denote by m_i the mean sojourn time in a state $i \in E$,

$$m_i = \mathbb{E}(S_1 \big| J_0 = i) = \sum_{k\ge 0} (1 - H_i(k)).$$

For G the cumulative distribution function of a certain *r.v.* X, we denote its *survival function* by $\overline{G}(k) = 1 - G(k) = \mathbf{P}(X > k), k \in \mathbb{N}$. Thus, for all states $i, j \in E$, we put $\overline{F_{ij}}$ and $\overline{H_i}$ for the corresponding survival functions.

The operation which will be commonly used when working on the space $\mathcal{M}_E(\mathbb{N})$ of matrix-valued functions will be the discrete-time matrix convolution product. In the sequel we recall its definition, we see that there exists an identity element, we define recursively the n-fold convolution and we introduce the notion of the inverse in the convolution sense.

Definition 5: Let $\mathrm{A},\mathrm{B}\in\mathcal{M}_E(\mathbb{N})$ be two matrix-valued functions. *The matrix convolution product* $A*B$ is a matrix-valued function $\mathrm{C}\in\mathcal{M}_E(\mathbb{N})$ defined by

$$C_{ij}(k):=\sum_{r\in E}\sum_{l=0}^{k}A_{ir}(k-l)B_{rj}(l),i,j\in E,k\in\mathbb{N}.$$

The following result concerns the existence of the identity element for the matrix convolution product in discrete time.

Lemma 1: Let $\delta I=(d_{ij}(k);i,j\in E)\in\mathcal{M}_E(\mathbb{N})$ be the matrix-valued function defined by

$$d_{ij}(k):=\begin{cases}1 & \text{if } i=j \text{ and } k=0,\\ 0 & \text{elsewhere.}\end{cases}$$

Then, δI satisfies

$$\delta I*A=A*\delta I=A,A\in\mathcal{M}_E(\mathbb{N}),$$

i.e., δI is *the identity element* for the discrete-time matrix convolution product.

The power in the sense of convolution is defined straightforwardly, using Definition 5.

Definition 6: Let $A\in\mathcal{M}_E(\mathbb{N})$ be a matrix-valued function and $n\in\mathbb{N}$. *The n-fold convolution* $A^{(n)}$ is a matrix-valued function in $\mathcal{M}_E(\mathbb{N})$ defined recursively by:

$$A_{ij}^{(0)}(k):=d_{ij}(k),$$

$$A_{ij}^{(1)}(k):=A_{ij}(k),$$

$$A_{ij}^{(n)}(k):=\sum_{r\in E}\sum_{l=0}^{k}A_{ir}(k-l)A_{rj}^{(n-1)}(l),n\geq 2,k\in\mathbb{N}.$$

For a MRC (J,S) the n-fold convolution of the semi-Markov kernel has the property expressed in the following result.

Lemma 2: Let $(J,S)=(J_n,S_n)_{n\in\mathbb{N}}$ be a Markov renewal chain and $\mathbf{q}=\left(q_{ij}(k);i,j\in E,k\in\mathbb{N}\right)$ be its associated semi-Markov kernel. Then, for all $n,k\in\mathbb{N}$ such that $n\geq k+1$, we have $\mathbf{q}^{(n)}(k)=0$.

This property of the discrete-time semi-Markov kernel convolution is essential for the simplicity and the numerical exactitude of the results obtained in discrete time. We need to stress the fact that this property is intrinsic to the work in discrete time and it is no longer valid for a continuous-time Markov renewal process.

Definition 7: Let $\mathrm{A}\in\mathcal{M}_E(\mathbb{N})$ be a matrix-valued function. If there exists a $B\in\mathcal{M}_E(\mathbb{N})$ such that $B*A=\delta I$, then B is called *the left inverse of* A *in the convolution sense* and it is denoted by $A^{(-1)}$.

It can be shown that given a matrix-valued function $\mathrm{A}\in\mathcal{M}_E(\mathbb{N})$ such that $\det A(0)\neq 0$, then the left inverse B of A exists and is unique (see [14] for the proof).

Let us now introduce the notion of the semi-Markov chain, strictly related to that of the Markov renewal chain.

Definition 8: Let (J,S) be a Markov renewal chain. The chain $Z=(Z_k)_{k\in\mathbb{N}}$ is said to be *a semi-Markov chain* associated to the MRC (J,S), if

$$Z_k:=J_{N(k)},k\in\mathbb{N},$$

where

$$N(k):=\left\{n\in\mathbb{N}\middle|S_n\leq k\right\}\qquad(24.2)$$

is the discrete-time counting process of the number of jumps in $[1,\mathrm{k}]\subset\mathbb{N}$. Thus, Z_k gives the system state at time k. We also have $J_n=Z_{S_n},n\in\mathbb{N}$. Let the row vector $\boldsymbol{\alpha}=\left(\alpha(1),\ldots,\alpha(s)\right)$ denote *the initial distribution* of the semi-Markov chain $Z=(Z_k)_{k\in\mathbb{N}}$, where $\alpha(i):=\mathbf{P}(Z_0=i)=\mathbf{P}(J_0=i)$, $i\in E$.

Definition 9: The transition function of the semi-Markov chain Z is the matrix-valued function $\mathbf{P}\in\mathcal{M}_E(\mathbb{N})$ defined by

$$P_{ij}(k):=\mathbb{P}(Z_k=j\middle|Z_0=i),i,j\in E,k\in\mathbb{N}.$$

The following result consists in a recursive formula for computing the transition function $\mathbf{P}$ of the semi-Markov chain Z.

Proposition 1: For all $i,j\in E$ and for all $k\in\mathbb{N}$, we have

$$P_{ij}(k)=\mathbf{1}_{\{i=j\}}\left(1-H_i(k)\right)+\sum_{r\in E}\sum_{l=0}^{k}q_{ir}(l)P_{rj}(k-l),$$

where

$$\mathbf{1}_{\{i=j\}} := \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{elsewhere.} \end{cases}$$

Let us define for all $k \in \mathbb{N}$:

- $I(k) := \mathbf{I}_E$ for $k \in \mathbb{N}$, $\mathbf{I} := (I(k); k \in \mathbb{N})$;
- $\mathbf{H}(k) := \mathrm{diag}(H_i(k); i \in E)$, $\mathbf{H} := (H(k); k \in \mathbf{N})$.

In matrix-valued function notation, the transition function $\mathbf{P}$ of the semi-Markov chain verifies the equation

$$\mathbf{P} = \mathbf{I} - \mathbf{H} + \mathbf{q} * \mathbf{P}.$$

This is an example of what is called the discrete-time Markov renewal equation. We know that the solution of this equation exists, is unique (see [14]) and, for all $k \in \mathbb{N}$, has the following form:

$$\begin{aligned} \mathbf{P}(k) &= (\delta I - \mathbf{q})^{(-1)} * (\mathbf{I} - \mathbf{H})(k) \\ &= (\delta I - \mathbf{q})^{(-1)} * (\mathbf{I} - \mathrm{diag}(\mathbf{Q} \cdot \mathbf{1}))(k). \end{aligned} \tag{24.3}$$

24.3 Reliability Modeling

In this section we consider a reparable discrete-time semi-Markov system and we obtain closed form solutions for reliability measures: reliability, availability, failure rate, mean time to failure, mean time to repair.

24.3.1 State Space Split

Consider a system (or a component) $\mathcal{S}$ whose possible states during its evolution in time are $E = \{1, \ldots, s\}$. Denote by $U = \{1, \ldots, s_1\}$ the subset of working states of the system (the up-states) and by $D = \{s_1 + 1, \ldots, s\}$ the subset of failure states (the down-states), with $0 < s_1 < s$ (obviously, $E = U \bigcup D$ and $U \bigcap D = \emptyset$, $U \neq \emptyset$, $D \neq \emptyset$). One can think of the states of U as different operating modes or performance levels of the system, whereas the states of D can be seen as failures of the system with different modes. According to the partition of the state space in up-states and down-states, we will partition the vectors, matrices or matrix functions we are working with.

Firstly, for $\boldsymbol{\alpha}, \mathbf{p}, \mathbf{q}(k), \mathbf{f}(k), \mathbf{F}(k), \mathbf{H}(k), \mathbf{Q}(k)$, we consider the natural matrix partition corresponding to the state space partition U and D. For example, we have

$$\mathbf{p} = \begin{pmatrix} \mathbf{p}_{11} & \mathbf{p}_{12} \\ \mathbf{p}_{21} & \mathbf{p}_{22} \end{pmatrix} \text{ and } \mathbf{q}(k) = \begin{pmatrix} \mathbf{q}_{11}(k) & \mathbf{q}_{12}(k) \\ \mathbf{q}_{21}(k) & \mathbf{q}_{22}(k) \end{pmatrix}.$$

Secondly, for $\mathbf{P}(k)$ we consider the restrictions to $U \times U$ and $D \times D$ induced by the corresponding restrictions of the semi-Markov kernel $\mathbf{q}(k)$. To be more specific, using the partition given above for the kernel $\mathbf{q}(k)$, we note that:

$$\mathbf{P}_{11}(k) := (\delta I - \mathbf{q}_{11})^{(-1)} * (\mathbf{I} - \mathrm{diag}(\mathbf{Q} \cdot \mathbf{1})_{11})(k),$$

$$\mathbf{P}_{22}(k) := (\delta I - \mathbf{q}_{22})^{(-1)} * (\mathbf{I} - \mathrm{diag}(\mathbf{Q} \cdot \mathbf{1})_{22})(k).$$

The reasons fort taking this partition for $\mathbf{P}(k)$ can be found in [19].

For $m, n \in \mathbb{N}^*$ such that $m > n$, let $\mathbf{1}_{m,n}$ denote the m-dimensional column vector whose n first elements are 1 and last $m - n$ elements are 0; for $m \in \mathbb{N}^*$ let $\mathbf{1}_m$ denote the m-column vector whose elements are all 1, that is, $\mathbf{1}_m = \mathbf{1}_{m,m}$.

24.3.2 Reliability

Consider a system $\mathcal{S}$ starting to function at time $k = 0$ and let T_D denote the first passage time in subset D, called *the lifetime of the system*, *i.e.*,

$$T_D := \inf\{k \in \mathbb{N} \,|\, Z_k \in D\} \text{ and } \inf \emptyset := \infty.$$

The reliability of a discrete-time semi-Markov system $\mathcal{S}$ at time $k \in \mathbb{N}$, that is the probability that the system has functioned without failure in the period $[0, k]$, is

$$R(k) := \mathbb{P}(T_D > k) = \mathbb{P}(Z_n \in U, n = 0, \ldots, k).$$

The following result gives the reliability of the system in terms of the basic quantities of the semi-Markov chain.

Proposition 2: The reliability of a discrete-time semi-Markov system at time $k \in \mathbb{N}$ is given by

$$\begin{aligned} R(k) &= \boldsymbol{\alpha}_1 \mathbf{P}_{11}(k) \mathbf{1}_{s_1} \\ &= \boldsymbol{\alpha}_1 (\delta I - \mathbf{q}_{11})^{(-1)} * (\mathbf{I} - \mathrm{diag}(\mathbf{Q} \cdot \mathbf{1})_{11})(k) \mathbf{1}_{s_1}. \end{aligned}$$

24.3.3 Availability

The point-wise (or instantaneous) availability of a system $\mathcal{S}$ at time $k \in \mathbb{N}$ is the probability that the system is operational at time k (independently of the fact that the system has failed or not in $[0,k)$). So, the point-wise availability of a semi-Markov system at time $k \in \mathbb{N}$ is

$$A(k) := \mathbb{P}(Z_k \in U) = \sum_{i \in E} \alpha(i) A_i(k),$$

where we have denoted by $A_i(k)$ the system's availability at time $k \in \mathbb{N}$, given that it starts in state $i \in E$,

$$A_i(k) = \mathbb{P}(Z_k \in U \big| Z_0 = i).$$

The following result gives an explicit form of the availability of a discrete-time semi-Markov system.

Proposition 3: The point-wise availability of a discrete-time semi-Markov system at time $k \in \mathbb{N}$ is given by

$$\begin{aligned} A(k) &= \boldsymbol{\alpha} \mathbf{P}(k) \mathbf{1}_{s,s_1} \\ &= \boldsymbol{\alpha} (\delta I - \mathbf{q})^{(-1)} * (\mathbf{I} - \mathrm{diag}(\mathbf{Q} \cdot \mathbf{1}))(k) \mathbf{1}_{s,s_1}. \end{aligned}$$

24.3.4 The Failure Rate

We consider here the classical failure rate, introduced by Barlow, Marshall and Proschan in 1963 (see [20]). We call it *the BMP-failure rate* and denote it by $\lambda(k), k \in \mathbb{N}$.

Let $\mathcal{S}$ be a system starting to function at time $k = 0$. The BMP-failure rate at time $k \in \mathbb{N}$ is the conditional probability that the failure of the system occurs at time k, given that the system has worked until time $k-1$.

For a discrete-time semi-Markov system, the failure rate at time $k \geq 1$ has the expression

$$\begin{aligned} \lambda(k) &:= \mathbb{P}(T_D = k \big| T_D \geq k), \\ &= \begin{cases} 1 - \dfrac{R(k)}{R(k-1)}, & R(k-1) \neq 0, \\ 0, & \text{otherwise}, \end{cases} \\ &= \begin{cases} 1 - \dfrac{\boldsymbol{\alpha}_1 \mathbf{P}_{11}(k) \mathbf{1}_{s_1}}{\boldsymbol{\alpha}_1 \mathbf{P}_{11}(k-1) \mathbf{1}_{s_1}}, & R(k-1) \neq 0, \\ 0, & \text{otherwise}. \end{cases} \end{aligned} \tag{24.4}$$

The failure rate at time $k = 0$ is defined by $\lambda(0) := 1 - R(0)$.

It is worth noticing that the failure rate $\lambda(k)$ in discrete-time case is a probability function and not a general positive function as in the continuous-time case. There exists a more recent failure rate, proposed in [2] as being adapted to reliability studies carried out in discrete time. Discussions justifying the use of this discrete-time adapted failure rate can also be found in [3, 4]. In this chapter we do not present this alternative failure rate. Its use for discrete-time semi-Markov systems can be found in [18, 19].

24.3.5 Mean Hitting Times

There are various mean times which are interesting for the reliability analysis of a system. We will be concerned here only with the mean time to failure and the mean time to repair.

We suppose that $\boldsymbol{\alpha}_2 = 0$, *i.e.,* the system starts in a working state. The *mean time to failure* (MTTF) is defined as the mean lifetime, *i.e.*, the expectation of the hitting time to down-set D, $MTTF := \mathbb{E}(T_D)$.

Symmetrically, consider now that $\boldsymbol{\alpha}_1 = 0$, *i.e.* the system fails at the time $t = 0$. Denote by T_U the first hitting time of the up-set U, called *the repair duration*, *i.e.*,

$$T_U := \inf\{k \in \mathbb{N} \big| Z_k \in U\}.$$

The *mean time to repair* (MTTR) is defined as the mean of the repair duration, *i.e.*, $MTTR := \mathbb{E}(T_U)$.

The following result gives expressions for the MTTF and the MTTR of a discrete-time semi-Markov system.

Proposition 4: If the matrices $I-\mathbf{p}_{11}$ and $I-\mathbf{p}_{22}$ are non-singular, then

$$MTTF=\boldsymbol{\alpha}_1(I-\mathbf{p}_{11})^{-1}\mathbf{m}_1,$$
$$MTTR=\boldsymbol{\alpha}_2(I-\mathbf{p}_{22})^{-1}\mathbf{m}_2,$$

where $\mathbf{m}=(\mathbf{m}_1\ \mathbf{m}_2)^{\mathrm{T}}$ is the partition of the mean sojourn times vector corresponding to the partition of the state space E in up-states U and down-states D. If the matrices are singular, we put $MTTF=\infty$ or $MTTF=\infty$.

24.4 Reliability Estimation

The objective of this section is to provide estimators for reliability indicators of a system and to present their asymptotic properties. In order to achieve this purpose, we firstly show how estimators of the basic quantities of a discrete-time semi-Markov system are obtained.

24.4.1 Semi-Markov Estimation

Let us consider a sample path of a Markov renewal chain $(J_n,S_n)_{n\in\mathbb{N}}$, censored at fixed arbitrary time $M\in\mathbb{N}^*$,

$$\mathcal{H}(M)=(J_0,X_1\ldots,J_{N(M)-1},X_{N(M)},J_{N(M)},u_M),$$

where $N(M)$ is the discrete-time counting process of the number of jumps in (see (24.2)) and $u_M:=M-S_{N(M)}$ is the censored sojourn time in the last visited state $J_{N(M)}$.

Starting from the sample path $\mathcal{H}(M)$, we will propose empirical estimators for the quantities of interest. Let us firstly define the number of visits to a certain state, the number of transitions between two states and so on.

Definition 10: For all states $i,j\in E$ and positive integer $k\le M$, define:

1. $N_i(M):=\sum_{n=0}^{N(M)-1}\mathbf{1}_{\{J_n=i\}}$ - the number of visits to state i, up to time M;
2. $N_{ij}(M):=\sum_{n=1}^{N(M)}\mathbf{1}_{\{J_{n-1}=i,J_n=j\}}$ - the number of transitions from i to j, up to time M;
3. $N_{ij}(k,M):=\sum_{n=1}^{N(M)}\mathbf{1}_{\{J_{n-1}=i,J_n=j,X_n=k\}}$ - the number of transitions from i to j, up to time M, with sojourn time in state i equal to $k,1\le k\le M$.

For a sample path of length M of a semi-Markov chain, for any states $i,j\in E$ and positive integer $k\in\mathbb{N},k\le M$, we define the empirical estimators of the transition matrix of the embedded Markov chain p_{ij}, of the conditional distributions of the sojourn times $f_{ij}(k)$ and of the discrete-time semi-Markov kernel $q_{ij}(k)$ by:

$$\begin{aligned}\widehat{p}_{ij}(M)&:=N_{ij}(M)/N_i(M),\\ \widehat{f}_{ij}(k,M)&:=N_{ij}(k,M)/N_{ij}(M),\\ \widehat{q}_{ij}(k,M)&:=N_{ij}(k,M)/N_i(M).\end{aligned}\qquad(24.5)$$

Note that the proposed estimators are natural estimators. For instance, the probability p_{ij} that the system goes from state i to state j is estimated by the number of transitions from i to j, devised by the number of visits to state i. As can be seen in [17] or [19], the empirical estimators proposed in (24.5) have good asymptotic properties. Moreover, they are in fact approached maximum likelihood estimators (Theorem 1). In order to see this, consider the likelihood function corresponding to the history $\mathcal{H}(M)$

$$L(M)=\prod_{k=1}^{N(M)}p_{J_{k-1}J_k}f_{J_{k-1}J_k}(X_k)\overline{H}_{J_{N(M)}}(u_M),$$

where $\overline{H}_i(\cdot)$ is the survival function in state i. We have the following result concerning the asymptotic behavior of u_M (see [19] for a proof).

Lemma 3: For a semi-Markov chain $(Z_n)_{n\in\mathbb{N}}$ we have $u_M/M\xrightarrow{a.s.}0$, as $M\to\infty$.

Let us consider the approached likelihood function

$$L_1(M) = \prod_{k=1}^{N(M)} p_{J_{k-1}J_k} f_{J_{k-1}J_k}(X_k), \qquad (24.6)$$

obtained by neglecting the last term in the expression of $L(M)$. Using Lemma 3, we see that the maximum likelihood function $L(M)$ and the approached maximum likelihood function $L_1(M)$ are asymptotically equivalent, as M tends to infinity. Consequently, the estimators obtained by estimating $L(M)$ or $L_1(M)$ are asymptotically equivalent, as M tends to infinity.

The following result shows that $\widehat{p}_{ij}(M)$, $\widehat{f}_{ij}(k,M)$ and $\widehat{q}_{ij}(k,M)$ defined in (24.5) are obtained in fact by maximizing $L_1(M)$ (a proof can be found in [17]).

Theorem 1: For a sample path of a semi-Markov chain $(Z_n)_{n\in\mathbb{N}}$, of arbitrary fixed length $M \in \mathbb{N}$, the empirical estimators of the transition matrix of the embedded Markov chain $(J_n)_{n\in\mathbb{N}}$, of the conditional distributions of the sojourn times and of the discrete-time semi-Markov kernel, proposed in (24.5), are approached nonparametric maximum likelihood estimators, *i.e.*, they maximize the approached likelihood function $L_1(M)$ given in (24.6).

As any quantity of interest of a semi-Markov system can be written in terms of the semi-Markov kernel, we can now use the kernel estimator $\widehat{q}_{ij}(k,M)$ in order to obtain plug-in estimators for any functional of the kernel. For instance, the cumulative semi-Markov kernel $\mathbf{Q} = (\mathbf{Q}(k); k \in \mathbb{N})$ defined in (24.1) has the estimator

$$\widehat{\mathbf{Q}}(k,M) := \sum_{l=1}^{k} \widehat{\mathbf{q}}(l,M).$$

Similarly, using the expression of the transition function of the semi-Markov chain Z given in (24.3), we get its estimator

$$\widehat{\mathbf{P}}(k,M) = (\delta I - \widehat{\mathbf{q}})^{(-1)}(\cdot,M) * (\mathbf{I} - \mathrm{diag}(\widehat{\mathbf{Q}}(\cdot,M)\cdot\mathbf{1}))(k).$$

Proofs of the consistency and of the asymptotic normality of the estimators defined up to now can be found in [16, 17, 19].

We are able now to construct estimators of the reliability indicators of a semi-Markov system and to present their asymptotic properties.

24.4.2 Reliability Estimation

The expression of the reliability given in Proposition 2, together with the estimators of the semi-Markov transition function and of the cumulative semi-Markov kernel given above, allow us to obtain the estimator of the system's reliability at time k given by

$$\widehat{R}(k,M) = \boldsymbol{\alpha}_1 \widehat{\mathbf{P}}_{11}(k,M)\mathbf{1}_{s_1}. \qquad (24.7)$$

Let us give now the result concerning the consistency and the asymptotic normality of the reliability estimator. A proof of the asymptotic normality of reliability estimator, based on CLT for Markov renewal processes (see [21]) can be found in [17]. An alternative proof based on CLT for martingales, can be found in [19].

Theorem 2: For any fixed arbitrary positive integer $k \in \mathbb{N}$, the estimator of the reliability of a discrete-time semi-Markov system at instant k is strongly consistent, *i.e.,*

$$\left|\widehat{R}(k,M) - R(k)\right| \xrightarrow{a.s.} 0, \text{ as } M \to \infty,$$

and asymptotically normal, *i.e.*, we have

$$\sqrt{M}\left[\widehat{R}(k,M) - R(k)\right] \xrightarrow{\mathcal{D}} \mathcal{N}\left(0, \sigma_R^2(k)\right), \text{ as } M \to \infty,$$

with the asymptotic variance

$$\sigma_R^2(k) = \sum_{i=1}^{s} \mu_{ii} \left\{ \sum_{j=1}^{s} \left[D_{ij}^U - \mathbf{1}_{\{i\in U\}} \sum_{t\in U} \alpha(t)\Psi_{ti} \right]^2 * q_{ij}(k) \right.$$

$$\left. - \left[\sum_{j=1}^{s} \left(D_{ij}^U * q_{ij} - \mathbf{1}_{\{i\in U\}} \sum_{t\in U} \alpha(t)\psi_{ti} * Q_{ij} \right) \right]^2 (k) \right\},$$

where

$$D_{ij}^U := \sum_{n\in U} \sum_{r\in U} \alpha(n)\psi_{ni} * \psi_{jr} * \left(\mathbf{I} - \mathrm{diag}(\mathbf{Q}\cdot\mathbf{1})\right)_{rr},$$

$$\boldsymbol{\psi}(k) := \sum_{n=0}^{k} \mathbf{q}^{(n)}(k), \quad \boldsymbol{\Psi}(k) := \sum_{n=0}^{k} \mathbf{Q}^{(n)}(k),$$

and μ_{ii} is the mean recurrence time of the state i for the chain Z.

24.4.3 Availability Estimation

Taking into account the expression of the availability given in Proposition 3, we propose the following estimator for the availability of a discrete-time semi-Markov system:

$$\widehat{A}(k,M) = \boldsymbol{\alpha}\widehat{\mathbf{P}}(k,M)\mathbf{1}_{s,s_1}.$$

The following result concerns the consistency and the asymptotic normality of the reliability estimator. A proof can be found in [19].

Theorem 3: For any fixed arbitrary positive integer $k \in \mathbb{N}$, the estimator of the availability of a discrete-time semi-Markov system at instant k is strongly consistent and asymptotically normal, in the sense that

$$\left|\widehat{A}(k,M) - A(k)\right| \xrightarrow{a.s.} 0, \text{ as } M \to \infty,$$

and

$$\sqrt{M}\left[\widehat{A}(k,M) - A(k)\right] \xrightarrow{\mathcal{D}} \mathcal{N}\left(0, \sigma_A^2(k)\right), \text{ as } M \to \infty,$$

with the asymptotic variance

$$\sigma_A^2(k) = \sum_{i=1}^{s} \mu_{ii} \left\{ \sum_{j=1}^{s} \left[D_{ij} - \mathbf{1}_{\{i\in U\}} \sum_{t=1}^{s} \alpha(t)\Psi_{ti} \right]^2 * q_{ij}(k) \right.$$

$$\left. - \left[\sum_{j=1}^{s} \left(D_{ij} * q_{ij} - \mathbf{1}_{\{i\in U\}} \sum_{t=1}^{s} \alpha(t)\psi_{ti} * Q_{ij} \right) \right]^2 (k) \right\},$$

where $D_{ij} := \sum_{n=1}^{s} \sum_{r\in U} \alpha(n)\psi_{ni} * \psi_{jr} * \left(\mathbf{I} - \text{diag}(\mathbf{Q}\cdot\mathbf{1})\right)_{rr}$.

24.4.4 Failure Rate Estimation

For a matrix function $A \in \mathcal{M}_E(\mathbb{N})$, we denote by $A^+ \in \mathcal{M}_E(\mathbb{N})$ the matrix function defined by $A^+(k) := A(k+1), k \in \mathbb{N}$. Using the expression of the failure rate obtained in (24.4), we obtain the following estimator:

$$\widehat{\lambda}(k,M) := \begin{cases} 1 - \dfrac{\widehat{R}(k,M)}{\widehat{R}(k-1,M)}, & \widehat{R}(k-1,M) \neq 0, \mathrm{k} \geq 1, \\ 0, & \widehat{R}(k-1,M) = 0, \mathrm{k} \geq 1, \end{cases}$$

$$\widehat{\lambda}(0,M) := 1 - \widehat{R}(0,M).$$

For the failure rate estimator we have a similar result as for reliability and availability estimators. A proof can be found in [18, 19].

Theorem 4: For any fixed arbitrary positive integer $k \in \mathbb{N}$, the estimator of the failure rate of a discrete-time semi-Markov system at instant k is strongly consistent and asymptotically normal, *i.e.*,

$$\left|\widehat{\lambda}(k,M) - \lambda(k)\right| \xrightarrow{a.s.} 0, \text{ as } M \to \infty,$$

and

$$\sqrt{M}\left[\widehat{\lambda}(k,M) - \lambda(k)\right] \xrightarrow{\mathcal{D}} \mathcal{N}\left(0, \sigma_\lambda^2(k)\right), \text{ as } M \to \infty,$$

swith the asymptotic variance

$$\sigma_\lambda^2(k) = \sigma_1^2(k) / R^4(k-1),$$

where $\sigma_1^2(k)$ is given by

$$\sigma_1^2(k) =$$

$$\sum_{i=1}^{s} \mu_{ii} \left\{ R^2(k) \sum_{j=1}^{s} \left[D_{ij}^U - \mathbf{1}_{\{i\in U\}} \sum_{t\in U} \alpha(t)\Psi_{ti} \right]^2 * q_{ij}(k-1) \right.$$

$$+ R^2(k-1) \sum_{j=1}^{s} \left[D_{ij}^U - \mathbf{1}_{\{i\in U\}} \sum_{t\in U} \alpha(t)\Psi_{ti} \right]^2 * q_{ij}(k) - T_i^2(k)$$

$$+ 2R(k-1)R(k) \sum_{j=1}^{s} \left[\mathbf{1}_{\{i\in U\}} D_{ij}^U \sum_{t\in U} \alpha(t)\Psi_{ti}^+ \right.$$

$$+ \mathbf{1}_{\{i\in U\}} \left(D_{ij}^U\right)^+ \sum_{t\in U} \alpha(t)\Psi_{ti} - \left(D_{ij}^U\right)^+ D_{ij}^U$$

$$\left. \left. - \mathbf{1}_{\{i\in U\}} \left(\sum_{t\in U} \alpha(t)\Psi_{ti} \right) \left(\sum_{t\in U} \alpha(t)\Psi_{ti}^+ \right) \right] * q_{ij}(k-1) \right\},$$

where

$$T_i(k) := \sum_{j=1}^{s} \left[R(k) D_{ij}^U * q_{ij}(k-1) - R(k-1) D_{ij}^U * q_{ij}(k) \right.$$

$$- R(k) \mathbf{1}_{\{i\in U\}} \sum_{t\in U} \alpha(t)\psi_{ti} * Q_{ij}(k-1)$$

$$\left. + R(k-1) \mathbf{1}_{\{i\in U\}} \sum_{t\in U} \alpha(t)\psi_{ti} * Q_{ij}(k) \right]$$

and D_{ij}^U is given in Theorem 2.

24.4.5 Asymptotic Confidence Intervals

The previously obtained asymptotic results allow one to construct asymptotic confidence intervals for reliability, availability and failure rate. For this purpose, we need to construct a consistent estimator of the asymptotic variances.

Firstly, using the definitions of $\boldsymbol{\psi}(k)$ and of $\boldsymbol{\Psi}(k)$ given in Theorem 2, we can construct the corresponding estimators $\widehat{\boldsymbol{\psi}}(k,M)$ and $\widehat{\boldsymbol{\Psi}}(k,M)$. One can check that these estimators are strongly consistent. Secondly, for $k \le M$, replacing $\mathbf{q}(k)$, $\mathbf{Q}(k)$, $\boldsymbol{\psi}(k)$ and $\boldsymbol{\Psi}(k)$ by the corresponding estimators in the asymptotic variance of the reliability given in Theorem 2, we obtain an estimator $\widehat{\sigma}_R^2(k,M)$ of the asymptotic variance $\sigma_R^2(k)$. From the strong consistency of the estimators $\widehat{\mathbf{q}}(k,M)$, $\widehat{\mathbf{Q}}(k,M)$, $\widehat{\boldsymbol{\psi}}(k,M)$ and $\widehat{\boldsymbol{\Psi}}(k,M)$ (see [17, 19]), we obtain that $\widehat{\sigma}_R^2(k,M)$ converges almost surely to $\sigma_R^2(k)$, as M tends to infinity. Finally, the asymptotic confidence interval of $R(k)$ at level $100(1-\gamma)\%$, $\gamma \in (0,1)$, is:

$$\left[\widehat{R}(k,M) - u_{1-\gamma/2}\frac{\widehat{\sigma}_R(k,M)}{\sqrt{M}}, \widehat{R}(k,M) + u_{1-\gamma/2}\frac{\widehat{\sigma}_R(k,M)}{\sqrt{M}}\right],$$

where $u_{1-\gamma/2}$ is the $(1-\gamma/2)$ fractile of $\mathcal{N}(0,1)$. In the same way, we can obtain the other confidence intervals.

24.5 A Numerical Example

Let us consider the three-state discrete-time semi-Markov system described in Figure 24.2.

The state space $E = \{1,2,3\}$ is partitioned into the up-state set $U = \{1,2\}$ and the down-state set $D = \{3\}$.

The system is defined by the initial distribution $\boldsymbol{\alpha} = (1\ 0\ 0)$, by the transition probability matrix $\mathbf{p}$ of the embedded Markov chain $(J_n)_{n\in\mathbb{N}}$ and by the conditional distributions of the sojourn times:

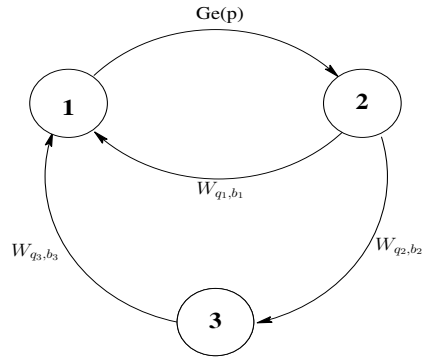


Figure 24.2. A three-state semi-Markov system

$$\mathbf{p} = \begin{pmatrix} 0 & 1 & 0 \\ 0.95 & 0 & 0.05 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\mathbf{f}(k) = \begin{pmatrix} 0 & f_{12}(k) & 0 \\ f_{21}(k) & 0 & f_{23}(k) \\ f_{31}(k) & 0 & 0 \end{pmatrix}, k \in \mathbb{N}.$$

We consider the following distributions for the conditional sojourn time:

$-\ f_{12}$ is a geometric distribution on $\mathbb{N}^*$, of parameter $p = 0.8$.

$-\ f_{21} := W_{q_1,b_1}$, $f_{23} := W_{q_2,b_2}$, $f_{31} := W_{q_3,b_3}$ are discrete-time, first type Weibull distributions (see [1]), defined by $W_{q,b}(0) := 0$, $W_{q,b}(k) := q^{(k-1)^b} - q^{k^b}$, $k \ge 1$, where we take $q_1 = 0.3$, $b_1 = 0.5$, $q_2 = 0.5$, $b_2 = 0.7$, $q_3 = 0.6$, $b_3 = 0.9$. Note that we study here a strictly semi-Markov system, which cannot be reduced to a Markov one.

Using the transition probability matrix and the sojourn time distributions given above, we have simulated a sample path of the three state semi-Markov chain, of length M. This sample path allows us to compute $N_i(M)$, $N_{ij}(M)$ and $N_{ij}(k,M)$, using Definition 10, and to obtain the empirical estimators $\widehat{p}_{ij}(M)$, $\widehat{f}_{ij}(k,M)$ and $\widehat{q}_{ij}(k,M)$ from (24.5). Consequently, we can

obtain the estimators $\widehat{\mathbf{Q}}(k,M)$, $\widehat{\boldsymbol{\psi}}(k,M)$ and $\widehat{\boldsymbol{\Psi}}(k,M)$. Thus, from (24.7), we obtain the estimator of the reliability. In Theorem 2, we have obtained the expression of the asymptotic variance of reliability. Replacing $\mathbf{q}(k)$, $\mathbf{Q}(k)$, $\boldsymbol{\psi}(k)$ and $\boldsymbol{\Psi}(k)$ by the corresponding estimators, we get the estimator $\widehat{\sigma}_R^2(k,M)$ of the asymptotic variance $\sigma_R^2(k)$. This estimator will allow us to have the asymptotic confidence interval for reliability, as shown in Section 24.4.5.

The consistency of the reliability estimator is illustrated in Figure 24.3, where reliability estimators obtained for several values of the sample size M are drawn. We can note that the estimator approaches the true value, as the sample size M increases. Figure 24.4 presents the estimators of the asymptotic variance of the reliability $\sigma_R^2(k)$, obtained for different sample sizes. Note also that the estimator approaches the true value, as M increases. In Figure 24.5, we present the confidence interval of the reliability. Note that the confidence interval covers the true value of the reliability.

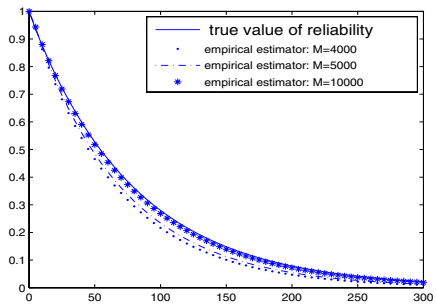


Figure 24.3. Consistency of reliability estimator

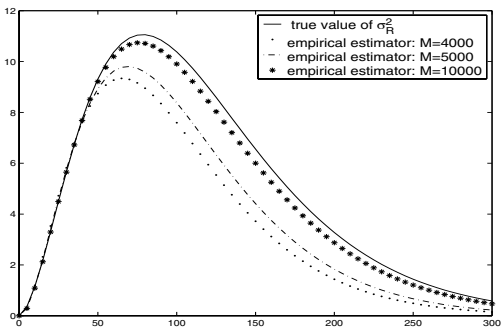


Figure 24.4. Consistency of $\widehat{\sigma}_R^2(k,M)$

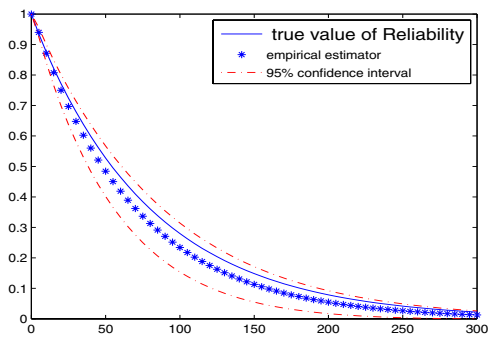


Figure 24.5. Confidence interval of reliability

References

[1] Bracquemond C, Gaudoin O. A survey on discrete lifetime distributions. International Journal on Reliability, Quality, and Safety Engineering 2003; 10 (1): 69–98.

[2] Roy D, Gupta R. Classification of discrete lives. Microelectronics Reliability. 1992; 32 (10): 1459–1473.

[3] Xie M, Gaudoin O, Bracquemond C. Redefining failure rate function for discrete distributions. International Journal on Reliability, Quality, and Safety Engineering 2002; 9 (3): 275–285.

[4] Lai C-D, Xie M. Stochastic ageing and dependence for reliability. Springer, New York, 2006.

[5] Balakrishnan N, Limnios N, Papadopoulos C. Basic probabilistic models in reliability. In: Balakrishnan N, Rao CR, editors. Handbook of statistics 20-advances in reliability. Elsevier, Amsterdam, 2001; 1–42.

[6] Platis A, Limnios N, Le Du M. Hitting times in a finite non-homogeneous Markov chain with applications. Applied Stochastic Models and Data Analysis1998; 14: 241–253.

[7] Sadek A, Limnios N. Asymptotic properties for maximum likelihood estimators for reliability and failure rates of Markov chains. Communications in Statistics – Theory and Methods 2002; 31(10): 1837–1861.

[8] Limnios N, Oprişan G. Semi-Markov processes and reliability. Birkhäuser, Boston, 2001.
[9] Ouhbi B, Limnios N. Nonparametric reliability estimation for semi-Markov processes. J. Statistical Planning and Inference 2003; 109: 155–165.
[10] Limnios N, Ouhbi B. Empirical estimators of reliability and related functions for semi-Markov systems. In: Lindqvist B, Doksum KA, editors. Mathematical and statistical methods in reliability. World Scientific, Singapore, 2003; 7: 469–484.
[11] Port SC. Theoretical probability for applications. Wiley, New York, 1994.
[12] Howard R. Dynamic Probabilistic systems, vol. II, Wiley, New York, 1971.
[13] Mode CJ, Sleeman CK. Stochastic processes in epidemiology. World Scientific, Singapore, 2000.
[14] Barbu V, Boussemart M, Limnios N. Discrete time semi-Markov model for reliability and survival analysis. Communications Statistics – Theory and Methods 2004; 33 (11): 2833–2868.
[15] Csenki A. Transition analysis of semi-Markov reliability models - a tutorial review with emphasis on discrete-parameter approaches. In: Osaki S, editor. Stochastic Models in reliability and maintenance. Springer, Berlin, 2002; 219–251.
[16] Barbu V, Limnios N. Discrete time semi-Markov processes for reliability and survival analysis - a nonparametric estimation approach. In: Nikulin M, Balakrishnan N, Meshbah M, Limnios N, editors. Parametric and semiparametric models with applications to reliability, survival analysis and quality of life, statistics for industry and technology. Birkhäuser, Boston, 2004; 487–502.
[17] Barbu V, Limnios N. Empirical estimation for discrete time semi-Markov processes with applications in reliability. Journal of Non-parametric Statistics; 2006; 18(7-8):483–493.
[18] Barbu V, Limnios N. Nonparametric estimation for failure rate functions of discrete time semi-Markov processes. In: Nikulin M, Commenges D, Hubert C. editors. Probability, statistics and modelling in public health. Springer, Berlin, 2006; 53–72.
[19] Barbu V, Limnios N. Semi-Markov chains and hidden semi-Markov models towards applications in reliability and DNA analysis. Lecture Notes in Statistics, Springer, New York; Vol. 191, 2008.
[20] Barlow RE, Marshall AW, Prochan F. Properties of probability distributions with monotone hazard rate. The Annals of Mathematical Statistics 1963; 34 (2): 375–389.
[21] Pyke R, Schaufele S. Limit theorems for Markov renewal processes. The Annals of Mathematical Statistics 1964; 35: 1746–1764.
[22] Limnios N, Ouhbi B, Platis A, Sapountzoglou G. Nonparametric estimation of performance and performability for semi-Markov process. International Journal of Performability Engineering 2006; 2(1), 19–27.

25

Binary Decision Diagrams for Reliability Studies

Antoine Rauzy

IML CNRS, 169, Avenue de Luminy, 13288 Marseille cedex 9, France

Abstract: Bryant's binary ecision diagrams are state-of-the-art data structures used to encode and to manipulate Boolean functions. Risk and dependability studies are heavy consumers of Boolean functions, for the most widely used modeling methods, namely fault trees and event trees, rely on them. The introduction of BDD in that field renewed its algorithmic framework. Moreover, several central mathematical definitions, like the notions of minimal cutsets and importance factors, were questioned. This article attempts to summarize fifteen years of active research on those topics.

25.1 Introduction

Binary decision diagrams (BDD for short) are state-of-the-art data structures used to encode and to manipulate Boolean functions. They were introduced in 1986 by R. Bryant [1] to handle logical circuits and further improved by Bryant and others in the early 1990s [2, 3]. Since then, they have been used successfully in a wide variety of applications (see [4] for a glance). Reliability and dependability studies are heavy consumers of Boolean functions, for the most widely used modeling methods, namely fault trees and event trees, rely on them. The introduction of BDD in that field [5, 6] renewed completely its algorithmic framework. Moreover, several central mathematical definitions, like the notions of minimal cutsets and importance factors, were questioned. This article attempts to summarize fifteen years of active research on those topics.

Fault tree and event tree analyses are classically performed in two steps: first, the minimal cutsets (MCS for short) of the model are determined by some top-down or bottom-up algorithm; second, some probabilistic quantities of interest are assessed from MCS (see, *e.g.*, [7, 8, 9]). Usually, not all of the MCS are considered: cut-offs are applied to keep only the most relevant ones, *i.e.* those with the highest probabilities. With BDD, the methodology is different: first, the BDD of the model is constructed. Then, a second BDD, technically a ZBDD [10], is built from the first one to encode MCS. Probabilistic quantities are assessed either from the BDD or from the ZBDD. From an engineering viewpoint, this new approach changes significantly the process: first, MCS are now used mainly for verification purposes since they are not necessary to assess probabilistic quantities. Second, probabilistic assessments provide exact results, for no cut-off needs to be applied. Last, both coherent (monotone) and non-coherent models can be handled, which is not possible, at least accurately, with the classical approach. However, the new approach has a drawback: the construction of the BDD must be feasible and, as with many Boolean problems, it is

of exponential worst case complexity. The design of strategies and heuristics to construct BDD for large reliability models is still challenging.
In this article, we focus on three issues: the computation of minimal cutsets, the assessment of various probabilistic quantities, and finally the treatment of large models.

A minimal cutset of a fault tree is a minimal set of basic events that induces the top event. The notion minimal cutset is thus related to the logical notion of prime implicant. For a coherent model the two notions actually correspond. For non-coherent models however, they differ. Until recently, the reliability engineering literature stayed at a very intuitive level on this subject. With the introduction of BDD, not only new efficient algorithms to compute MCS have been designed, but the mathematical foundations of MCS have been more firmly established [11].

Beyond the top event probability, a fault tree study involves in general the computation of various quantities like importance factors or equivalent failure rates. The BDD approach makes it possible (and necessary) to revisit these notions and to improve the computations in terms of both efficiency and accuracy [12, 13, 14].

Event trees of the nuclear industry involve up to thousands of basic events. The calculation of BDD for these models is still challenging, while the classical approach (based on the extraction of MCS) is always able to give results, approximate results of course, but still results. Recent studies showed however that, conversely to what was commonly admitted, these results may be not very accurate [15]. The design of heuristics and strategies to assess huge reliability models is therefore of a great scientific and technological interest.

The remainder of this article is organized as follows. Section 25.2 recalls basics about fault trees, event trees, and BDD. Section 25.3 presents the notion of minimal cutsets. Section 25.4 shows the various probabilistic quantities of interest that can be computed by means of BDD. Section 25.5 discusses the assessment of large models. Section 25.6 concludes the article.

25.2 Fault Trees, Event Trees and Binary Decision Diagrams

This section recalls basics about fault trees, event trees and BDD.

25.2.1 Fault Trees and Event Trees

A fault tree is a Boolean formula built over variables, so called basic events that represent failures of basic components (the e_i of Figure 25.1 , and gates (AND, OR, *k*-out-of-*n*). Gates are usually given a name, like the G_i's of Figure 25.1 and called intermediate events. The formula is rooted by an event, called the top event (T in Figure 25.1). The top event encodes the various combinations of elementary failures, *i.e.,* of basic events, that induce a failure of the system under study.

Fault tree studies are twofold. Qualitative analyses consist of determining the minimal cutsets, *i.e.* the minimal combinations of basic events that induce the top event. Quantitative analyses consist of computing various probabilistic quantities of interest, given the probabilities of occurrence of the basic events. Both problems are hard–counting the number of minimal solution of a Boolean formula in assessing the probability of the formula–and fall into the P-hard complexity class [16]. It is worth noting that these complexity results stand even in the case where the underlying function is monotone (coherent), which is in general the case (usually, fault trees do not involve negations).

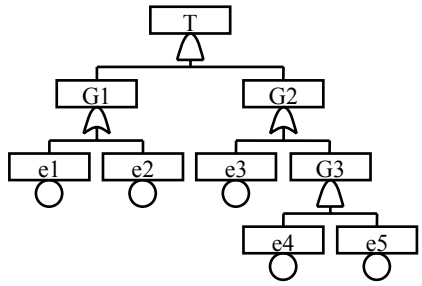


Figure 25.1. A fault tree

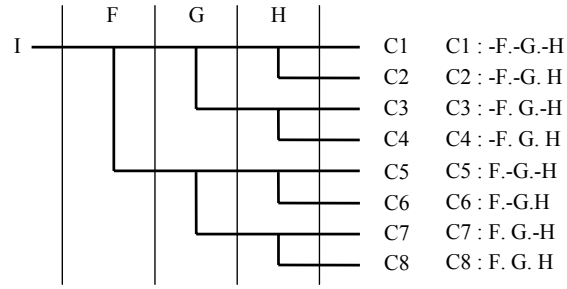


Figure 25.2. An event tree

Depending on the success or the failure of the system, the upper or the lower branch is taken. At the end, a consequence is reached (one of the C_i's on). Failures of safety systems are described by means of fault trees. Sequences are compiled into conjunctions of the initiating event and top events or negations of top events, as illustrated on the right hand side of Figure 25.2. The assessment of sequences, or groups of sequences, is similar to the assessment of fault trees. However, it is worth noting that, due to success branches, formulae may involve negations.

Fault trees are the most widely used method for risk analyses. Virtually all industries that present a risk for the environment use it. Event trees are used mainly in the nuclear industry. A good introduction to both techniques can be found in reference [9].

25.2.2 Binary Decision Diagrams

Binary Decision Diagrams are a compact encoding of the truth tables of Boolean formulae [1, 2]. The BDD representation is based on the Shannon decomposition: Let F be a Boolean function that depends on the variable v, then the following equality holds.

$$F = v.F[v \leftarrow 1] + \overline{v}.F[v \leftarrow 0]$$

By choosing a total order over the variables and applying recursively the Shannon decomposition, the truth table of any formula can be graphically represented as a binary tree. The nodes are labeled with variables and have two outedges (a *then*-outedge, pointing to the node that encodes F[v←1], and an *else*-outedge, pointing to the node that encodes F[v←0]). The leaves are labeled with either 0 or 1. The value of the formula for a given variable assignment is obtained by descending along the corresponding branch of the tree. The Shannon tree for the formula $F = ab + \overline{a}c$ and the lexicographic order is pictured Figure 25.3 (dashed lines represent *else*-outedges).

Indeed, such a representation is very space consuming. It is possible, however, to shrink it by means of the following two reduction rules.

- Isomorphic subtrees merging. Since two isomorphic subtrees encode the same formula, at least one is useless.
- Useless nodes deletion. A node with two equal sons is useless since it is equivalent to its son ($F = v.F + \overline{v}.F$).

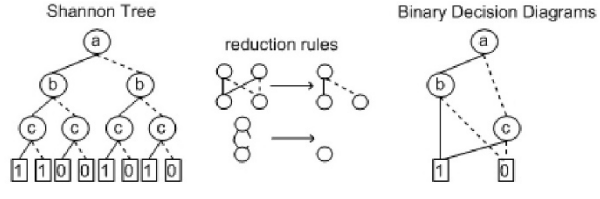


Figure 25.3. From the Shannon tree to the BDD

By applying these two rules as far as possible, one gets the BDD associated with the formula. A BDD is therefore a directed acyclic graph. It is unique, up to an isomorphism. This process is illustrated Figure 25.3.

25.2.3 Logical Operations

Logical operations (and, or, xor, ...) can be directly performed on BDD. This results from the orthogonality of the Shannon decomposition with usual connectives:

$$(v.F_1 + \overline{v}.F_0) \oplus (v.G_1 + \overline{v}.G_0)$$
$$=$$
$$v.(F_1 \oplus G_1) + \overline{v}.(F_0 \oplus G_0)$$

where $\oplus$ stands for any binary connective.

Among other consequences, this means that the complete binary tree is never built and then shrunk: the BDD encoding a formula is obtained by composing the BDD encoding its subformulae. Hash tables are used to store nodes and to ensure, by construction, that each node represents a different function. Moreover, a caching principle is used to store intermediate results of computations. This makes the usual logical operations (conjunction, disjunction) polynomial in the sizes of their operands. The complete implementation of a BDD package is described in reference [2].

25.2.4 Variable Orderings and Complexity Issues

It has been known since the very first uses of BDD that the chosen variable ordering has a great impact on the size of BDD and therefore on the efficiency of the whole methodology [1]. Finding the best ordering, or even a reasonably good one, is a hard problem (see *e.g.*, [17, 18]). Two kinds of heuristics are used to determine which variable ordering to apply. Static heuristics are based on topological considerations and select the variable ordering once for all (see, *e.g.*, [19, 20, 21]). Dynamic heuristics change the variable ordering at some points of the computation (see, *e.g.*, [3, 22]). They are thus more versatile than the former, but the price to pay is a serious increase of running time. Sifting is the most widely used dynamic heuristics [3]. We shall come back to this topic in Section 25.5.

25.2.5 Zero-suppressed Binary Decision Diagrams

Minato's zero-suppressed binary decision diagrams are BDD with a different semantics for nodes (and slightly different reduction rules) [10]. They are used to encode sets of minimal cutsets and prime implicants. Nodes are labeled with literals (and not just by variables). Let p be a literal and U be a set of products. By abuse, we denote p.U the set $\{\{p\} \cup \pi;\ \pi \in U\}$. The semantics of ZBDD is as follows.

The leaf 0 encodes the empty set: Set[0] = $\varnothing$.

The leaf 1 encodes the set that contains only the empty product: Set[1] = $\{\{\}\}$.

A node Δ(p,S1,S0), where p is a literal and S1 and S0 are two ZBDD encodes the following set of products.

Set[Δ(p,S1,S0)] = p.Set[S1] $\cup$ Set[S0]

It is possible to encode huge sets of MCS with relatively small ZBDD, provided MCS have some regularity that can be captured by the sharing of nodes.

25.3 Minimal Cutsets

Minimalcutsets (MCS for short) are the keystone of reliability studies. A minimal cutset is a minimal set of basic events that induces the realization of the top event. For coherent models, this informal definition is sufficient. It corresponds to the formal notion of prime implicant (PI for short). For non-coherent models, MCS and PI differ, for the latter contain negative literals while the former do not. A full understanding of both notions requires some algebraic developments (borrowed mainly to reference [11]).

25.3.1 Preliminary Definitions

A *literal* is either a variable v (positive literal), or its negation $\neg v$ (negative literal). v and $\neg v$ are said to be *opposite*. We write $\overline{p}$ the opposite of the

literal p. A *product* is a set of literals interpreted as the conjunction of its elements. Products are often written like words. For instance, the product {a, b, ¬c} is written $ab\bar{c}$. A *minterm* on a set of variables V = {v_1,...,v_n} is a product which contains exactly one literal built over each variable of V. We write minterms(V) for the set of minterms built on V. If V contains n variables, minterms(V) has 2^n elements.

An *assignment* of a set of variables V = {v_1,...,v_n} is a function σ from V to {0, 1} that assigns a value (true or false) to each variable of V. Using the truth tables of connectives, assignments are extended into functions from formulae built over V to {0, 1}. An assignment σ *satisfies* a formula F if σ(F) = 1. It falsifies F if σ(F) = 0.

There is a one-to-one correspondence between the assignments of V and the minterms built on V: a variable v occurs positively in the minterm π iff and only if σ(v)=1 in the corresponding assignment σ. For instance, the minterm $ab\bar{c}$ corresponds to the function σ such that σ(a)=σ(b)=1 and σ(c)=0, and vice-versa. Similarly, a formula F can be interpreted as the set of minterms (built on the set var(F) of its variables) that satisfy it. For instance, the formula $F = ab + \bar{a}c$ can be interpreted as the set $\{abc, ab\bar{c}, \bar{a}bc, \bar{a}b\bar{c}\}$. For the sake of convenience, we use set notations for formulae and minterms, *e.g.,* we note σ∈ F when σ(F)=1.

There exists a natural order over literals: ¬v < v. This order can be extended to minterms: $\pi \le \rho$ iff for each variable v, π(v)≤ ρ(v), *e.g.*, $\bar{a}\bar{b}c \le a\bar{b}c$ because a occurs negatively in $\bar{a}\bar{b}c$ and positively in $a\bar{b}c$. A physical interpretation of the inequality π≤ρ is that π contains less information than ρ for it realizes fewer basic events. From an algebraic viewpoint, the set minterms(V) equipped with the above partial order forms a lattice, as illustrated in Figure 25.4 (left). The order relation is represented by lines (bottom-up). For the sake of the simplicity, transitive relations are not pictured.

A formula F is said to be *monotone* if for any pair of minterms π and ρ such that $\pi \le \rho$, then ρ∈ F implies that π∈ F. The formula $F = ab + \bar{a}c$ is not monotone because, $\bar{a}\bar{b}c \in F$, $\bar{a}\bar{b}c \le a\bar{b}c$ but $a\bar{b}c \notin F$. This is graphically illustrated Figure 25.4 (right), where the minterms not in F are grayed. Coherent fault trees that are built over variables, and-gates, or-gates and *k*-out-of-*n* connectives are monotone formulae. Non-monotony is introduced by negations.

25.3.2 Prime Implicants and Minimal Cutsets

25.3.2.1 Prime Implicants

We can now introduce the notion of prime implicant. A *product* π is an implicant of a formula F if for all minterms ρ containing π, ρ∈ F. An implicant π of F is *prime* if no proper subset of π is an implicant of F. The set of prime implicants of F is denoted PI[F].

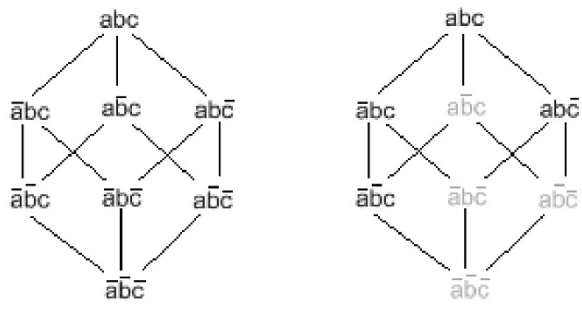


Figure 25.4. The lattice of minterms for {a,b,c}

For instance, the formula $F = ab + \bar{a}c$ admits the following set of prime implicants: $PI[F] = \{ab, \bar{a}c, bc\}$. Note that $\bar{a}b$ is an implicant of F because both $\bar{a}b\bar{c}$ and $\bar{a}bc$ satisfy F. It is prime because neither $\bar{a}$ nor b are implicants of F.

25.3.2.2 Minimal Cutsets

In reliability models, there exists a fundamental asymmetry between positive and negative literals. Positive literals represent undesirable and rare events such as failures. Negative literals represent thus the non occurrence of these events. Positive literals are the only ones that convey relevant information. This is the reason why most of the fault tree assessment tools never produce minimal cutsets with negative literals. To illustrate this idea, consider again the formula $F = ab + \bar{a}c$. We have $PI[F] = \{ab, \bar{a}c, bc\}$. This does correspond to the notion of minimal solutions of F, but this does not correspond to the intuitive notion of minimal cutsets. The expected minimal cutsets are ab and c which are the "positive parts" of prime implicants. There are cases however where negative literals are informative as well. This is typically the case when the values of some physical parameters have to be taken into account (see, *e.g.*, [23]). Thus, we have to consider the set L of literals that convey interesting information. L is typically the set of all positive literals plus possibly some negative literals. A literal p is *significant* if it belongs to L. It is *critical* if it is significant while its opposite is not.

Let V be a finite set of variables. Let L be a subset of significant literals built over V. Finally, let F be a formula built over V. We shall define minimal cutsets of F as minimal solutions (prime implicants) from which literals outside L are removed because they "do not matter". Let $PI_L[F]$ be the set of products obtained first by removing from products of PI[F] literals not in L and second by removing from the resulting set the non minimal products. Formally, $PI_L[F]$ is defined as follows.

$PI_L[F] = \{\pi \cap L;\ \pi \in PI[F]$ and there is no ρ in PI[F] such that $\rho \cap L \subset \pi \cap L\}$

This first definition captures the intuitive notion of minimal cutsets. For instance, it is easy to verify that $PI_{\{a,b,c\}}[ab + \bar{a}c] = \{ab, c\}$. However, it relies on the definition of prime implicants. This makes it not suitable for the design of an algorithm to compute MCS without computing prime implicants. The second way to define MCS which avoids this drawback is as follows. Let $\leq_L$ be the binary relation among opposite literals defined as follows.

$$p \leq_L \bar{p} \text{ if } p \notin L$$

The comparator $\leq_L$ is extended into a binary relation over minterms(V) as follows:

$$\sigma \leq_L \rho \text{ if for any variable v, } \sigma[v] \leq \rho[v],$$

where $\sigma[v]$ (or $\rho[v]$) denotes the literal built over v that belongs to σ (or. to ρ). Intuitively, $\sigma \leq_L \rho$ when σ is less significant than ρ. For instance, $ab\bar{c} \leq_{\{a,b,c\}} abc$ because $ab\bar{c}$ contains fewer positive literals than abc. The comparator $\leq_L$ is both reflexive ($\sigma \leq_L \sigma$ for any σ) and transitive ($\pi \leq_L \sigma$ and $\sigma \leq_L \rho$ implies $\pi \leq_L \rho$, for any π, σ and ρ). Therefore, $\leq_L$ is a pre-order.

A product π over V is a *cutset* of F w.r.t. L if $\pi \subset L$ and for all minterms σ containing π there exists a minterm $\delta \in F$ such that $\delta \leq_L \sigma$. A cutset π is *minimal* if no proper subset of π is a cutset. We denote by $MC_L[F]$ the set of minimal cutsets w.r.t. L of F.

Consider again the formula $F = ab + \bar{a}c$. If $L = \{a, \bar{a}, b, \bar{b}, c, \bar{c}\}$, minterms are pairwise incomparable. Therefore, MCS are products π such that all minterms σ containing π belong to F, $MC_L[F] = PI[F]$.

If $L = \{a,b,c\}$, $ab\bar{c} \leq_L abc$, and $\bar{a}\bar{b}c \leq_L abc$, $a\bar{b}c$, $\bar{a}bc$, therefore the cutsets of F w.r.t. L are abc, ab, ac, bc and c and $MC_L[F] = \{ab, c\}$. As an illustration, consider the product c. Four minterms contain it: abc, $\bar{a}bc$, $a\bar{b}c$, $\bar{a}\bar{b}c$. Except $a\bar{b}c$, they all belong to F. $\bar{a}\bar{b}c \leq_L a\bar{b}c$, therefore there is a minterm of F smaller than $\bar{a}\bar{b}c$. So, all the minterms containing c are covered and c is a cutset.

If $L = \{b, \bar{b}, c, \bar{c}\}$, the cutsets of F w.r.t. L are bc, b and c and $MC_L[F] = \{b,c\}$.

The two definitions of MCS are actually equivalent. Let F be a Boolean formula and let L be a set of literals built over var(F). Then, the following equality holds [11].

$$PI_L[F] = MC_L[F]$$

Note finally that if L=V, a positive product π is a cutset if and only if the minterm $\pi \cup \{\overline{v}; v \in V \text{ and } v \notin \pi\}$ is an implicant of F.

25.3.3 What Do Minimal Cutsets Characterize?

Any formula is equivalent to the disjunction of its prime implicants. A formula is not in general equivalent to the disjunction of its minimal cutsets. The widening operator ω_L gives some insights about the relationship between a formula F, its prime implicants and its minimal cutsets w.r.t. the subset L of the significant literals. The operator ω_L is an endomorphism of the Boolean algebra (minterms(V), $\cap$, $\cup$, $\overline{\ }$) that associates to each set of minterms (formula) F the set of minterms ω_L defined as follows.

$\omega_L = \{\pi$; there exists ρ s.t. $\rho \leq_L \pi$ and $\rho \in F\}$

Intuitively, ω_L enlarges F with all of the minterms that are more significant than a minterm already in F.

Consider again the formula $F = ab + \overline{a}c$.

If $L=\{a, \overline{a}, b, \overline{b}, c, \overline{c}\}$, then, $\omega_L[F] = F$.

If L={a,b,c}, then

$\omega_L[F] = abc + ab\overline{c} + a\overline{b}c + \overline{a}bc + \overline{a}\overline{b}c$.

If L={b, $\overline{b}$,c, $\overline{c}$ }, then

$\omega_L[F] = abc + ab\overline{c} + a\overline{b}c + \overline{a}bc + \overline{a}\overline{b}c$

The operator ω_L has the following properties.

ω_L is idempotent; $\omega_L(\omega_L(F)) = \omega_L(F)$.

$PI[\omega_L(F)] = MC_L[F]$.

The above facts show that ω_L acts as a projection. Therefore, the formulae F such that $PI[F]=MC_L[F]$ are the fixpoints of ω_L, *i.e.* the formulae such that $\omega_L(F) = F$. If L=V, fixpoints are monotone formulae. They also give a third way to define MCS: MCS of a formula F are the prime implicants of the least monotone approximation of F. This approximation is obtained by widening F with all of the minterms that are more significant, and therefore less expected, than a minterm already in F.

25.3.4 Decomposition Theorems

The recursive algorithms to compute prime implicants and minimal cutsets from BDD rely on so-called decomposition theorems. These theorems use the Shannon decomposition as a basis. They are as follows.

Decomposition Theorem for Prime Implicants [24]
Let $F = v.F_1 + \overline{v}.F_0$ be a formula (such that F_1 and F_0 don't depend on v). Then the set of prime implicants of F is the as follows.

$$PI[F] = PI_n \cup PI_1 \cup PI_0$$

where

$PI_n = PI[F_1.F_0]$
$PI_1 = \{v.\pi ; \pi \in PI[F_1]/PI_n\}$
$PI_0 = \{\overline{v} .\pi ; \pi \in PI[F_0]/PI_n\}$

and "/" stands for the set difference.

Decomposition Theorem for Minimal Cutsets [11]:
Let $F = v.F_1 + \overline{v}.F_0$ be a formula (such that F_1 and F_0 don't depend on v). Let L be the set of relevant literals. Then, the set of minimal cutsets F is the as follows.

Case 1: Both v and its negation belong to L. In that case, the decomposition theorem is the same as for prime implicants.

Case 2: v belongs to L, its negation does not. In that case, there are two ways to compute MCS[F].

First Decomposition:
$MCS[F] = MCS_1 \cup MCS_0$,
where

$MCS_0 = MCS[F_0]$
$MCS_1 = \{v.\pi; \pi \in MCS[F_1+F_0]/MCS_0\}$

Second Decomposition:
$MCS[F] = MCS_1 \cup MCS_0$,
where

$MCS_0 = MCS[F_0]$

$MCS_1 = \{v.\pi; \pi \in MCS[F_1] \div MCS_0\}$

and $P \div Q = \{\pi \in P ; \rho \in Q, \rho$ is not included in $\pi\}$

Case 3: Neither v nor $\overline{v}$ belong to L. In that case,

$$MCS[F] = MCS[F_1] \cup MCS[F0]$$

25.3.5 Cutoffs, p-BDD and Direct Computations

The number of prime implicants of a Boolean function involving *n* variables is in $O(3^n)$, and $O(2^n)$ if the function is monotone [25]. There is no direct relationship between the size of the BDD encoding the function and the ZBDD encoding its prime implicants. Not much progress has been done in establishing this relationship (see however [26]). In practice, it is sometimes the case that building the BDD is tractable, while building the ZBDD is not. Non-coherent models are more specifically subject to this phenomenon.

When the ZBDD takes too much time or space to build, it is still possible to apply cutoffs to keep only PI or MCS whose size (or equivalently probability) is lower than a given threshold. To do so, it suffices to introduce the threshold into the decomposition theorem (see [11] for more details).

Moreover, rather than computing the BDD and then the ZBDD encoding MCS, it is possible either to compute a truncated BDD and then the ZBDD from this truncated BDD [11] or to compute directly the ZBDD encoding (the most important) MCS [27] (see Section 25.5.1).

25.4 Probabilistic Assessments

One of the main advantages, if not the main, of the BDD technology for reliability and dependability analyses stands in the accuracy and the efficiency of the assessment of probabilistic quantities. In this section, we present algorithms to compute top event probabilities, importance factors, and to perform time dependent analyses.

25.4.1 Probabilities of Top (and Intermediate) Events

Top event probabilities can be assessed either from BDD or from ZBDD. Since these data structures are based on different decomposition principles, algorithms used in each case are different. Exact computations are performed with BDD. Rare events approximation is applied on ZBDD similarly to what is done with an explicit encoding of MCS, but with a better efficiency, thanks to sharing. The algorithm to compute the probability of a gate from a BDD is based on the Shannon Decomposition. It is defined by the following recursive equations [6].

$$\text{BDD-Pr}(0) = 0.0$$
$$\text{BDD-Pr}(1) = 1.0$$
$$\text{BDD-Pr}(v.F_1 + \overline{v}.F_0) = p(v).\text{BDD-Pr}(F_1) + (1-p(v)).\text{BDD-Pr}(F_0)$$

As a consequence, the result is exact. Moreover, a caching mechanism is used to store intermediate results. Therefore, the algorithm is linear in the size of the BDD.

The algorithm to compute the top event probability from a ZBDD is based on the rare events approximation, i.e: $p(S) \approx \sum_{\pi \in MCS[S]} p(\pi)$. It is defined by the following recursive equations.

$$\text{ZBDD-Pr}(0) = 0.0$$
$$\text{ZBDD-Pr}(1) = 1.0$$
$$\text{ZBDD-Pr}(v.S_1 \cup S_0) = p(v).\text{ZBDD-Pr}(S_1) + \text{ZBDD-Pr}(S_0)$$

The corresponding algorithm is also linear in the size of the ZBDD which is in general much smaller than the size of the set of MCS. Therefore, even when the BDD technology just mimics MCS calculations, it improves significantly the efficiency of the approach.

The assessment of importance factors rely on the computation conditional probabilities $p(S|e)$ and $p(S|\overline{e})$, where S is a gate and e is a basic event. BDD makes it possible to compute both (thanks again to the Shannon decomposition). Recursive equations are as follows.

BDD-Pr(0|e) = 0.0
BDD-Pr(1|e) = 1.0
BDD-Pr($v.F_1 + \overline{v}.F_0$ |e) = // if (v<e)
p(v).BDD-Pr(F_1|e) + (1-p(v)).BDD-Pr(F_0|e)
BDD-Pr($v.F_1 + \overline{v}.F_0$ |e) = // if (v>e)
BDD-Pr($v.F_1 + \overline{v}.F_0$)
BDD-Pr($v.F_1 + \overline{v}.F_0$ |v) = BDD-Pr(F_1|v)
BDD-Pr($v.F_1 + \overline{v}.F_0 | \overline{v}$) = BDD-Pr(F_0| $\overline{v}$)

Again, the corresponding algorithm gives exact results and is linear in the size of the BDD. The ZBDD algorithm is very similar and does not deserve a further presentation.

25.4.2 Importance Factors

One of the principal activities of risk assessment is expected to be either the ranking or the categorization of structures, systems and components with respect to their risk-significance or their safety significance. Several measures of such significance have been proposed for the case where the support model is a fault tree. These measures are grouped under the generic designation of "importance factors". Many articles and book chapters have been devoted to their mathematical expressions, their physical interpretations, and the various ways they can be evaluated by computer programs (see, *e.g.*, [7, 8]). Seminal work on the use of BDD to assess importance factors has been done by J. Andrews and his students [28 and 12], followed by Dutuit and Rauzy [14]. In this section, we review the main importance factors and we discuss the BDD and ZBDD algorithms to assess them. Our presentation follows mainly the reference [14].

25.4.2.1 Marginal Importance Factor

The first importance factor to consider is the marginal importance factor, denoted by MIF(S,e) which is defined as follows.

$$\mathrm{MIF}(S,e) = \frac{\partial(p(S))}{\partial(p(e))}.$$

MIF is often called the Birnbaum importance factor in the literature [29]. It can be interpreted, when S is a monotone function, as the conditional probability that, given that e occurred, the system S has failed and e is critical, *i.e.,* a repair of e makes the system work. The following equalities hold.

$$\mathrm{MIF}(S,e) = \frac{\partial(p(S))}{\partial(p(e))}$$

$$= p(S_{[e\leftarrow 1]}.\overline{S_{[e\leftarrow 0]}}) \qquad \text{(i)}$$

$$= p(S/e) - p(S/\overline{e}) \qquad \text{(ii)}$$

Equality (i) holds only in the case of monotone functions. Equality (ii) can be used to compute MIF(S,e), by means of two conditional probability calculations. However, MIF(S,e) can also be computed in a single BDD traversal using the following recursive equations.

BDD-MIF(0|e) = 0.0
BDD-MIF(1|e) = 0.0
BDD-MIF($v.S_1 + \overline{v}.S_0$ |e) = // if e < v
p(v).BDD-MIF(S_1|e) + (1-p(v)).BDD-MIF(S_0|e)
BDD-MIF($v.S_1 + \overline{v}.S_0$ |e) = 0.0 // if e > v
BDD-MIF($e.S_1 + \overline{e}.S_0$ |e) =
BDD-Pr(S_1|e) - BDD-Pr(S_0| $\overline{e}$)

The corresponding algorithm is linear in the size of the BDD. A last way to compute MIF(S,e) is to use a numerical differentiation. The ZBDD algorithm to compute MIF(S,e) is very similar and is also linear in the size of the ZBDD.

25.4.2.2 Other Classical Importance Factors: CIF, DIF, RAW and RRW

Beyond the MIF, the most diffuse importance factors and their definitions are reported in Table 25.1. We refer to [14, 30, 31] for a thorough discussion of the definitions of CIF, DIF, RAW and RRW. BDD and ZBDD algorithms to compute these importance factors are derived straight from their definition and the rare event approximation, respectively.

It is worth noting that there are many real-life models for which the ranking obtained with BDD and ZBDD algorithms do not coincide (see, *e.g.*, [15]). The effects of such a discrepancy are ignored

by most of the practitioners and by regulation authorities.

25.4.2.3 Discussion

The reliability engineering literature often refers to another importance factor called Fussel–Vesely which is defined as follows.

$$\mathrm{FV}(S,e) = \frac{p\left(\bigcup_{e.\pi \in \mathrm{MCS}[S]} e.\pi\right)}{p(S)}$$

If the rare event approximation is applied and the numerator is approximated by $\sum_{e.\pi \in \mathrm{MCS}[S]} p(e.\pi)$, we have FV(S,e) = CIF(S,e). Many authors consider thus that these two measures are actually the same. However, FV(S,e) as defined above has no interpretation in terms of system state. One of the merits of the introduction of BDD algorithm has been to show this kind of incoherence in the mathematical foundations of reliability engineering.

Recently,E. Borgonovo and G.E. Apostolakis introduced a new importance measure, called the differential importance measure (DIM), which is defined as follows [32].

$$\mathrm{DIM}(S,e) = \frac{\frac{\partial p(S)}{\partial p(e)} \mathrm{d}\,p(e)}{\sum_v \frac{\partial p(S)}{\partial p(v)} \mathrm{d}\,p(v)}$$

DIM(S,e) has a number of interesting properties. It is additive, so the DIM of a group of basic events is the sum of their DIM. It is shown in [32] that if the dp(v) are all the same then DIM(S,e) is proportional to MIF(S,e) and if the dp(v) are proportional to the p(v), then DIM(S,e) is proportional to CIF(S,e). As noted by the authors, the calculations of DIM(S,e) can be done at almost no cost once either the MIF(S,e)'s or the CIF(S,e)'s have been computed (depending of the chosen type of variations).

Table 25.1. Importance factors

Importance factor	Symbol	Definition	Rare event approximation
Top event probability	p(S)	p(S)	$\sum_{\pi \in \mathrm{MCS}[S]} p(\pi)$
Marginal importance factor	MIF(S,e)	$\frac{\partial(p(S))}{\partial(p(e))}$	$\sum_{e.\pi \in \mathrm{MCS}[S]} p(\pi)$
Critical importance factor	CIF(S,e)	$\frac{p(e)}{p(S)} \times \mathrm{MIF}(S,e)$	$\frac{\sum_{e.\pi \in \mathrm{MCS}[S]} p(e.\pi)}{\sum_{\pi \in \mathrm{MCS}[S]} p(\pi)}$
Diagnostic importance factor	DIF(S,e)	$p(e\|S) = \frac{p(e) \times p(S\|e)}{p(S)}$	$p(e) \times \mathrm{RAW}(S,e)$
Risk achievement worth	RAW(S,e)	$\frac{p(S\|e)}{p(S)}$	$\frac{\sum_{\pi \in \mathrm{MCS}[S]} p(\pi[e \leftarrow 1])}{\sum_{\pi \in \mathrm{MCS}[S]} p(\pi)}$
Risk reduction worth	RRW(S,e)	$\frac{p(S)}{p(S\|\overline{e})}$	$\frac{\sum_{\pi \in \mathrm{MCS}[S]} p(\pi)}{\sum_{\pi \in \mathrm{MCS}[S]} p(\pi[e \leftarrow 0])}$

25.4.3 Time Dependent Analyses

Another important issue stands in so-called time dependent analyses. A fault tree model makes it possible to assess system availability, *i.e.*, the probability that the system works at time t. The system reliability, *i.e.*, the probability that the system worked without interruption from time 0 to time t, can only be approximated if the system involves repairable components.

There are industrial systems for which the latter notion is more relevant than the former, *e.g.*, the safety instrumented system with a high demand described in the norm CEI 61508. Other norms require the assessment of an equivalent failure rate for the system, which is strongly related to its reliability, as we shall see. The accuracy and efficiency of BDD calculations make it possible to design interesting algorithms to approximate both reliability and equivalent failure rate. The following presentation follows reference [33].

25.4.3.1 Assumptions, Definitions and Basic Properties

Throughout this section, we make the following assumptions.

Systems under study involve repairable and non-repairable components.

Each component e has two modes (working and failed), a failure rate λ_e and repair rate μ_e. If the component is non-repairable, μ_e is null. λ_e and μ_e are constant through time. The probability $Q_e(t)$ that the component has failed at time t is therefore obtained by the following equation [9].

$$Q_e(t) = \frac{\lambda_e}{\lambda_e + \mu_e} \times \left(1 - e^{-(\lambda_e + \mu_e).t}\right)$$

Components are independent, *i.e.*, both their failures and their repairs are statistically independent.

Components are as good as new after a repair. They are as good as new at time 0. Failures of systems under study are modeled by means of coherent fault trees. In the sequel, we assimilate systems with their fault trees.

As a consequence, systems under study can also be represented as Markov models. Let S denote the system under study. Let T denote the date of the first failure of S. T is a random variable. It is called the lifetime of S.

The *availability* $A_S(t)$ of S at t is the probability that S is working at t, given that all its components were working at 0. The *unavailability* $Q_S(t)$ is just the opposite.

$$A_S(t) \stackrel{def}{=} \Pr\{\text{S is working at t}\}$$

$$Q_S(t) \stackrel{def}{=} 1 - A_S(t)$$

The *reliability* $R_S(t)$ of S at t is the probability that S experiences no failure during time interval [0,t], given that all its components were working at 0. The *unreliability*, or cumulative distribution function $F_S(t)$, is just the opposite. Formally,

$$R_S(t) \stackrel{def}{=} \Pr\{t < T\}$$

$$F_S(t) \stackrel{def}{=} \Pr\{t \geq T\} = 1 - R_S(t)$$

The curve $R_S(t)$ is a survival distribution. This distribution is monotonically decreasing. Moreover, the following asymptotic properties hold.

$$\lim_{t \to 0} R_S(t) = 1$$

$$\lim_{t \to \infty} R_S(t) = 0$$

Note that $Q_S(t) \leq F_S(t)$, for general systems and that $Q_S(t) = F_S(t)$, for systems with only non-repairable components. The algorithms described in Section 25.4.1 compute $F_S(t)$.

The *failure density* $f_S(t)$ refers to the probability density function of the distribution of T. It is the derivative of $F_S(f)$:

$$f_S(t) \stackrel{def}{=} \frac{d\,F_S(t)}{dt}$$

For sufficiently small dt's, $f_S(t).dt$ expresses the probability that the system fails between t and t+dt, given its was working at time 0.

The *failure rate* or hazard rate $r_S(t)$ is the probability the system fails for the first time per unit of time at age t. Formally,

$$r_S(t) \stackrel{def}{=} \lim_{dt \to 0} \frac{\Pr\{\text{S fails btw. t and t + dt} / C\}}{dt}$$

where C denotes the event "the system experienced no failure during the time interval [0,t]". The following property is well known.

$$R_S(t) = \exp\left[-\int_0^t r_S(u)\,du\right]$$

The *conditional failure intensity* $\lambda_S(t)$ refers to the probability that the system fails per unit time at time t, given that it was working at time 0 and is working at time t. Formally,

$$\lambda_S(t) \stackrel{def}{=} \lim_{dt\to 0} \frac{\Pr\{\text{S fails btw. t and t + dt / D}\}}{dt}$$

where D denotes the event: "the system S was working at time 0 and is working at time t". The conditional failure intensity is sometimes called Vesely rate. $\lambda_S(t)$ is an indicator of how likely the system is to fail.

The *unconditional failure intensity* $w_S(t)$ refers to the probability that the system fails per unit of time at time t, given it was working at time 0. Formally,

$$w_S(t) \stackrel{def}{=} \lim_{dt\to 0} \frac{\Pr\{\text{S fails btw. t and t + dt / E}\}}{dt}$$

where E denotes the event "the system was working at time 0". Note that $w_S(t) = f_S(t)$ for systems with only non-repairable components. The following property is easily deduced from the definitions [33]:

$$\lambda_S(t) = \frac{w_S(t)}{A_S(t)}.$$

The unconditional failure intensity is sometimes called the "instantaneous equivalent failure rate". In some reliability studies, regulation authorities require the computation of its mean value through a period of time. This *mean equivalent failure rate* is defined as follows:

$$\lambda_S^{[Mean]}(t) = \frac{\int_0^t \lambda_S(t).dt}{t}.$$

25.4.3.2 Calculations

The set of states in which the system S has failed can be decomposed in three subsets: the set S_1 of states in which the repair of the component e repairs the system, the set S_0 of states in which the failure of e repairs the system, and the set S_2 of states in which the system has failed, whatever the state of the component e.

Since the system is assumed to be coherent, $S_0 = \varnothing$. It follows that $S[e\leftarrow 1]$ describes $S_1 \cup S_2$ and $S[c\leftarrow 0]$ describes S_2. Let $CRIT_{S,e}(t)$ denote the probability that system S is in a critical state w.r.t. the component e at time t, *i.e.* a state in which S has not failed and a failure of e induces a failure of S. From the above developments, the following equality holds:

$$CRIT_{S,e}(t) = A_e(t) \times MIF_{S,e}(t).$$

For a sufficiently small value of dt, the probability that the system fails between t and dt is as follows:

$$\Pr\{\text{the system fails between t and t + dt}\} \approx \sum_{e\in S} dt.\lambda_e.CRIT_{S,e}(t).$$

Therefore, assuming that the system was perfect at time 0, the following equality holds:

$$w_S(t) = \sum_{e\in S} MIF_{S,e}(t).w_e(t),$$

where $w_e(t) = \lambda_e.A_e(t)$. In reference [33], four approximations of the reliability are considered, each having its own merits and drawbacks. They are given (without justification) in Table 25.2 .

Table 25.2. Approximations of reliability

Name	Approximation of $F_S(t)$
Murchland	$\int_0^t w_S(t).dt$
Barlow–Proschan [34]	$t.\lambda_S(\infty)$
Vesely	$1-\exp\left[-\int_0^t \lambda_S(u)\,du\right]$
asymptotic Vesely	$1-e^{-\lambda_S(\infty).t}$

The assessment of both the reliability and of equivalent failure rate rely on the evaluation of $w_S(t)$. Moreover, lots of calculations are required for numerical integrations. That is the reason why the BDD technology improves significantly, here again, the engineering process. In order to implement these computations, we need basically two algorithms: an algorithm to assess $Q_S(t)$ and an

algorithm to assess $MIF_{S,e}(t)$ or equivalently $w_S(t)$. Integrals are computed numerically using in general triangular approximation. Sections 25.4.1 and 25.4.2 present the algorithms to evaluate $Q_S(t)$ and $MIF_{S,e}(t)$. However, $w_S(t)$ can be obtained by means of two traversals of the BDD which avoids performing a computation of $MIF_{S,e}(t)$ for each basic event e. The corresponding recursive equations are as follows (for the sake of simplicity, the time t is omitted).

$$\text{BDD-w}(1) = 0$$
$$\text{BDD-w}(0) = 0$$
$$\text{BDD-w}(e.S_1 + \bar{e}.S_0) =$$
$$w_e \times [\text{BDD-Pr}(S_1) - \text{BDD-Pr}(S_0)] + p(e) \times \text{BDD-w}(S_1) + (1-p(e)) \times \text{BDD-w}(S_0)$$

The algorithm derived from the above equations is linear in the size of the BDD and therefore does not depend on the number of components, conversely to the algorithm that calculates the MIF of each component.

25.5 Assessment of Large Models

The assessment with BDD of large models, especially large event trees coming from the nuclear industry, is still challenging. Two different approaches can be tried to handle this problem: the first one consists of using ZBDD to implement classical MCS algorithms. The second approach consists of designing heuristics and strategies to reduce the complexity of the BDD construction. In this section, we discuss both approaches.

25.5.1 The MCS/ZBDD Approach

Set operations (union, intersection, elimination of non-minimal cutsets…) can be performed on ZBDD in the same way logical operations are performed on BDD. It is therefore possible to design ZBDD algorithms to compute MCS, without constructing BDD at all. Moreover, cutoffs can be applied on each intermediate ZBDD. By tuning these cutoffs, one is always able to get a result. In practice, the obtained results are often accurate enough. Such algorithms can be seen as ZBDD implementations of classical MCS algorithms, with the advantage of a compact representation and efficient set operations. The algorithm proposed in [27] outperforms the classical MCS algorithm previously implemented in the same fault tree tool. This additional success of the BDD technology should not hide the problems inherent in this approach.

These problems come from three sources: first, the MCS approximation of the underlying function; second, the use of cutoffs; and third, the use of rare event approximations. Rare event approximation is not really an issue if basic event probabilities are low (say below 10^{-3}), which is in general the case. Moreover, it is conservative. The effect of the two other approximations is pictured in Figure 25.5.

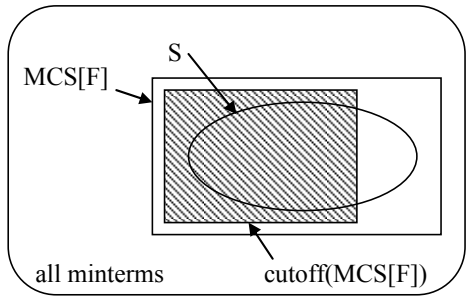


Figure 25.5. Effects of MCS approximation and cutoffs

Considering MCS[S] rather than the function S itself is an upper approximation of the function [11], *i.e.,* it is conservative. Note that MCS[S] = S if S is a coherent model. The use of cutoffs is an optimistic approximation of MCS[S]. It follows that if the model is not coherent, like success branches of event trees, what is computed and the actual function may be quite different. Epstein and Rauzy showed that the MCS approach may lead to erroneous results [15].

The determination of the "right" cutoffs requires some expertise and always results in a tradeoff between the complexity of calculations and the accuracy of the results [35, 36]. From a theoretical view point, nothing can prevent cutoffs from producing flawed results.

The MCS approach has another drawback: if the probability of a basic event varies (like in sensitivity analyses), the whole set of MCS should be recomputed which is indeed costly.

Despite all these problems, the MCS/ZBDD approach is the state-of-the-art technology used to assess large models of nuclear industry.

25.5.2 Heuristics and Strategies

Many techniques have been proposed to improve the construction of the BDD, including various preprocessing of the formula (rewritings, modularization), static and dynamic variable ordering heuristics, and strategies of construction. Dozens of articles have been published on those subjects. We give here only a few hints about their respective interest and limits.

Rewritings like those proposed in [37, 38] (coalescing, literal propagation, grouping of common factors, application of de Morgan's law) simplify formulae and must certainly be present in any fault tree assessment toolbox. However, they are not so easy to implement efficiently. Modularization [39, 40], which consists of isolating independent parts of the formulae, can also be helpful, but in our experience, large models have only few modules.

Most of the static variable ordering heuristics can be seen as two steps processes: first, arguments of gates are sorted according to some metrics and second, a depth first left most ordering is applied (*e.g.*, [20, 21]). This later ordering is interesting because it tends to keep close related variables. Static variable ordering heuristics can improve significantly the BDD construction. However, they are not versatile: a heuristic may be very efficient on one model and quite bad on another one. In [41], it is suggested to embed these heuristics into strategies. The idea is to rearrange more or less at random the arguments of gates and then to apply a heuristics. If the obtained formula is not tractable in a limited amount of time or space, then a new rearrangement is tried, and so on. The allowed time and space for each try may evolve based on the results of the first tries. This kind of strategy has been applied successfully to several large fault trees.

Dynamic variable reordering heuristics (see, *e.g.*, [3 and 22]) are considered as a significant improvement of the BDD technology when applied to logical circuits. Their application to large reliability models has been up to now quite deceptive: they are much too time consuming. It is often better to restart the calculation from scratch with a new candidate order, as suggested in [41].

Dramatic improvements can be obtained by combining the above ideas and there is room for innovation. Assessing large event trees of nuclear industry is still challenging.

25.6 Conclusions

Since their introduction in reliability and dependability studies, binary decision diagrams (BDD) have proved to be of great interest from both a practical and theoretical point of view. Not only does this technology provide more efficient and more accurate algorithms, but also mathematical foundations have been questioned and more firmly established.

In this chapter, we presented various aspects of the use of BDD for reliability and dependability studies. First, we discussed the mathematical basis of the notion of minimal cutsets (MCS). We described BDD algorithms to compute and to store MCS. Second, we reviewed the notion of importance factors. We gave recursive equations from which linear time BDD algorithms to compute MIF, CIF, DIF, RAW and RRW are easily derived. Third, we studied so-called time dependent analyses, which include approximations of reliability and computation of equivalent failure rates. Finally, we reviewed various techniques that can be used to handle large models.

The introduction of BDD in the reliability engineering framework has been successful. However, large event tree models coming from the nuclear industry are still out of the reach of an exact evaluation. It can be argued that these models are anyway too large to be mastered and that approximate computations are good enough. Nevertheless, the design of heuristics and strategies to handle these models and the integration of these

techniques into user friendly toolboxes would be a real accomplishment.

References

[1] Bryant R. Graph based algorithms for boolean function manipulation. IEEE Transactions on Computers 1986; 35(8):677–691.

[2] Brace K, Rudell R, Bryant R. Efficient implementation of a BDD package. In Proceedings of the 27th ACM/IEEE Design Automation Conference, IEEE 1990; 0738.

[3] Rudell R. Dynamic Variable ordering for ordered binary decision diagrams. In Proceedings of IEEE International Conference on Computer Aided Design, ICCAD 1993; Nov.:42–47.

[4] Bryant R. Symbolic Boolean manipulation with ordered binary decision diagrams. ACM Computing Surveys 1992; Sept. 24:293–318.

[5] Coudert O, Madre J.-C. Fault tree analysis: 10^{20} prime implicants and beyond. In Proceedings of the Annual Reliability and Maintainability Symposium, ARMS'93, Atlanta NC, USA. 1993; January.

[6] Rauzy A. New algorithms for fault trees analysis. Reliability Engineering and System Safety 1993; 59(2):203–211.

[7] Vesely WE, Goldberg FF, Robert NH, Haasl DF. Fault tree handbook. Technical report NUREG 0492, U.S. Nuclear Regulatory Commission 1981.

[8] Høyland A, Rausand M. System reliability theory. John Wiley & Sons, 1994; ISBN 0–471-59397.

[9] Kumamoto H, Henley EJ. Probabilistic risk assessment and management for engineers and scientists. IEEE Press, 1996; ISBN 0–7803-6017-6.

[10] Minato S.-I. Binary decision diagrams and applications to VLSI CAD. Kluwer, Dordrecht, 1996; ISBN 0–7923-9652-9.

[11] Rauzy A. Mathematical foundation of minimal cutsets. IEEE Transactions on Reliability 2001; 50(4):389–396.

[12] Sinnamon RM, Andrews JD. Improved accuracy in qualitative fault tree analysis. Quality and Reliability Engineering International 1997; 13:285–292.

[13] Sinnamon RM, Andrews JD. Improved efficiency in qualitative fault tree analysis. Quality and Reliability Engineering International 1997; 13:293–298.

[14] Dutuit Y, Rauzy A. Efficient algorithms to assess components and gates importance in fault tree analysis. Reliability Engineering and System Safety 2000; 72(2):213–222.

[15] Epstein S, Rauzy A. Can we trust PRA? Reliability Engineering and System Safety 2005; 88(3):195–205.

[16] Papadimitriou CH. Computational complexity. Addison Wesley, Reading, MA, 1994; ISBN 0-201-53082-1.

[17] Friedman SJ, Supowit KJ. Finding the optimal variable ordering for binary decision diagrams. IEEE Transactions on Computers 1990; 39(5):710–713.

[18] Bollig B, Wegener I. Improving the variable ordering of OBDDs is NP-complete. IEEE Trans. on Software Engineering 1996; 45(9):993–1001.

[19] Aloul FA, Markov IL, Sakallah KA. FORCE: A fast and easy-to-implement variable-ordering heuristic. Proceedings of GLVLSI 2003.

[20] Fujita M, Fujisawa H, Kawato N. Evaluation and improvements of Boolean comparison method based on binary decision diagrams. In Proceedings of IEEE International Conference on Computer Aided Design, ICCAD 1988; 2–5.

[21] Fujita M, Fujisawa H, and Matsugana Y. Variable ordering algorithm for ordered binary decision diagrams and their evaluation. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 1993; 2(1):6–12.

[22] Panda S, Somenzi F. Who are the variables in your neighborhood. In Proceedings of IEEE International Conference on Computer Aided Design, ICCAD 1995; 74–77.

[23] Yau M, Apostolakis G, Guarro S. The use of prime implicants in dependability analysis of software controlled systems. Reliability Engineering and System Safety 1998; 62:23–32.

[24] Morreale E. Recursive operators for prime implicant and irredundant normal form determination. IEEE Transactions on Computers 1970; C-19(6):504–509.

[25] Chandra AK, Markowsky G. On the number of prime implicants. Discrete Mathematics 1978; 24:7–11.

[26] Hayase K, Imai H. OBDDs of a monotone function and its prime implicants. Theory of Computing Systems 1998; 41:579–591.

[27] Jung WS, Han SH, Ha J. A fast BDD algorithm for large coherent fault trees analysis. Reliability Engineering and System Safety 2004; 83:69–-374.

[28] Sinnamon RM, Andrews JD. Quantitative fault tree analysis using binary decision diagrams. Journal Européen des Systèmes Automatisés, RAIRO-APII-JESA, Special Issue on Binary Decision Diagrams 1996; 30:1051–1072.

[29] Birnbaum ZW. On the importance of different components and a multicomponent system. In: Korishnaiah PR, editor. Multivariable analysis II. Academic Press, New York, 1969.

[30] Cheok MC, Parry GW, Sherry RR. Use of importance measures in risk informed regulatory applications. Reliability Engineering and System Safety 1998; 60:213–226.

[31] Vesely WE. Supplemental viewpoints on the use of importance measures in risk informed regulatory applications. Reliability Engineering and System Safety 1998; 60:257–259.

[32] Borgonovo E, Apostolakis GE. A new importance measure for risk-informed decision making. Reliability Engineering and System Safety 2001; 72(2):193–212.

[33] Dutuit Y, Rauzy A. Approximate estimation of system reliability via fault trees. Reliability Engineering and System Safety 2005; 87(2):163–172.

[34] Barlow RE, Proschan F. Theory for maintained system: Distribution of time to first failure. Mathematics of Operation Research 1976; 1:32–42.

[35] Čepin M. Analysis of truncation limit in probabilistic safety assessment. Reliability Engineering and System Safety 2005; 87(3):395–403.

[36] Jung WS, Han SH. Development of an analytical method to break logical loops at the system level**.** Reliability Engineering and System Safety 2005; 90(1):37–44.

[37] Camarinopoulos L, Yllera J. An improved top-down algorithm combined with modularization as highly efficient method for fault tree analysis. Reliability Engineering and System Safety 1985; 11:93–108.

[38] Niemelä I. On simplification of large fault trees. Reliability Engineering and System Safety 1994; 44:135–138.

[39] Chatterjee P. Modularization of fault trees: A method to reduce the cost of analysis. Reliability and Fault Tree Analysis, SIAM 1975; 101–137.

[40] Dutuit Y, Rauzy A. A linear time algorithm to find modules of fault trees. IEEE Transactions on Reliability 1996; 45(3):422–425.

[41] Bouissou M, Bruyère F, Rauzy A. BDD based fault-tree processing: A comparison of variable ordering heuristics. In: Soares C Guedes, editor. Proceedings of European Safety and Reliability Association Conference, ESREL, Pergamon, London, 1997; 3(ISBN 0–08–042835–5):2045–2052.

26

Field Data Analysis for Repairable Systems: Status and Industry Trends

David Trindade and Swami Nathan

Sun Microsystems Inc., USA

Abstract: The purpose of this chapter is to present simple graphical methods for analyzing the reliability of repairable systems. Many talks and papers on repairable systems analysis deal primarily with complex parametric modeling methods. Because of their highly esoteric nature, such approaches rarely gain wide acceptance into the reliability monitoring practices of a company. This chapter will present techniques based on non-parametric methods that have been successfully used within Sun Microsystems to transform the way reliability of repairable systems is analyzed and communicated to management and customers. Readers of the chapter will gain the ability analyze a large dataset of repairable systems, identify trends in the rates of failures, identify outliers, causes of failures, and present this information using a series of simple plots that can be understood by management, customers and field support engineers alike.

26.1 Introduction

Any system that can be restored to operating condition after experiencing a failure can be defined as a repairable system. The restoration to operating condition can be any action, manual or automated, that falls short of replacing the entire system. A non-repairable system, on the other hand, is discarded upon failure, *i.e.*, there are no cost effective actions to restore the system to its operating state. Repairable systems are common in all walks of life, *e.g.*, computer servers, network routers, printers, storage arrays, automobiles, locomotives, *etc*. Although repairable systems are very common, the techniques for analyzing repairable systems are not as prevalent as those for non-repairable systems. Most textbooks on reliability deal primarily with the analysis of non-repairable systems.

The techniques for repairable systems found in the literature are primarily parametric methods based on assuming a non-homogeneous Poisson process. These techniques demand a high degree of statistical knowledge on the part of the practitioner to understand various distributional assumptions, the concept of independence, and so on. This situation often leads to incorrect analysis techniques due to confusion between the hazard rate and rate of occurrence of failures [1, 2]. Furthermore, the difficulty of communicating these techniques,to management and customers (who often lack statistical background knowledge) renders them impractical for widespread usage within an organization.

Widespread adoption of any technique can become a reality within an organization only if it is easy to use as well as articulated by the lay person. Recently, analysis of repairable systems based on non-parametric methods have become increasingly popular due to their simplicity as well as their ability to handle more than just *counts of recurrent events* [3, 4, 5, 6, 7].

This chapter provides a simple yet powerful approach for performing reliability analysis of repairable systems using non-parametric methods. Simple plotting methods can be used for identifying trends, discerning deeper issues relating to failure modes, assessing effects of changes and comparing reliability across platforms, manufacturing vintages, and environments. These approaches have been applied with great success to datacenter systems (both hardware and software). This chapter is based on courses and training sessions given to sales, support services, management, and engineering personnel within Sun Microsystems™. These techniques can be easily applied within a spreadsheet environment such as StarOffice™ or Excel™ by anybody. Only a very rudimentary knowledge of statistics is needed. Interesting examples and case studies from actual analysis of computer servers at customer datacenters are provided for all concepts.

Notation and Acronyms

MTBF	mean time between failure
MCF	mean cumulative function
CTF	calendar time function
RR	recurrence rate
ROCOF	rate of occurrence of failures
HPP	homogeneous Poisson process
NHPP	non-homogeneous Poisson process

26.2 Dangers of MTBF

The most common metric used to represent the reliability of repairable systems is MTBF or mean time between failures. This term is used pervasively and indiscriminately in many industries. MTBF is calculated by adding all the operating hours of all the systems and dividing by the number of failures. The popularity of the MTBF metric is due to its simplicity and its ability to cater to the *one number syndrome*. MTBFs are often stated by equipment manufacturers with imprecise definitions of a failure. MTBF hides information by not accounting for any trends in the arrival of failures and treating machines of all ages as coming from the same population.

There are several assumptions involved in stating an MTBF. Firstly, it is assumed that the failures of a repairable system follow a renewal process, *i.e.,* all failure times come from a single population distribution. A further assumption is that the times between events are independent and exponentially distributed with a constant rate of occurrence of events, and consequently, we have what is called a homogeneous Poisson process (HPP). The validity of a HPP is rarely checked in reality. As a result, strict reliance on the MTBF without a full understanding of the consequences can result in missing developing trends and drawing erroneous conclusions.

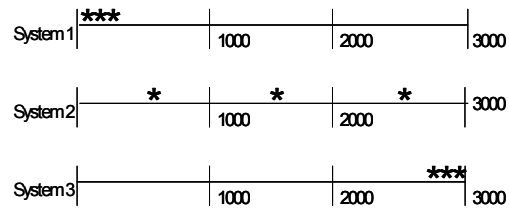


Figure 26.1. MTBF hides information

In Figure 26.1, we have three systems that have been operating for 3000 hours. Each system has experienced three failures within those 3000 hours. The MTBF for all three systems is 3000/3 = 1000 hours. The three machines have identical MTBFs but are their behaviors identical? Let us assume that each failure represents failure of an air regulator in scuba diving equipment. Which system should a user choose? Based on MTBFs, a customer may decide that any system is as good as the other for the next dive. However, System 1 had three early failures and none thereafter. System 2 had a failure in each 1000 hour interval while System 3 had three recent failures. The behaviors of the three systems are dramatically different and yet they have the same MTBF! When a customer is

shown the complete data instead of just MTBFs, the decision would be quite different. Thus, MTBF hides information. Relying entirely on a single metric can have severe consequences.

At the design stage of a product, the designer has to deal with components that are new and have no failure history. Often it may not be possible to find components from previous generations of the product that are "similar" in order to use field data. In these situations, it is permissible to use an MTBF for each component to build reliability estimates at the system levels. These metrics are used primarily to evaluate the relative merits of one design alternative against the other. It can also be used to make initial estimates of service costs and spares planning. However, it is not to be used as a guarantee on the reliability that a customer would experience. The following example illustrates how failures are actually distributed in the presence of a HPP.

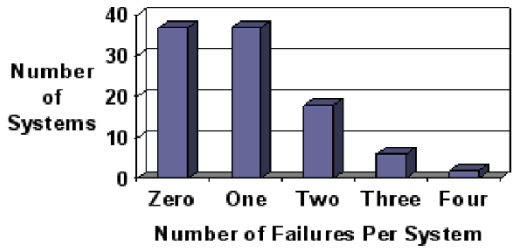


Figure 26.2. Distribution of 100 failures across 100 systems reaching MTBF

Consider a group of 100 identical HPP systems with an MTBF of 1000 hours. When all the systems reach 1000 hours, the expected number of failures is 1 failure per system or 100 total failures. However, we can use the Poisson distribution with an MTBF of 1000 hours to calculate the number of machines with zero, one, two failures and so on.

When all the systems reach 1000 hours (MTBF) there will be 37 systems with zero failures (on the average), 37 machines with 1 failure, 18 with 2 failures, 6 machines with 3 failures and 2 machines with 4 failures. It is obvious that from simple Poisson calculations there will be machines with 2, 3, and 4 failures. So a customer who assumes or is made to assume that the MTBF is a system life guarantee is going to be completely misled. Clearly there is a need for better reliability metrics that account for the time dependent nature of the reliability of repairable systems.

26.2.1 The "Failure Rate" Confusion

Despite Ascher's arguments more then 20 years ago [8], the term failure rate continues to be arbitrarily used in the industry and sometimes in academia to describe both a hazard rate of a lifetime distribution of a non-repairable system and a rate of occurrence of failures of a sequences of failure times of a repairable system. This lack of distinction can lead to poor analysis choices even by practicing reliability engineers.

Often the reciprocal of the MTBF is used to obtain what is commonly referred to as a failure rate. However the term failure rate has become a confusing term in the literature [1, 2] and even more so in the industry. Failure rate has been used for non-repairable systems, repairable systems and non-repairable components functioning within a repairable system. In each case, the meaning of the term changes slightly and the nuance is often lost on even the most well-intentioned of practitioners. Often engineers analyze data from repairable systems using methods for the analysis of data from non-repairable systems.

A non-repairable system is one that is discarded upon failure. The lifetime is a random variable described by a single time to failure. For a group of systems, the lifetimes are assumed to be *independent and identically distributed, i.e.*, from the same population. In this case, the "failure rate" is the hazard rate of the lifetime distribution and is a property of a time to failure. The hazard rate is the *conditional* probability that a component fails in a small time interval given that it has survived from zero until the beginning of the time interval. It is the *relative rate* of failure of a component that has survived until the previous instant.

A repairable system, on the other hand, is one that can be restored to an operating condition by any means short of replacing the entire system. The lifetime of the system is the age of the system or the total hours of operation. The random variables of interest are the *times between failures* and

number of failures at a particular age. In this case, the "failure rate" is the rate of occurrence of failures and is a property of a sequence of failure times. ROCOF or rate of occurrence of failures is the probability that a failure (not necessarily the first) occurs in a small time interval. It is the *absolute rate* at which failures occur.

Table 26.1 shows 10 failures. The failure times are provided in column 2 and the times between failures are provided in column 3. Each failure time represents failure of the server due to a CPU. The CPU is replaced with an identical CPU from the same population.

Table 26.1. Failure data for a CPU in a computer server

Failure Number	Failure Times	Time Between Failures
1	876	876
2	2382	1506
3	2576	194
4	2863	287
5	2912	49
6	2964	52
7	3120	156
8	3195	75
9	3249	54
10	3284	35

Let us consider the failure of a computer server due to a central processing unit or CPU. The computer server is a repairable system while the CPU is a non-repairable component. Table 26.1 provides the failure data.

If the data is analyzed as if it were from a non-repairable system, then the times between failures are treated as lifetimes of the CPU, *i.e.*, times to failure. The lifetimes can be sorted and a distribution can be fit to the ordered times to failure. There is no difference between the CPU being replaced 10 times within the server and 10 CPUs placed on a life test. Figure 26.3 shows a Weibull fit to the data. Maximum likelihood estimation provides a characteristic life of 277 and a shape parameter of 0.78. Since the shape parameter is less than 1, we can conclude that we have a decreasing hazard rate. In a repairable systems approach, we would plot the failures of

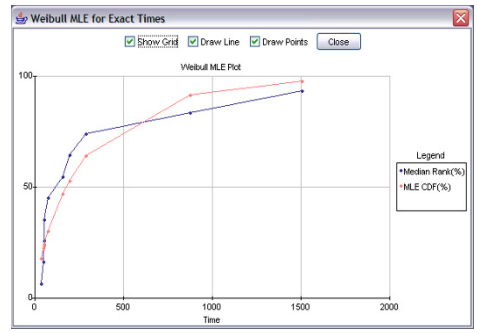


Figure 26.3. Weibull fit for the data in Table 26.1

CPUs as it would happen in the server, *i.e.*, against the age of the server.

In Figure 26.4, we have a plot of the cumulative number of CPU failures as a function of the age of the computer server. We can see that as the server gets older, CPU failures appear to be happening faster, *i.e.*, the slope of the curve which is the rate of occurrence of failures is actually increasing!

How can the rate of failures be increasing in reality when the Weibull analysis showed a decreasing rate? This behavior occurs because the times between failures are not independent and identically distributed. The time to first failure distribution is not identical to the time between first and second failure distribution and so on. The order of occurrence of failures is important because the component failures need to be viewed in the repairable system context. In fact, the fan was degrading in the computer, resulting in decreased ability of the system to remove thermal load. Increasing ambient temperatures decreased the

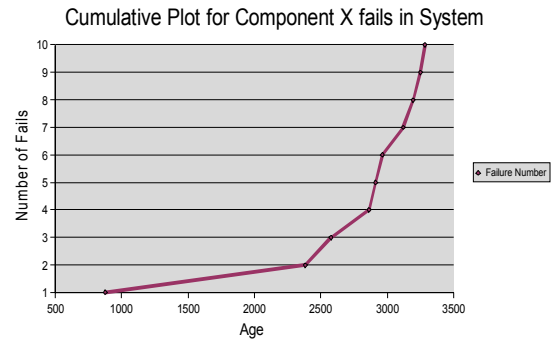


Figure 26.4. Cumulative CPU fails *vs*. system age

prospective lifetime of the CPU. Even though each replaced CPU was from the same population, it was performing in a harsher environment than its predecessor. Hence the Weibull analysis was invalid.

26.3 Parametric Methods

Most of the literature on the reliability of repairable systems deals with parametric methods. One of the common parametric approaches to modeling repairable systems reliability typically assumes that failures occur according to a non-homogeneous Poisson process with an intensity function. One of the popular intensity functions is the power law Poisson process [9, 10], which has an intensity function of the form

$$u(t) = \lambda\beta t^{\beta-1} \qquad \lambda, \beta > 0 \tag{26.1}$$

The probability that a system experiences n failures in *t* hours has the following expression:

$$P(N(t) = n) = \frac{(\lambda t^{\beta}) e^{-\lambda t^{\beta}}}{n!} \tag{26.2}$$

To estimate the two parameters in the model one can use maximum likelihood estimation. The equations for the parameter estimates are given in [8, 9]

$$\hat{\lambda} = \frac{\sum_{q=1}^{K} N_q}{\sum_{q=1}^{K} T_q^{\hat{\beta}} - S_q^{\hat{\beta}}}$$

$$\hat{\beta} = \frac{\sum_{q=1}^{K} N_q}{\hat{\lambda}\sum_{q=1}^{K}(T_q^{\hat{\beta}} \ln T_q - S_q^{\hat{\beta}} \ln S_q) - \sum_{q=1}^{K}\sum_{i=1}^{N_q} \ln X_{iq}} \tag{26. 3}$$

where we have *K* systems, *S* and *T* are start and end times of observation accounting for censoring, *Nq* is the number of failures on the *q*th system and *Xiq* is the age of the *q*th system at the *i*th failure.

These equations cannot be solved analytically and require an iterative procedure or special software. Crow [9] also provides methods for confidence interval estimation and a test statistic for testing the adequacy of the power law assumption. Further extensions of renewal process techniques known as the generalized renewal process were proposed by Kijima [11, 12]. Kijima models removed several of the assumptions regarding the state of the machine after repair that were present in earlier models. However, because of the complexity of the renewal equation, closed form solutions are not possible and numerical analysis can be quite tedious.

A Monte Carlo simulation based approach for the Kijima formulation was developed in [13]. Mettas and Zhao [14] present a general likelihood function formulation for estimating the parameters of the general renewal process in the case of single and multiple repairable systems. They also provide confidence bounds based on Fisher information matrix. A variety of intensity functions can be used and the software reliability literature has a plethora of such models.

Due to the complexity of these models, analysts often resort to using a simple HPP by hiding behind Drenick's theorem [15], which states that the superposition of a large number of stochastic processes over a long period of time behaves like a homogeneous Poisson process. This "central limit theorem" for renewal processes has been much abused similar to the indiscriminate usage of the normal distribution in day to day statistical analysis.

Despite the abundance of literature on the subject, parametric approaches are computationally intensive and not intuitive to the average person who performs data analysis. Special solution techniques are required along with due diligence in justifying distributional assumptions (rarely done in practice). The incorrect application of Weibull analysis shown in the previous section is a classic example. Communicating reliability information to customers using parametric methods can become quite difficult because often times customers think information is being hidden through *statistical cleverness*.

Non-parametric approaches based on MCFs are far simpler, understandable by lay persons and customers, and are easily implemented in a spreadsheet. The next sections cover the methodology.

26.4 Mean Cumulative Functions

26.4.1 Cumulative Plots

Given a set of failure times for a repairable system, the simplest graph that can be constructed is a cumulative plot.

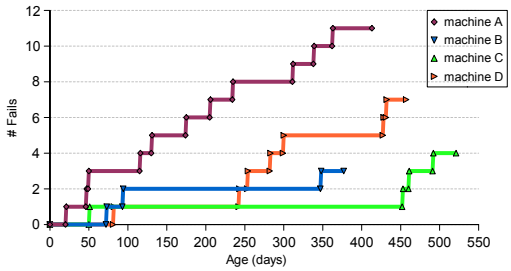


Figure 26.5. Cumulative plots for a group of four machines

The cumulative plot is a plot of the number of failures *versus* the age of the system.

The term failure is a generic term in the sense that one can plot hardware failures, software failures, outages, reboots, combinations of all failure modes, *etc*. The cumulative plot shows the evolution of failures over time. We can construct such a plot for every machine in the population. Figure 26.5 shows an example cumulative plot for a population with four machines. We have data on the age of the machine at various failure events. For example, machine C had one failure at 50 days and was failure free for over 400 days. After about 450 days machine, C had a rash of failures within the next 100 days of operation. Machine A has had the most number of failures at all ages.

Although a cumulative plot looks quite simple it is of great importance because of its ability to reveal trends. Figures 26.6, 26.7, and 26.8 show three different cumulative plots.

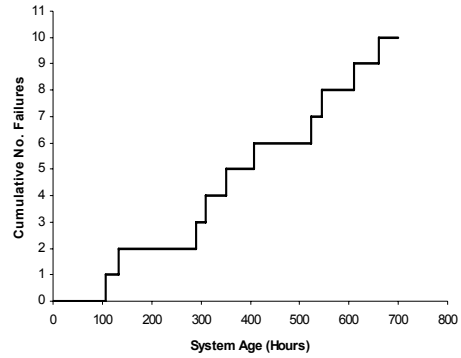


Figure 26.6. Cumulative plot for a stable system

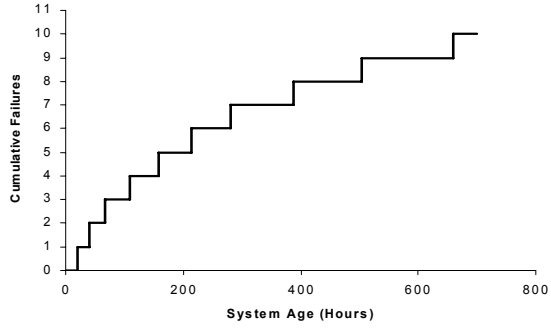


Figure 26.7. Cumulative plot for an improving system

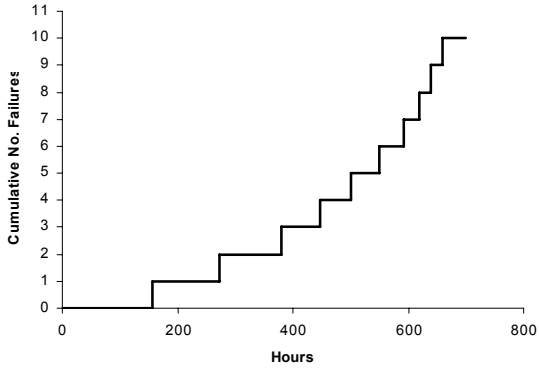


Figure 26.8. Cumulative plot for a worsening system

The shape of the cumulative plot can provide ready clues as to whether the system is improving, worsening, or stable. An improving system has the times between failures lengthening with age (takes longer to get to the next failure) while a worsening

system has times between failures shortening with age (takes less time to get to the next failure).

It is to be noted that all three plots show a system with 10 failures in 700 hours, *i.e.*, MTBF of 70 hours. Despite having identical MTBFs, the behaviors of the three systems are dramatically different.

26.4.2 Mean Cumulative Function *Versus* Age

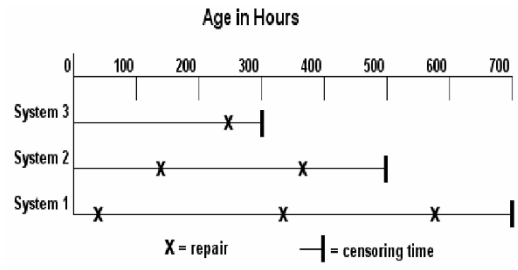
Typically a population consists of numerous machines, and so it could be quite tedious to construct a cumulative plot for each machine and visually extract the trend. A useful construct would be to plot the average behavior of these numerous machines. This is accomplished by calculating the mean cumulative function (MCF).

By taking a vertical slice on the set of cumulative plots at a particular point in time we can compute an average number of failures at that point in time. By moving this vertical slice along the time axis we can imagine an average function begin to emerge. The MCF is constructed incrementally at each failure event by considering the number of machines at risk at that point in time. The number of machines at risk depends on how many machines are contributing information at that particular point in time. Information can be obscured by the presence of censoring and truncation.

Right censoring occurs when information is not available beyond a certain age, *e.g.*, a machine that is 100 days old cannot contribute information to the reliability at 200 days, and hence is not a *machine at risk* when calculating the average at 200 days. Some machines may be removed from the population, *e.g.*, decommissioned. If a machine is decommissioned when it is 500 days old, then it is no longer a machine at risk when calculating the fails/machine at 600 days.

Left censoring occurs when information is not available before a certain age. Information may be obscured at earlier ages if for example a machine is installed on 1 June 2005 and the service contract was initiated on 1 June 2006. In this case there is no failure information available during the first year of operation. Therefore, this machine cannot contribute any information before 365 days of age but will factor into the calculation only after 365 days. One could also have interval or window censoring that is dealt with extensively in [16]. The MCF accounts for gaps in information by appropriately normalizing the number of failures by the number of machines at risk at each point in time and accumulating them.

The example below illustrates a step by step calculation of the MCF for three systems. The failure and censoring times are first sorted by magnitude. Now we can look at the population from a common time zero and see the evolution of failures and censoring with age. At age 33, system 1 had a failure, and since three machines operated beyond 33 hours (*i.e.,* number of machines at risk is three), the fails/machine is 1/3 and the MCF is 1/3. The MCF aggregates the fails/machine at all points in time where failures happen. At 135 hours, system 2 has a failure and there are still three machines at risk in the population. Therefore the fails/machine is 1/3, and the MCF aggregate of the fails/machine at points of failure is now 2/3. Similarly at 247 hours the MCF jumps to 3/3 due to a failure of System 3. At 300 hours, system 3



Time (Hrs)	Number of Systems at Risk	Failures per Machine	MCF
33	3	1/3	1/3
135	3	1/3	2/3
247	3	1/3	1
300	3		1
318	2	1/2	1.5
368	2	1/2	2
500	2		2
582	1	1/1	3
700	1	1/1	3

Figure 26.9. Step by step calculation of the MCF

drops out of the calculation, and the number of machines at risk becomes two. System 3 drops out not because it is removed (in this case), but simply because it is not old enough to contribute information beyond its current age, *i.e.*, it is not a machine at risk at ages beyond 300. At 318 hours, system 1 has a failure, and the fails/machine is now 1/2 since we have only two machines in the population that are contributing information. The MCF now becomes 3/3+1/2 and so on. This fairly straightforward procedure can be easily implemented in a spreadsheet.

Statistical software like SAS can be used to easily automate such a calculation for thousands of machines. Figure 26.10 shows the MCF for the population of machines shown in Figure 26.5. The MCF represents the average number of failures experienced by this population as a function of age. If a new machine enters the population, the MCF represents its expected behavior. It is to be noted that the parametric methods with all the distributional assumptions and mathematical complexities eventually attempt to estimate the same average number of failures *versus* system age. Confidence intervals can be provided for the MCF. Nelson [3, 7] provides several procedures for point-wise confidence bounds.

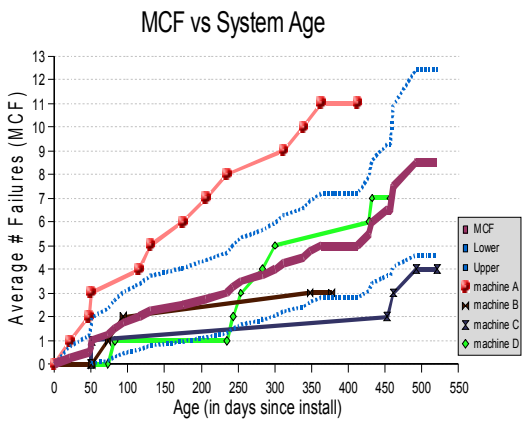


Figure 26.10. MCF and confidence intervals for the population in Figure 26.5

26.4.3 Identifying Anomalous Machines

In computer systems installed in datacenters, often a small number of misbehaving machines tend to obscure the behavior of the population at large. When the sample sizes are not too large, the simple confidence bounds can serve to graphically point out machines that have been having an excessively high number of failures compared to the average. In Figure 26.10, we can see that machine A has been having a much higher number of failures than the average at all ages. Although it is not a statistically correct test of an outlier, overlaying the cumulative plots of individual machines with the MCF and confidence bounds tend to visually point to problem machines when sample sizes are small. Support engineers can easily identify these problem machines and propose remediation measures to the customer. When sample sizes are larger, the confidence limits are close to the mean and so a visual approach would be meaningless to identify errant cumulative plots. More rigorous approaches for identifying these anomalous machines has been the subject of recent research. Glosup [17] proposes an approach for comparing the MCF with N machines with the MCF for (N−1) machines and arrive at a test statistic for determining if the omitted machine had a significant influence on the MCF. Heavlin [18] proposed a powerful alternate approach based on 2X2 contingency tables and the application of Cochran Mantel Hanzel statistic to identify anomalous machines. It can be thought of as an extension of the log rank test used to compare two Kaplan–Meier survival curves to mean cumulative functions.

26.4.4 Recurrence Rate *Versus* Age

Since the MCF is the cumulative average number of failures *versus* time one can take the slope of the MCF curve to obtain a rate of occurrence of events as a function of time. This slope is called the recurrence rate to avoid confusion with terms like failure rate [7].

The recurrence rate can be calculated by a simple numerical differentiation procedure, *i.e.,* estimate the slope of the curve numerically. This

can be easily implemented in a spreadsheet using the SLOPE(Y_1:Y_n, X_1:X_n) function where MCF is the Y axis and time is the X axis. One can take five or seven adjacent points and calculate the slope of that section of the curve by a simple ruler method and plot the slope value at the midpoint. The degree of smoothing is controlled by the number of points used in the slope calculation [19]. The rate tends to amplify sharp changes in curvature in the MCF. If the MCF rises quickly, it can be seen by a sharp spike in the recurrence rate, and similarly, if the MCF is linear the recurrence rate is a flat line. When the recurrence rate is a constant, it may be a reasonable assumption to conclude that the data follows a HPP, allowing for the use of metrics such as MTBF to describe the reliability of the population. It is also possible to fit an NHPP to the MCF and then take the derivative to get a smooth recurrence rate function which can be used for extrapolation and prediction.

Figure 26.11 is an example of a recurrence rate from a population of systems at a customer site. One can see from Figure 26.11 that the recurrence rate is quite high initially and drops sharply after around 50 days. Beyond 50 days the recurrence rate is fairly stable and keeps fluctuating around a fairly constant value. If the cause of failures were primarily hardware, then this would indicate potential early life failures, and one would resort to more burn-in or pre-release testing. In this case, the causes of the failures were more software and configuration type issues. This problem was identified as *learning curve issues* with systems administrators. When new software products are released, there is always a learning process to figure out the correct configuration procedures, setting up the correct directory paths, network links and so on. These activities are highly prone to human error because of lack of knowledge, improper documentation, and installation procedures. Making the installation procedure simpler and providing better training to the systems administrators resolved this issue in future installs of the product. Recurrence rates can be invaluable in identifying situations of interest to managing systems at customer sites.

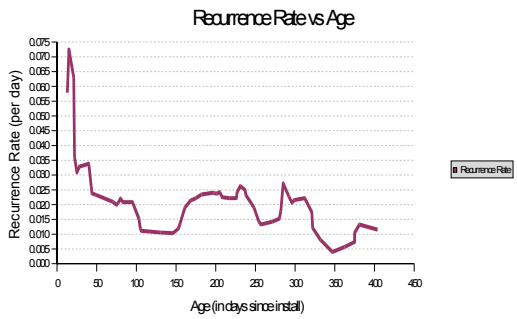


Figure 26.11. Example of recurrence rate *versus* age

26.5 Calendar Time Analysis

The reliability literature for the most part focuses on analyzing reliability as a function of the age of the system or the component. The time axis is always lifetime of the component from time zero. This approach is used because the systems are assumed not to undergo any dramatic changes during lifetimes other than routine maintenance. In the case of advanced computing and networking equipment installed in datacenters, the systems undergo changes on a routine basis that affect the reliability. There are software patches, upgrades, new applications, hardware upgrades to faster processors, larger memory, physical relocation of systems, *etc*. This situation can be quite different from other repairable systems like automobiles where the product configuration is fairly stable from production. Cars may undergo changes in the physical operating environment, but rarely do we see upgrades to a bigger transmission.

In datacenter systems many of the effects are a result of operating procedures that change the configuration and operational environment and not related to the age. So the textbook notion of the bathtub curve effects is often overwhelmed by activities that occur within a datacenter during particular periods of time. These changes are typically applied to a population of machines in the datacenter and the machines can all be of different ages. For example, we may have machines that were installed at various points during 2005. On 1 June 2006 all these machines will have different ages. However, an operating system upgrade may

be performed on all the machines on this particular date. If this improves or worsens the number of outages, then it is not an age related effect but a calendar time effect. It will be difficult to catch changes if the analysis is done as a function of the only of the age of the machine, but some effects will be quite evident when the events are viewed in calendar time [6]. This possibility is illustrated in Figures 26.12a and 26.12b.

Figure 26.12a shows the recurrence rate *versus* age for two systems, *i.e.*, the slopes of their cumulative plots. One can see that System 1 had a spike in the rate around 450 days while system 2 had a spike in the rate around 550 days. When looked at purely from an age perspective one can

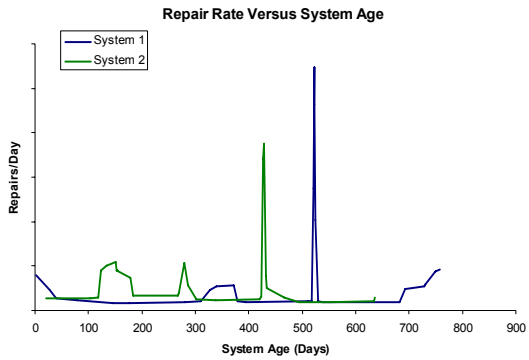


Figure 26.12(a). Recurrence rates for two systems *versus* age

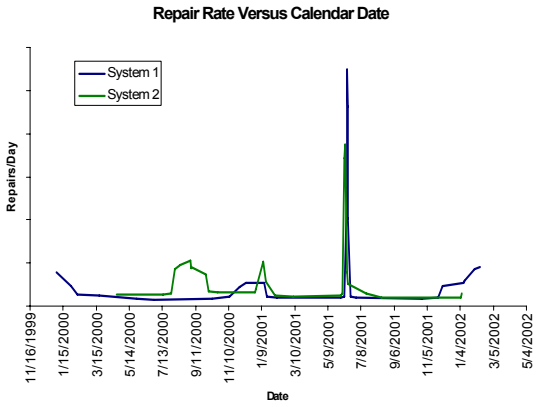


Figure 26.12(b). Recurrene rate for two systems *versus* date

easily conclude that they were two independent spikes related only to that particular system. One might falsely conclude that two different failure mechanisms may be in place. However, in Figure 26.12b, the recurrence rate *versus* date shows that the two spikes coincide on the same date. This indicates clearly that we are not dealing with an age related phenomenon but an external event related to calendar time. In this case it was found that a new operating systems patch was installed on both machines at the same time, and shortly thereafter, there was an increase in the rate of failures. By plotting the date as a function of calendar time one can easily separate the age related phenomenon from the date related phenomenon.

Calendar time analysis can reveal causes that will never be found by an age related analysis. In one study, a customer complained that all platforms from 2 processor machines to 32 processor machines were having serious quality problems. The customer mentioned that there were failures being observed at all ages of the machines indicating a severe quality problem. When the data was analyzed in calendar time, each platform showed a spike in the recurrence rate starting April of that year. When the customer was questioned about any special events that occurred in April, it was revealed that the customer had relocated all the machines from one datacenter to another and that the relocation was performed while construction was being complete. Clearly the stress of relocation and working in a not so clean environment was showing as problems in all platforms meaning there was not a severe quality problem with the products.

In order to analyze the data in calendar time, one can perform an analogous procedure by calculating the cumulative average number of fails per machine at various dates of failure. This result is called the calendar time function (CTF). We begin with the date on which the first machine was installed and calculate the number of machines at risk at various dates on which events occurred. As more machines are installed, the number of machines at risk keeps increasing until the current date. The population will decrease if machines are physically removed from the datacenter at

particular dates. This consideration is contrary to the machines at risk as a function of age where the number of machines will be a maximum at early ages and will start decreasing as machines are no longer old enough to contribute information. The calculation is identical to the table shown in Figure 26.9 except that we have calendar dates instead of age. The recurrence rate *versus* date is extremely important in practical applications because support engineers and customers can more easily correlate spikes or trends with specific events in the datacenter. The calculation of the recurrence rate *versus* date is identical to the procedure outlined for recurrence rate *versus* age. The SLOPE function in spreadsheets automatically converts dates into days elapsed and can calculate a numerical slope. This routine is an extremely useful and versatile function in spreadsheets.

26.6 Failure Cause Plots

The common approach to representing failure cause information is a Pareto chart or simple bar chart as shown in Figure 26.13. The frequencies of each failure cause are plotted independent of time. Based on Figure 26.13, one can conclude that cause A is the highest ranking cause while causes B,C and D are all equal contributors, and cause E is the lowest ranked cause in terms of counts. However, one can see that the Pareto chart has no time element, *i.e.*, one cannot tell which causes are current threats and which have been remediated. Yet this chart is one of the most popular representations in the industry. Sometimes stacked bar charts are used to divide the failure causes between multiple time periods, *i.e.*, a bar of one color representing time period one and a bar on top of a second color representing time period two. Use of these charts should be avoided due to their high ink-to-information ratio [20]. One can plot the failure causes as a function of time (age or calendar) to ascertain the evolution of failure mechanisms as a function of time.

Figure 26.14 shows the same plot as a function of calendar time, and it is quite revealing. One can see that even though cause A is only slightly higher than the other causes in Figure 26.13, its effect is

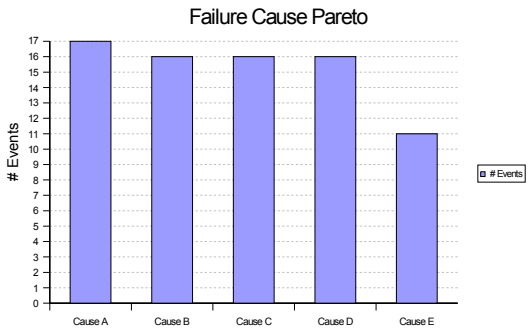


Figure 26.13. Example Pareto chart showing failure causes

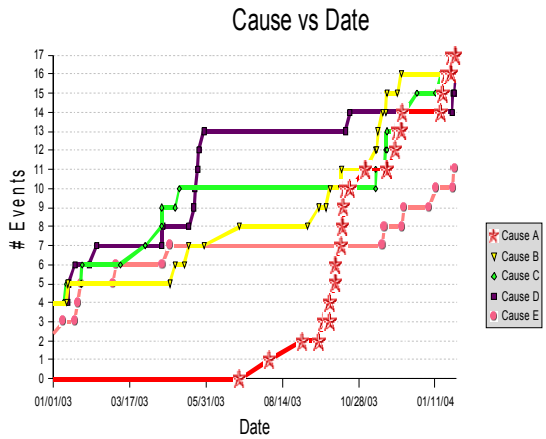


Figure 26.14. Failure causes *versus* date

dramatic when viewed in calendar time. It was non-existent for a while but became prevalent around September, with an extremely increasing trend. Even though Figure 26.13 showed that causes B,C and D were all equal contributors, their contributions in time are clearly not equivalent. Cause E was shown as the lowest ranked cause but we can see in Figure 26.14 that even though it has been dormant for a long time, there have been a rash of cause E events in very recent times, a situation that needs to be addressed immediately.

In Figure 26.14 the causes are plotted simply as counts. One can definitely plot MCFs as a function of age or calendar for each of the causes and normalize them by the machines at risk. One can easily imagine an MCF of all events with MCFs

for individual causes plotted along with it to show the contribution of each cause to the overall MCF at various points in time. This leads to one of the most useful aspects of MCFs which is the ability to compare one effect against another in a consistent fashion, *i.e.*, normalized and across time.

26.7 MCF Comparisons

26.7.1 Comparison by Location, Vintage or Application

Comparing one population with another in terms of reliability is a popular problem of interest in the industry. The company is interested in the performance of a particular server platform across all customers in a particular market segment, *e.g.*, finance, telecommunications, *etc*, to see if there are differences between customers. Customers are interested in comparing a population of machines in datacenter X with their machines in datacenter Y to see if there are differences in operating procedures between the two datacenters. Engineers might be interested in comparing machines running high performance technical computing with machines running online transaction processing to see if the effect of applications is something that needs to be considered in designs. Manufacturing might be interested in comparing machines manufactured in a particular year with machines manufactured in the following year to see if there are tangible improvements in reliability. The standard approach in the industry has been to calculate the MTBF of two populations and see if there is a significant difference. This approach is flawed because of inherent issues with the MTBF metric. The populations at multiple sites will be of different ages and comparing summary statistics will obscure all time dependent effects similar to the Pareto charts described in the failure cause plots section. The MCF by virtue of being time dependent and normalized by the number of machines at risk at all points in time facilitates meaningful comparisons of two or more populations. Figure 26.15 compares populations of machines belonging to the same customer but located in different datacenters.

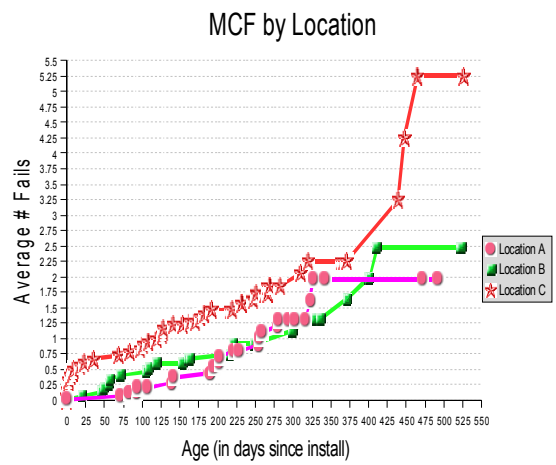


Figure 26.15. Comparison by location

One can see that location C has an MCF that has been consistently higher than the other locations. The difference between the locations starts to become visually apparent after about 300 days. Investigation into the procedures at location C revealed that personnel were not following correct procedures for avoiding electrostatic discharge while handling memory modules. This issue was rectified by policy and procedural changes and the reliability at this location improved. One can see that flattening of the MCF towards the end and becoming parallel with the MCFs for the other locations, *i.e.*, same slope or recurrence rate. Nelson provides procedures for assessing statistically significant difference between two MCFs [3]. However, procedures for comparing the differences of MCFs over the entire range and simultaneously comparing multiple MCFs are still topics of active research. Also, an approach to directly compare recurrence rates would be a quite useful notion and is also currently being researched. In most practical situations, a visual comparison is enough to initiate an investigation into the causes of differences between multiple platforms. It is easier to convince a lay person using visual significance than statistical significance, and a reliability engineer should err on the side of doing more root cause analysis (subject to resource constraints).

26.7.2 Handling Left Censored Data

Left censoring occurs when information on machines is not available before a certain age. Computers and storage equipment are installed at various times in a datacenter as part of the IT infrastructure. Often reliability data collection begins as an afterthought or possibly with the initiation of a service contract. Consequently, proper data is available only after a particular date. Due to the amount of missing information in the earlier ages, it would be difficult to compare MCFs because we do not know how many failures have occurred before we started collecting data. One way to deal with that is to do a parametric fit to the MCF, *e.g.*, linear or power law. We can then determine where the curve intersects the origin and use that intercept value as an estimate for the number of failures at the beginning of the measurement window. We can therefore create adjusted MCF curves as shown in Figure 26.16.

Alternatively, in this situation it would be advantageous to compare recurrence rates as a function of time instead of expected number of failures. This way we directly compare the rates in one time window with the rates in another time window to get an idea. With this we can avoid the estimation of the initial number of failures at the beginning of the time window; however, the rates being compared are in different time windows. This idea is shown in Figure 26.17. Machines manufactured in year XXXX appear to have the highest rate of failures. Year WWWW had small

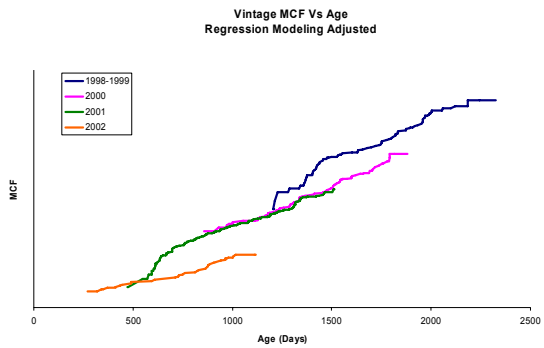


Figure 26.16. Adjusted MCF curve to account for window truncation

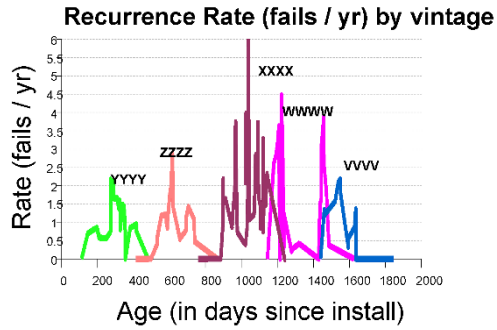


Figure 26.17. Comparison of recurrence rates *versus* age by vintage

spikes in the rate due to clustering of failures but otherwise has enjoyed long periods of low rates of failure. There appears to be no difference among years VVVV, YYYY and ZZZZ.

There does not appear to be a statistically rigorous procedure to assess significant difference between two recurrence rate curves. Visual interpretation has proved to be sufficient in practical experience.

One of the disadvantages of using MCF *versus* age is that the population at risk can fluctuate tremendously depending on the ages at which left and right censoring occurred and it can make interpretation quite difficult. It can be difficult to say with reasonable precision what the expected number of failures for a new machine entering the datacenter is going to be. Since computer systems are quite often subject to calendar time effects rather than age effects, we can look at the data in terms of date. By looking at the data in terms of date and not age we gain precision (sample size) in the later (recent) dates compared to the earlier dates. Hence the recurrence rate as a function of date can be used to state what the expected number of failures for a new machine entering the datacenter would be.

In Figure 26.18, we can see that the calendar time functions for all the manufacturing vintages begin on the same date because of left censoring. The difference between the vintages is clear. The newer vintages show significant reliability improvements over the older vintages. One can also take the slopes of these curves and plot the recurrence rates to compare the different vintages.

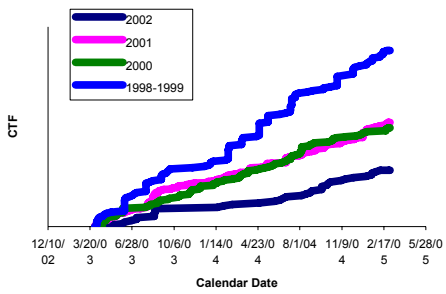


Figure 26.18. MCF *versus* calendar date by manufacturing vintage

Clearly these are superior approaches to simply comparing MTBFs.

26.8 MCF Extensions

All parametric methods apply primarily to "counts" data, *i.e.*, they provide an estimate of the expected number of events as they are generalizations of counting processes. However, the MCF is far more flexible than just counts data. It can be used in availability analysis by accumulating average downtime instead of just average number of outage events. MCFs can be used to track service cost per machine in the form of mean cumulative cost function. It can be used to track any continuous cumulative history (in addition to counts) such as energy output from plants, amount of radiation dosage in astronauts, *etc*. In this section we show two such applications that are quite useful for computer systems, namely downtime for availability and service cost.

26.8.1 The Mean Cumulative Downtime Function

Availability is of paramount importance to computing and networking organizations because of the enormous costs of downtime to business. Such customers often require service level agreements on the amount of downtime they can expect per year, and the vendor has to pay a penalty for exceeding the agreed upon guarantees. However, inherent availability defined as MTTF/(MTTF+MTTR) is merely a summary statistic. It is subject all the difficulties of interpretation described in the section on the dangers of MTBFs. The availability metric does not distinguish between a 50 minute outage and ten outages of 5 minutes each. However the two situations can be quite different for different customers. One customer might be able to live with numerous small outages while some customers prefer one single outage. For such situations it is useful to plot the cumulative downtime for individual machines and get a cumulative average downtime per machine as a function of time. The calculation would proceed identical to Figure 26.9 except that the integer counts of failure are replaced by the actual downtime due to the event. Since availability is a function of both the number of outage events and the duration of outage events, one needs to plot the mean cumulative downtime function as well as the MCF based on just outage events. Sometimes the cumulative downtime may be small but the number of outage events may be excessive, and this situation can be expensive because of the amount of failure analysis overhead that goes into understanding each outage. Contracts are often drawn on both the number of outage events as well as the amount of downtime. Figure 26.19 shows an example mean cumulative downtime function.

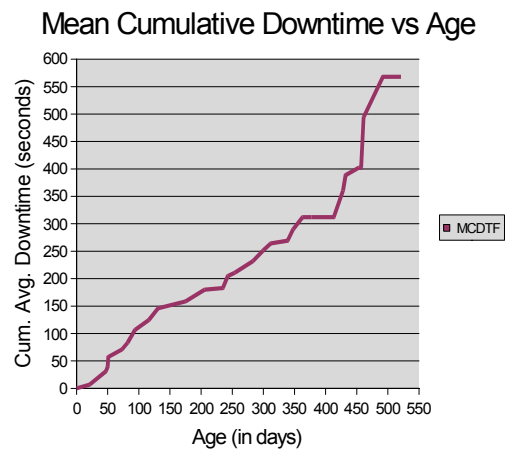


Figure 26.19. Mean cumulative downtime function

26.8.2 Mean Cumulative Cost Function

This application is quite similar to the downtime analysis mentioned in the previous section. This cost analysis could be performed by the vendor on service costs to understand one's cost structure, warranty program, pricing of subscription programs for support services, *etc*. The cost function could also be created by the customer to track the impact of failures on the business. The notion of downtime and the outage events can be combined to just one plot by looking at cost. The cost would be lost revenue due to loss of functionality plus all administrative costs involved in dealing with each outage. So in the situation of lots of outages with small amounts of downtime, the administrative costs will become noticeable. Again the calculation of the mean cumulative cost function would be similar to one of calculating an MCF for failure events except costs are used instead of counts of failures. These mean cumulative cost and downtime functions enjoy all the properties of an MCF in terms of being efficient, non-parametric estimators, and identifying trends in the quantity of interest.

In Figure 26.20, we have an example of a mean cumulative cost function for a population of machines in a datacenter. Similar to failure cause plots we can plot the breakdown of the total costs into their constituent costs, *i.e.*, cost of the event in terms of repair and root cause analysis costs and downtime costs in terms of lost revenue. This breakdown can provide invaluable information in understanding total cost of ownership as a function of time and assist in pricing service contracts and warranty offerings.

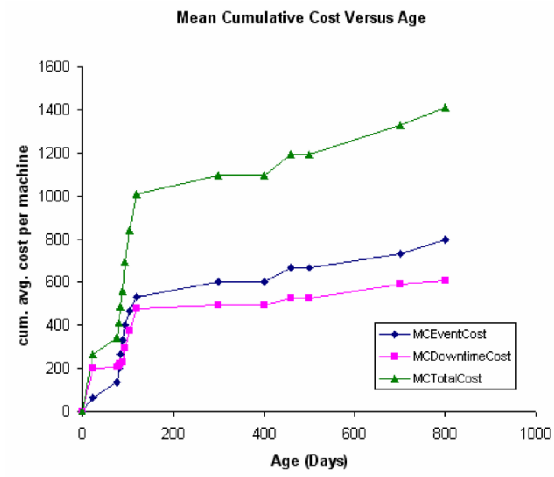


Figure 26.20. Mean cumulative cost function

26.9 Conclusions

This chapter discusses the analysis of repairable systems from the industry perspective. Parametric methods have been the mainstay of repairable systems research. However, they have not captured the attention of the industry because of the complexities of analysis as well as the difficulty in explaining the techniques to management and customers. These limitations are reasons why the industry persists on using summary statistics like MTBF. This chapter addresses the dangers of using summary statistics like MTBF and the important distinction between analyzing the data as a non-repairable or repairable system.

The analysis of repairable systems does not have to be difficult. Simple graphical techniques can provide excellent estimates of the expected number of failures without resorting to solving complex equations or justifying distributional assumptions. MCFs as a function of calendar time can provide important clues to non age related effects for certain classes of repairable systems. MCFs and recurrence rates are quite versatile because of their extensions to downtime and cost, while parametric methods mostly handle counts type data. The approaches outlined in this chapter have been successfully implemented at Sun Microsystems and also have found ready acceptance among people of varied backgrounds, from support technicians and executive management to statisticians and reliability engineers.

Non-parametric methods provide a happy medium between summary statistics and complex stochastic processes and are quite popular for non-repairable systems due to the huge survival analysis community in medical and biostatistics arena. However, the use of such techniques in repairable systems/recurrence analysis has not been as prolific as in survival analysis. There are still

several active areas of research in the use of MCFs, which will only serve to enhance the popularity of these techniques that are rapidly gaining acceptance within the industry.

References

[1] Ascher H. A set of numbers is NOT a data-set. IEEE Trans. on Reliability 1999; 48(2): 135–140.

[2] Usher J. Case study: Reliability models and misconceptions. Quality Engineering 1993; 6(2):261–271.

[3] Nelson W. Recurrence events data analysis for product repairs, disease recurrences and other applications. ASA-SIAM Series in Statistics and Applied Probability 2003.

[4] Tobias PA, Trindade DC. Applied reliability, 2nd edition, Chapman and Hall/CRC, Boca Raton, FL, 1995.

[5] Meeker WQ, Escobar LA. Statistical methods for reliability data. Wiley Interscience, New York, 1998.

[6] Trindade DC, Nathan S. Simple plots for monitoring the field reliability of repairable systems, Proceedings of the Annual Reliability and Maintainability Symposium (RAMS), Alexandria, Virginia; Jan. 24–27, 2005.

[7] Nelson W. Graphical analysis of recurrent events data. Joint Statistical Meetings, http://amstat.org/meetings, American Statistical Association, Minneapolis 2005.

[8] Ascher H, Feingold H. Repairable systems reliability: Modeling, inference, misconceptions and their causes. Marcel Dekker, New York 1984.

[9] Crow LH. Reliability analysis of complex repairable systems. In: Proschan F, Serfling RJ, editors. Reliability and biometry. SIAM, Philadelphia, 1974; 379–410.

[10] Crow LH. Evaluating the reliability of repairable systems. Proceedings of the Annual Reliability and Maintainability Symposium (RAMS) 1990; 275–279.

[11] Kijima M. Some results for repairable systems with general repair. Journal of Applied Probability 1989; 26:89–102.

[12] Kijima M, Sumita, N. A useful generalization of renewal theory: counting process governed by non-negative Markovian increments. Journal of Applied Probability 1986; 23:71–88.

[13] Kaminskiy M, Krivtsov V. A Monte Carlo approach to repairable system reliability analysis. Probabilistic Safety Assessment and Management, New York: Springer, 1998; 1063–1068.

[14] Mettas A, Zhao W. Modeling and analysis of repairable systems with general repair. Proceedings of the Annual Reliability and Maintainability Symposium (RAMS); Alexandria, Virginia; Jan. 24–27, 2005.

[15] Drenick RF. The failure law of complex equipment. Journal of the Society of Industrial and Applied Mathematics 1960; 8: 680–690.

[16] Zuo J, Meeker W, Wu H. Analysis of window-observation recurrence data. Joint Statistical Meeting, http://amstat.org/meetings, American Statistical Association, Minneapolis 2005.

[17] Glosup J. Detecting multiple populations within a collection of repairable systems. Joint Statistical Meeting, http://amstat.org/meetings, American Statistical Association, Toronto 2004.

[18] Heavlin W. Identification of anomalous machines using CMH statistic. Sun Microsystems Internal Report 2005.

[19] Trindade DC. An APL program to numerically differentiate data. IBM TR Report 1975; Jan. 12 (19.0361).

[20] Tufte ER. The visual display of quantitative information. Graphics Press, Cheshire, CT 2001.

27

Reliability Degradation of Mechanical Components and Systems

Liyang Xie, and Zheng Wang

Northeastern University, Shenyang, China

Abstract: This chapter focuses on time-dependent reliability assessment approaches. Two new methods are presented to depict the change of reliability with the increase of operation time or the number of applied load cycles. In the first part of this chapter, we present a time-dependent load-strength interference analysis method that models reliability degradation caused by a randomly repeated load. By describing the loading history as the Poisson stochastic process, time-dependent reliability models are developed, and the characteristics of the failure rate curve with respect to different component strength degradation patterns is discussed. In the second part, we present a residual life distribution based method by which we model the change of the residual fatigue life distribution with the number of load cycles. Based on the experimental study of residual fatigue life distributions of two metallic materials, a model is developed to calculate the parameters of residual fatigue life distribution under variable amplitude load history, by which residual life distribution parameters are determined with the known applied load history. Furthermore, a recursive equation is introduced to predict the probability of fatigue failure under variable amplitude load histories.

27.1 Introduction

Mechanical components or systems age in service, and their reliability decreases over service time or load history. The latter might result from strength degradation due to damage accumulation or simply from the multiple application effect of randomly imposed loads. To schedule a maintenance program reasonably, especially in the framework of reliability centered maintenance, the operation experience-dependent reliability of equipment in service must be correctly described and accurately predicted.

In contrast with the relatively mature reliability theory for electronic element and equipment, there are still difficulties with reliability design, reliability manufacturing, reliability assessment, and reliability management of mechanical systems. The techniques developed for the evaluation of electronic elements or systems are not always applicable to mechanical counterparts [1–2]. For instance, exponential distribution has been widely applied to electronic element or equipment life, but it is a serious drawback to the whole concept of RCM because the exponential distribution cannot be used to model items that fail due to wear, fatigue, corrosion or any other mode that is related to age [3].

Besides the more complicated failure mode and/or mechanism of mechanical components or systems compared with electronic element or equipment, more complex loading conditions, a

stronger dependence among different failure mechanisms or different component failures, more serious strength degradation and a more evident reliability decrease during operation also result in the complexity of the reliability problem of mechanical components and systems.

A great amount of research work has been done on reliability, availability and maintainability. For instance, Crocker [3] proposed a new approach for RCM to use the concepts of soft life and hard life to optimize the total maintenance cost. Xu *et al.* [4] developed a new class of computational methods, referred to as decomposition methods, to predict failure probability of structural and mechanical systems subject to random loads, material properties, and geometry. The idea of decomposition in multivariate functions originally developed by the authors for statistical moment analysis has been extended for reliability analysis. The methods involve a novel function decomposition that facilitates univariate and bivariate approximations of a general multivariate function, response surface generation of univariate and bivariate functions, and Monte Carlo simulation, and can solve both component and system reliability problems.

The necessity of time-variant reliability assessment of deteriorating structures is becoming increasingly recognized. Petryna [5] proposed an assessment strategy for structural reliability under fatigue conditions. It was illustrated that reliability assessment of structures under fatigue conditions is a highly complicated problem, which implies interaction of different scientific fields such as damage and continuum mechanics, non-linear structural analysis, and probabilistic reliability theory. In an earlier paper, Murty *et al.* [6] proposed an approach to describe residual fatigue strength distribution by which component fatigue reliability can be evaluated as a function of the number of load cycles.

Generally speaking, the conventional reliability model of component reliability calculation, *i.e.,* the well known load-strength interference model [7–12] underlies the hypothesis that the load is static or applied only once to the component during its life time. In other words, it cannot reflect the effect of the load history on reliability. For most mechanical systems, the operating loads subjected to components are dynamic or randomly repeated. In such a situation, the failure probability of a component or system will increase with the loading history, and a time-dependent reliability model is necessary.

27.2 Reliability Degradation Under Randomly Repeated Loading

FORM (first order reliability method) or SORM (second order reliability method) are widely used in reliability engineering. However, these methods cannot deal with time dependent random variables [13]. When fatigue reliability analysis has to consider certain time-dependent variables, it is difficult to incorporate discrete time dependent variables in FORM. Alternatively, the Monte Carlo method is applied when no case specific model can be used. The Monte Carlo method, although theoretically a universal approach, usually entails great computation effort, besides having other limitations.

A new time-dependent component reliability model is presented herein and the relationship between reliability/failure rate and service time (or the number of load cycles) is also described. First we analyze the failure process of a component subjected to randomly repeated load and the cumulative distribution function or the probability density function of the equivalent load. Based on the homogeneous Poisson process of the number of load cycles, time-dependent reliability models are derived with and without strength degradation, respectively, according to the load-strength interference relationship.

27.2.1 The Conventional Component Reliability Model

The load-strength interference model (as shown in Figure 27.1) is widely applied in the calculation and analysis of component reliability. According to this model, reliability is defined as the probability that the load does not exceed the strength. Here, both the load and the strength are general in meaning. Load can be any factors leading to

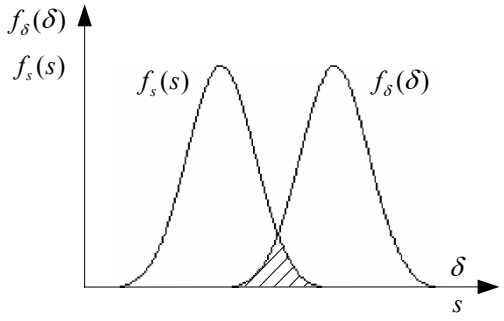


Figure 27.1. Load-strength interference relationship

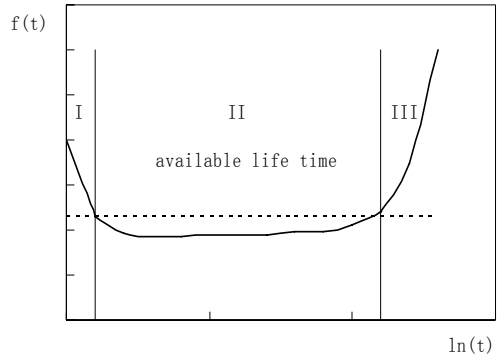


Figure 27.2. Typical failure rate curve (bathtub curve)

failure, such as mechanical loads, temperature, humidity or a corrosion environment, *etc*., and strength is the respective resistance capability to the load.

The load-strength interference model can be used to calculate component reliability when the probability distribution of load and that of strength are known. When the probability density function of strength is $f_\delta(\delta)$ and the probability density function of load is $f_s(s)$, the reliability of a component can be expressed as

$$\begin{aligned} R &= \int_{-\infty}^{+\infty} f_s(s) \int_{s}^{+\infty} f_\delta(\delta) d\delta ds \\ &= \int_{-\infty}^{+\infty} f_\delta(\delta) \int_{-\infty}^{\delta} f_s(s) ds d\delta \end{aligned} \tag{27.1}$$

Equation (27.1) is the general expression of the reliability model of a component with a single failure mode. Obviously, it is only reasonable for the situation that the load acts only once on the component during its service life. It cannot describe the relationship between reliability and time or the load action number when the load is not static.

Considering the performance of a product over its service life, the failure rate curve (*i.e.*, the bathtub curve) is also widely used to describe reliability-related behavior. A typical failure rate curve consists of three stages as shown in Figure 27.2. It is conventionally explained that the infant mortality phase (stage I) demonstrates a subpopulation dominated by quality-control defects due to poor workmanship, contamination, out-of-specification incoming parts and materials, and other substandard manufacturing practices [14]. It is also usually thought that mechanical systems may not appear to have an infant mortality period [14]. We will show below that the failure rate declination at the beginning of product service life is determined by both the strength distribution and the load distribution. Supposing that there is no strength degradation during the service life, a product will survive all the successive loads less than the highest load it has once resisted. Meanwhile, the likelihood that a higher load appears will become less and less with the increase of the number of the applied load cycles.

Concerning the situation of multiple actions of the random load, the component reliability can be modeled as [15]

$$R^{(m)} = \int_{-\infty}^{+\infty} f_\delta(\delta) \left(\int_{-\infty}^{\delta} f_s(s) ds \right)^m d\delta$$

or in a simpler form

$$R^{(m)} = R^m$$

based on the opinion that the failures caused by the individual loads applied to the component are independent of each other [15].

$R^{(m)}$ denotes the component reliability after m times of load action.

27.2.2 The Equivalent Load and Its Probability Distribution

The load acting on a mechanical component is normally stochastically repeated during operation. In the following, the cumulative distribution

function and probability distribution function of the equivalent load are defined by means of the order statistic of the load samples. Thereby, reliability models of components and systems in the situation of a stochastically repeated load are developed.

When component strength does not degrade, or the degradation is not evident, the event that a component survives m times of loading is equivalent to the event that the component does not fail under the maximum load of the m load samples. Thus, component reliability can be calculated through the interference relationship between strength and the maximum load among the m times of loading. Thus, the maximum load will also be called the equivalent load in the latter part of this chapter. Statistically, the maximum load is the maximum order statistic of the m load samples and is determined by the sample set $(s_1, s_2, \cdots, s_m)$ [16].

Let the cumulative distribution function and probability density function of a random variable x be denoted by $F_x(x)$ and $f_x(x)$, respectively, and the maximum of m samples be denoted by X_m. According to the order statistics theory, the cumulative distribution function of the maximum is

$$F_{X_m}(x) = \left[F_s(x)\right]^m \tag{27.2}$$

The probability density function of the maximum is

$$f_{X_m}(x) = m\left[F_s(x)\right]^{m-1} f_s(x) \tag{27.3}$$

If x denotes load, then the maximum X_m will be the equivalent load. Figure 27.3 shows the probability distribution of the load and the probability distributions of the equivalent loads of 10, 100 and 500 times the stochastic load, respectively. The stochastic load follows the normal distribution with mean $\mu_s = 50\text{MPa}$ and standard deviation $\sigma_s = 15\text{MPa}$.

It can be concluded that the mean of the equivalent load increases and the dispersion of the equivalent load decreases as the load sample sizes increase. When the strength distribution function $f_\delta(\delta)$ is known, the reliability $R^{(m)}$ of a component after m times of stochastic loading can be derived with the load-strength interference theory as

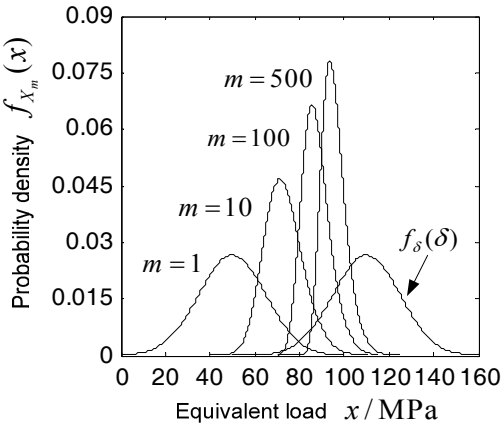


Figure 27.3. Probability distributions of equivalent loads and strength

$$\begin{aligned} R^{(m)} &= P(\delta > X_m) \\ &= \int_{-\infty}^{+\infty} f_\delta(\delta) \int_{-\infty}^{\delta} f_{X_m}(x)\,dx\,d\delta \\ &= \int_{-\infty}^{+\infty} f_\delta(\delta) \int_{-\infty}^{\delta} m\left[F_s(x)\right]^{m-1} f_s(x)\,dx\,d\delta \end{aligned} \tag{27.4}$$

Where, $f_{X_m}(x)$ is the probability density function of the equivalent load X_m, $f_\delta(\delta)$ is the probability density function of component strength, $F_s(x)$ is the cumulative distribution function of the stochastic load, and m is the times that the stochastic load is applied to the component. If the integration variable x is replaced with load s in (27.4), it can be rewritten as

$$R^{(m)} = \int_{-\infty}^{+\infty} f_\delta(\delta) \int_{-\infty}^{\delta} m\left[F_s(s)\right]^{m-1} f_s(s)\,ds\,d\delta \tag{27.5}$$

27.2.3 Time-dependent Reliability Model of Components

For most mechanical equipment and systems, the operation load during service can be described by a Poisson stochastic process [17, 18]. Let $M(t)$ denote the times of stochastic load subjected to a component in the time interval $(0,t)$. It is assumed to show the following characteristics:

(1) $M(0)=0$;

(2) For any $0<t_1<t_2<\cdots<t_m$, $M(t_1)$, $M(t_2)-M(t_1)$, …, $M(t_m)-M(t_{m-1})$ are independent of each other;

(3) The times of the load action depend only on the interval and not on the starting point, *i.e.*, $\forall s,t\geq 0,\ m\geq 0$,

$$P[M(s+t)-M(s)=m]=P[M(t)=m]$$

(4) For any $t>0$ and very small $\Delta t>0$,

$$\begin{cases}P[M(t+\Delta t)-M(t)=1]=\lambda\Delta t+o(\Delta t)\\ P[M(t+\Delta t)-M(t)\geq 2]=o(\Delta t)\end{cases}$$

Obviously, a loading process that satisfies the above conditions can be described by the homogeneous Poisson process with parameter λ and the probability of load acting m times ($M(t)=m$) over time t is

$$P\left[M(t)-M(0)=m\right]=\frac{(\lambda t)^m}{m!}e^{-\lambda t} \tag{27.6}$$

27.2.3.1 *Time-dependent Reliability Model Without Strength Degradation*

When strength does not degrade with the loading history, the component reliability at time t with load acting for m times can be calculated, according to (27.5) and (27.6), as:

$$\begin{aligned}R(m,t)&=P\left[M(s+t)-M(s)=m\right]\cdot R^{(m)}\\&=\frac{(\lambda t)^m}{m!}e^{-\lambda t}\int_{-\infty}^{+\infty}f_\delta(\delta)\\&\quad\int_{-\infty}^{\delta}m\left[F_s(s)\right]^{m-1}f_s(s)dsd\delta\end{aligned} \tag{27.7}$$

By means of the total probability formula, the reliability $R(t)$ of a component at time t is equal to

$$\begin{aligned}R(t)&=\sum_{m=0}^{+\infty}R(m,t)\\&=\sum_{m=0}^{+\infty}\frac{(\lambda t)^m}{m!}e^{-\lambda t}\int_{-\infty}^{+\infty}f_\delta(\delta)\\&\quad\int_{-\infty}^{\delta}m\left[F_s(s)\right]^{m-1}f_s(s)dsd\delta\end{aligned} \tag{27.8}$$

Using the Taylor expansion of the exponential function

$$e^x=1+\frac{x}{1!}+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots+\frac{x^m}{m!}+\cdots \tag{27.9}$$

Equation (27.8) can be simplified as

$$\begin{aligned}R(t)&=\int_{-\infty}^{+\infty}f_\delta(\delta)e^{-\lambda t}\sum_{m=0}^{\infty}\frac{(\lambda t)^m}{m!}\left[F_s(\delta)\right]^m d\delta\\&=\int_{-\infty}^{+\infty}f_\delta(\delta)e^{\left[F_s(\delta)-1\right]\lambda t}d\delta\end{aligned} \tag{27.10}$$

Equation (27.10) can be used to calculate the reliability of components without strength degradation. Further, the failure rate $h(t)$ can be derived as

$$\begin{aligned}h(t)&=\frac{f(t)}{R(t)}=-\frac{R'(t)}{R(t)}\\&=-\frac{\int_{-\infty}^{+\infty}f_\delta(\delta)\left[F_s(\delta)-1\right]\lambda e^{\left[F_s(\delta)-1\right]\lambda t}d\delta}{\int_{-\infty}^{+\infty}f_\delta(\delta)\lambda e^{\left[F_s(\delta)-1\right]\lambda t}d\delta}\end{aligned} \tag{27.11}$$

Let the parameter of the Poisson stochastic process λ be equal to 0.5 h^{-1}. The component strength follows the normal distribution with mean $\mu_\delta=600\mathrm{MPa}$ and standard deviation $\sigma_\delta=60\mathrm{MPa}$. The load follows the normal distribution with mean $\mu_s=400\mathrm{MPa}$ and standard deviation $\sigma_s=40\mathrm{MPa}$. The relationship between component reliability and time is shown in Figure

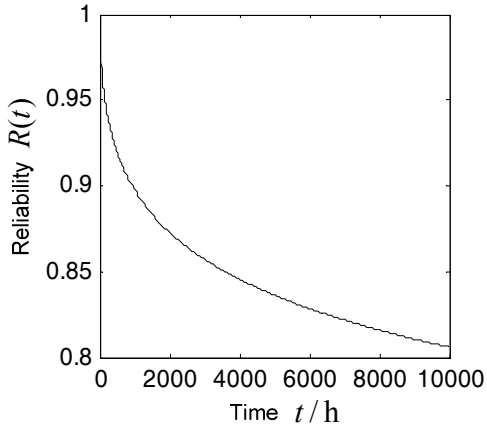


Figure 27.4. Relationship between reliability and time

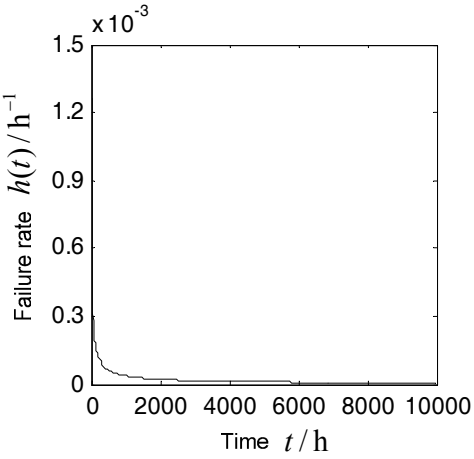


Figure 27.5. Failure rate curve

27.4, and the relationship between the component failure rate and time is shown in Figure 27.5.

It is shown that even if strength does not degrade, both the reliability and the failure rate decrease with time; the failure rate has the feature of the two former stages of a typical bathtub curve.

27.2.3.2 Time-dependent Reliability Model with Strength Degradation

When strength degrades with time or with the number of load actions, the effect of the strength degradation on reliability should be taken into account. In the following, a time-dependent component reliability model will be developed by means of the probability differential equation.

Assuming that the strength δ_t of a component at time t is a function of initial strength δ and time t, and the load appearing at time $t+\Delta t$ is independent with the load appearing at time t, the component failures are independent at time $t+\Delta t$ and time t. Based on the definition of the Poisson process, the probability that a load appears in the interval $(t,\ t+\Delta t)$ is $\lambda\Delta t$. If the reliability of the component at time t is $R(t)$, the reliability at time $t+\Delta t$ can be expressed as

$$\begin{aligned} &R(t+\Delta t)\\ &= R(t)P\left(\delta_\tau > s, \forall\tau\in[t,t+\Delta t]\right)\lambda\Delta t + R(t)\left(1-\lambda\Delta t\right)\\ &= R(t)+R(t)\lambda\Delta t\left[P\left(\delta_\tau > s, \forall\tau\in[t,t+\Delta t]\right)-1\right] \end{aligned} \tag{27.12}$$

According to the load-strength interference model, the above equation can be written as

$$\begin{aligned} R(t+\Delta t) &= R(t)+R(t)\lambda\Delta t\left[\int_{-\infty}^{\delta_\tau} f_s(s)ds - 1\right]\\ &= R(t)+R(t)\lambda\Delta t\left[F_s\left(\delta_\tau\right)-1\right] \end{aligned} \tag{27.13}$$

Note that the strength δ_t at time t is a function of the initial strength δ and time t, and

$$R(t+\Delta t)-R(t) = R(t)\lambda\Delta t\left[F_s(\delta,\tau)-1\right] \tag{27.14}$$

Dividing the items by Δt and letting $\Delta t\to 0$ and $\tau\to t$, (27.14) can be expressed as

$$\frac{dR(t)}{dt} = R(t)\lambda\left[F_s(\delta,t)-1\right] \tag{27.15}$$

Equation (27.15) is the differential equation of component reliability with strength degradation. Obviously,

$$\ln R(t) = \int_0^t \lambda\left[F_s(\delta,t)-1\right]dt \tag{27.16}$$

$$R(t) = e^{\int_0^t\left[F_s(\delta,t)-1\right]\lambda dt} \tag{27.17}$$

The above derivation is based on the precondition that the initial strength δ is deterministic. When the initial strength δ is a random variable with the probability density function $f_\delta(\delta)$, the time-dependent reliability model can be developed by means of the total probability formula for continuous variables,

$$R(t) = \int_{-\infty}^{+\infty} f_\delta(\delta)e^{\int_0^t\left[F_s(\delta,t)-1\right]\lambda\ dt}d\delta \tag{27.18}$$

It is easy to show that when the strength does not degrade (namely, $F_s(\delta,t)$ is independent of time t), (27.18) degenerates to (27.10).

Further, the component failure rate $h(t)$ can be derived as

$$\begin{aligned} h(t) &= \frac{f(t)}{R(t)} = -\frac{R'(t)}{R(t)}\\ &= -\frac{\int_{-\infty}^{+\infty} f_\delta(\delta)\left[F_s(\delta,t)-1\right]\lambda e^{\int_0^t\left[F_s(\delta,t)-1\right]\lambda dt}d\delta}{\int_{-\infty}^{+\infty} f_\delta(\delta)e^{\int_0^t\left[F_s(\delta,t)-1\right]\lambda dt}d\delta} \end{aligned} \tag{27.19}$$

Strength Degrades Exponentially

Assuming that the component strength degrades exponentially as $\delta_t = \delta \cdot e^{-0.00002\ t}$, when the parameter of the loading process (a Poisson stochastic process) λ equals $0.5\ \mathrm{h}^{-1}$, the component strength follows the normal distribution with mean $\mu_\delta = 600\mathrm{MPa}$ and standard deviation $\sigma_\delta = 60\mathrm{MPa}$, the load follows the normal distribution with mean $\mu_s = 400\mathrm{MPa}$ and standard deviation $\sigma_s = 40\mathrm{MPa}$. Figure 27.6 shows the relationship between component reliability and time and the relationship between the component failure rate and time is shown in Figure 27.7.

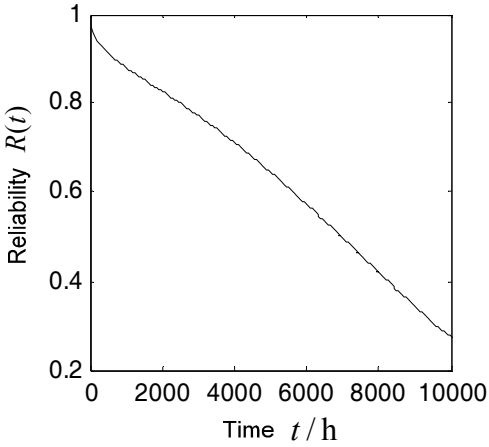


Figure 27.6. Relationship between reliability and time

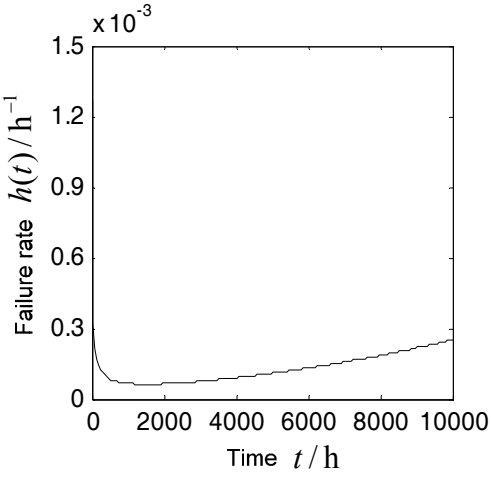


Figure 27.7. Failure rate curve

Strength Degrades Logarithmically

Assuming that the component strength degrades logarithmically as $\delta_t = \delta[1+\ln(1-0.0000125t)]$, when $\lambda = 0.5\ \mathrm{h}^{-1}$, the component strength follows the normal distribution with $\mu_\delta = 600\mathrm{MPa}$ and $\sigma_\delta = 60\mathrm{MPa}$, the load follows the normal distribution with $\mu_s = 400\mathrm{MPa}$ and $\sigma_s = 40\mathrm{MPa}$, the relationship between component reliability and time is shown in Figure 27.8, and the relationship between failure rate and time is shown in Figure 27.9.

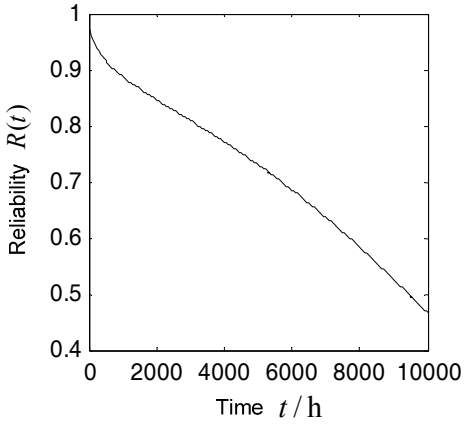


Figure 27.8. Relationship between reliability and time

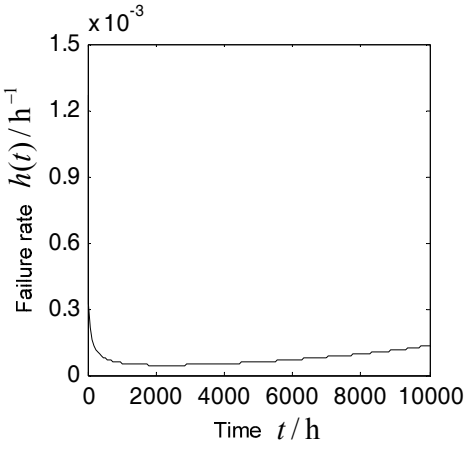


Figure 27.9. Failure rate curve

Strength Degrades Linearly

When the component strength degrades linearly, *e.g.*, $\delta_t = \delta(1-0.00002t)$, the Poisson process parameter $\lambda = 0.5\ \mathrm{h}^{-1}$, the component strength follows the normal distribution with $\mu_\delta = 600\mathrm{MPa}$ and $\sigma_\delta = 60\mathrm{MPa}$, the load follows the normal distribution with $\mu_s = 400\mathrm{MPa}$ and $\sigma_s = 40\mathrm{MPa}$. The relationship between component reliability and time, and the relationship between failure rate and time are shown in Figures 27.10 and 27.11, respectively.

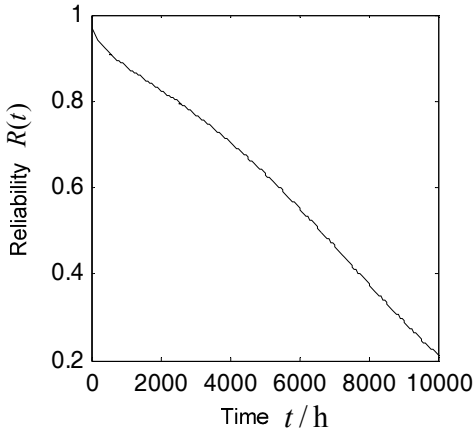


Figure 27.10. Relationship between reliability and time

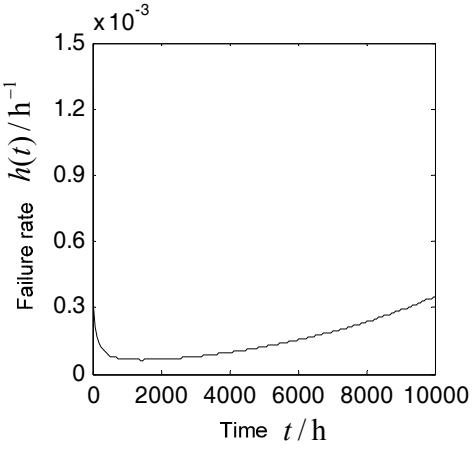


Figure 27.11. Failure rate curve

From Figures 27.6 through to Figure 27.11, it can be concluded that if the component strength degrades with time, the component reliability will decrease with time rapidly, while the component failure rate first decreases and then increases with time and shows the feature of the three stages of an entire bathtub curve.

27.2.4 The System Reliability Model

According to the system-level load-strength interference relationship [8], for the system composed of n independently identical distributed components, where the cumulative distribution function and the probability density function of the component strength are $F_\delta(\delta)$ and $f_\delta(\delta)$, respectively, and the load probability density function is $f_s(s)$. The respective reliability models for different systems are as follows.

Reliability of the series system

$$R_{seri} = \int_{-\infty}^{+\infty} \left(\int_{s}^{+\infty} f_\delta(\delta) d\delta \right)^n f_s(s) ds \quad (27.20)$$

Reliability of the parallel system

$$R_{para} = \int_{-\infty}^{+\infty} \left[1 - \left(\int_{-\infty}^{s} f_\delta(\delta) d\delta \right)^n \right] f_s(s) ds \quad (27.21)$$

Reliability of the k-out-of-n system

$$R_{k/n} = \int_{-\infty}^{+\infty} \sum_{i=k}^{n} C_n^i \left(\int_{s}^{+\infty} f_\delta(\delta) d\delta \right)^i \left(\int_{-\infty}^{s} f_\delta(\delta) d\delta \right)^{n-i} f_s(s) ds \quad (27.22)$$

27.2.5 The System Reliability Model Under Randomly Repeated Loads

If the strength does not degrade or the degradation can be neglected, the reliability that a system survives m times of randomly repeated loads is equal to the reliability that the system survives the maximum load of the m load samples.

Based on (27.20), (27.21) and (27.22), which are actually the reliability models under a single load action, the reliability models of different types of systems under multiple load actions can be developed for systems such as the series system for loads acting m times, the parallel system for loads acting m times, and the k-out-of-n system for loads acting m times. These systems are represented in (27.23), (27.24), and (27.25), respectively.

27.2.6 The Time-dependent System Reliability Model

Taking a series system as an example, when strength degradation can be neglected, according to (27.23) and (27.6), the reliability of a load acting m times at time t is given by (27.26).

Further, according to the total probability formula, the reliability model of the series system at time t is written as in (27.27).

$$\begin{aligned} R_{seri}^{(m)} &= \int_{-\infty}^{+\infty}\left(\int_{\mathrm{s}}^{+\infty} f_\delta(\delta)d\delta\right)^n m\left[F_s(s)\right]^{m-1} f_s(s)ds \\ &= \int_{-\infty}^{+\infty}\left[1-F_\delta(s)\right]^n m\left[F_s(s)\right]^{m-1} f_s(s)ds \end{aligned} \tag{27.23}$$

$$\begin{aligned} R_{para}^{(m)} &= \int_{-\infty}^{+\infty}\left[1-\left(\int_{-\infty}^{\mathrm{s}} f_\delta(\delta)d\delta\right)^n\right] m\left[F_s(s)\right]^{m-1} f_s(s)ds \\ &= \int_{-\infty}^{+\infty}\left\{1-\left[F_\delta(\delta)\right]^n\right\} m\left[F_s(s)\right]^{m-1} f_s(s)ds \end{aligned} \tag{27.24}$$

$$\begin{aligned} R_{k/n}^{(m)} &= \int_{-\infty}^{+\infty}\left(\sum_{i=k}^{n} C_n^{\,i}\left(\int_{s}^{+\infty} f_\delta(\delta)d\delta\right)^i \left(\int_{-\infty}^{\mathrm{s}} f_\delta(\delta)d\delta\right)^{n-i}\right) m\left[F_s(s)\right]^{m-1} f_s(s)ds \\ &= \int_{-\infty}^{+\infty}\left\{\sum_{i=k}^{n} C_n^{\,i}\left[1-F_\delta(s)\right]^i\left[F_\delta(s)\right]^{n-i}\right\} m\left[F_s(s)\right]^{m-1} f_s(s)ds \end{aligned} \tag{27.25}$$

$$\begin{aligned} R_{seri}(m,t) &= P\left[N(s+t)-N(s)=m\right] R_{seri}^{(m)} \\ &= \frac{(\lambda t)^m}{m!} e^{-\lambda t}\int_{-\infty}^{+\infty}\left[1-F_\delta(s)\right]^n m\left[F_s(s)\right]^{m-1} f_s(s)ds \end{aligned} \tag{27.26}$$

$$\begin{aligned} R_{\mathrm{seri}}(t) &= \sum_{m=0}^{+\infty} R_{\mathrm{seri}}(m,t) = \sum_{m=0}^{+\infty}\frac{(\lambda t)^m}{m!} e^{-\lambda t}\int_{-\infty}^{+\infty}\left[1-F_\delta(s)\right]^n m\left[F_s(s)\right]^{m-1} f_s(s)ds \\ &= \sum_{m=0}^{+\infty}\frac{(\lambda t)^m}{m!} e^{-\lambda t}\int_{-\infty}^{+\infty}\left[1-F_\delta(s)\right]^n d\left[F_s(s)\right]^m \\ &= \sum_{m=0}^{+\infty}\frac{(\lambda t)^m}{m!} e^{-\lambda t}\int_{-\infty}^{+\infty} n\left[1-F_\delta(s)\right]^{n-1}\left[F_s(s)\right]^m f_\delta(s)ds \\ &= \int_{-\infty}^{+\infty} n\left[1-F_\delta(s)\right]^{n-1} e^{-\lambda t}\sum_{m=0}^{+\infty}\frac{(\lambda t)^m}{m!}\left[F_s(s)\right]^m f_\delta(s)ds \end{aligned} \tag{27.27}$$

$$R_{\mathrm{seri}}(t) = \int_{-\infty}^{+\infty} e^{\left[F_s(s)-1\right]\lambda t} n\left[1-F_\delta(s)\right]^{n-1} f_\delta(s)ds \tag{27.28}$$

$$R_{para}(t) = \int_{-\infty}^{+\infty} e^{\left[F_s(s)-1\right]\lambda t} n\left[F_\delta(s)\right]^{n-1} f_\delta(s)ds \tag{27.29}$$

$$R_{k/n}(t) = \int_{-\infty}^{+\infty} e^{\left[F_s(s)-1\right]\lambda t}\left\{\sum_{i=k}^{n} C_n^{\,i}\left[1-F_\delta(s)\right]^{i-1}\left[F_\delta(s)\right]^{n-i-1}\left(i+nF_\delta(s)-n\right)\right\} f_\delta(s)ds \tag{27.30}$$

Using the Taylor expansion of an exponential function, the above equation can be simplified as (27.28). Similarly, the time-dependent reliability models of parallel system and *k*-out-of-*n* redundant system can be developed and are represented as in (27.29) and (27.30), respectively.

Taking the series system with three identical components, the parallel system with three identical components and the 2-out-of-3 system as examples, when the Poisson process parameter λ is $0.5\,\mathrm{h}^{-1}$, the component strength follows the normal distribution with mean $\mu_\delta = 600\mathrm{MPa}$ and standard $\sigma_\delta = 60\mathrm{MPa}$, the stress follows the normal distribution with mean $\mu_s = 400\mathrm{MPa}$ and standard $\sigma_s = 50\mathrm{MPa}$. The relationship between system reliability and time is shown in Figure 27.12. It can be concluded that the reliability of the series system decreases the fastest, the reliability of the parallel system decreases the most slowly and the reliability curve of the *k*-out-of-*n* system lies between those of the series system and the parallel system.

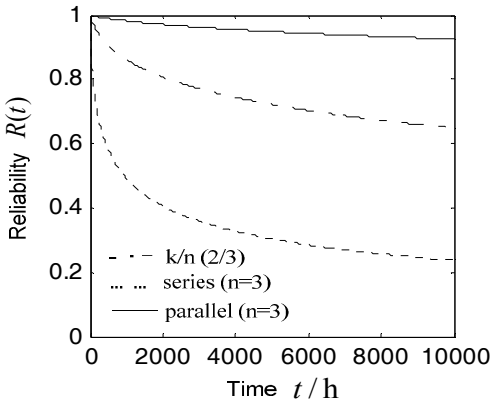


Figure 27.12. The relationship between system reliability and time

27.3 Residual Fatigue Life Distribution and Load Cycle-dependent Reliability Calculations

Stress-strength interference, or load cycle-fatigue life interference, is the most widely used concept in reliability analysis [19–31]. For a constant amplitude cyclic load, the interference model can be used directly to predict failure probability. For complex loading conditions, more comprehensive studies on probabilistic characteristics of fatigue failure can be found in many references [25–39], too. For instance, Kopnov [30] and Tanaka [31] studied the residual fatigue life distribution under both the constant amplitude cyclic loading condition and the two-stage loading condition, Bahring *et al.* [32] and Choukairi *et al.* [33] studied the impact of load changing on lifetime distributions, Wu *et al.* [34] developed a computer simulation approach, which was further developed in [35] for fatigue reliability analysis, Gauri *et al.* [36] and Tang *et al.* [37] investigated the mean residual life of lifetime distributions and its association with failure rate, Camarinopoulos *et al.* [38] and Zuo *et al.* [39] carried out reliability evaluations of engineering structures and components.

27.3.1 Experimental Investigation of Residual Fatigue Life

In the situation of variable amplitude loading, the residual fatigue life distribution changes considerably during the loading process. Therefore, it is necessary to investigate the variation of residual life distribution for the purpose of fatigue reliability prediction. To inspect the changing tendency of residual fatigue life, tests were conducted on a rotated-bending fatigue test machine, using smooth specimens made of normalized 0.45% carbon steel (St-45) and hot rolled alloy steel (16 Mn), respectively. The results are shown in Tables 27.1 and 27.2, in which residual lives are the test records of the residual life at the second level stress σ_2 after n_1 cycles of the first level stress σ_1. When failure occurs at the first-level stress, the residual life is negative and is calculated by $N_{2p}^1 = (N_1 - n_1)\bar{N}_2 / \bar{N}_1$, where N_1 is the number of cycles to failure at the first-level stress, n_1 is the assigned cycle number for the first level stress.

Table 27.1. Fatigue test results of normalized 0.45% carbon steel

Stress level and loading sequence	Sample size	Cycles of the 1st-level stress	Original fatigue life for constant amplitude stress tests or residual life at 2nd-level stress for two-level stress tests (in 100 cycles)	Mean of original life or mean of residual life	Std. of original life or std. of residual life
366MPa	15	-	444,397,533,368,487,433,305,665,395,403,449, 638,344,431,462	45027	9917
331MPa	18	-	2063,1197,1168,1354,1282,1564,1508,1324, 1159,1724,1053,1364,2620,2556,799,906,1975, 1743	151422	52286
309MPa	16	-	6021,2910,7099,9355,6429,8790,6752,7236, 9042,9618,5893,5519,7047,7089,3274,3531	658944	209045
331→366	14	40300	381,250,303,271,469,444,183,315,402,223,429, 421,356,325	34086	8820
	14	80600	183,301,285,168,114,463,551,372,181,24,283, 160,526,-10	25865	17144
	16	120900	394,96,-9.9,-58.8,269,-93.3,-29.1,206,337,-18, 252,168,-84,71,146	16267	24130
331→309	14	40300	5186,1470,1817,4248,1990,2884,1899,2010, 2211,3332,2508,4566,2526	262866	133326
	13	80600	2601,1225,762,993,2751,1237,144,1277,558, 1063,1950,382,2107	146239	110727
	13	120900	1435,1133,59,421,944,628,-631,-1022,269,- 209, 1284,-1583	70773	94040

Table 27.2. Fatigue test results of the hot rolled alloy steel 16Mn

Stress level or loading sequence	Sample size	Cycles of the 1st-level stress	Original fatigue life for constant amplitude stress test or residual life at 2nd-level stress for two-level stress test (in 100 cycles)	Mean of original life or mean of residual life	Std. of original life or std. of residual life
394MPa	15	-	915,1382,1066,1444,712,1120,1422,916,1532, 903,1310,1350,919,1149,953	113893	25130
373MPa	15	-	2087,1817,2262,1788,1929,2113,1685, 1744,1646,2632,1764,1833,2312,1903, 2011	196720	27322
373→394	10	62500	461,384,702,516,544,653,922,788,757, 885	74700	20290
	10	95200	1029,698,192,552,588,781,1019,654,686,632	68310	23878
	10	146000	506,130,776,100,210,534,96,115,252, 488	23123	26722
394→373	10	26000	1177,1460,1103,1207,1708,1157,1511,842, 1304,1541	130100	25549
	10	44000	611,466,691,835,485,524,656,841,1117,898,	71130	20881
	10	75000	314,797,392,67,438,310,745,138,591,190	39820	24804

27.3.2 The Residual Life Distribution Model

Test results show that, for the residual fatigue life distribution in the condition of constant amplitude cyclic loading without the occurrence of fatigue failure, the standard deviation of the residual fatigue life remains unchanged. The only change in the fatigue life distribution parameters is that the mean life decreases from $\bar{N}$ to ($\bar{N}-n$), where n is the applied load cycle number (see Figure 27.13). After stress σ_1 acts a cycle number of n_1, the pdf (probability density function) of the residual life under the same stress changes from $f_1(N) \sim N(\bar{N}_1, s_1)$ to $f_{1p}^1(N) \sim N(\bar{N}_1 - n_1, s_1)$. Where, $f_i(N) \sim N(\bar{N}_i, s_i)$ stands for $f_i(N)$ being a normal pdf with mean $\bar{N}_i$ and standard deviation s_i.

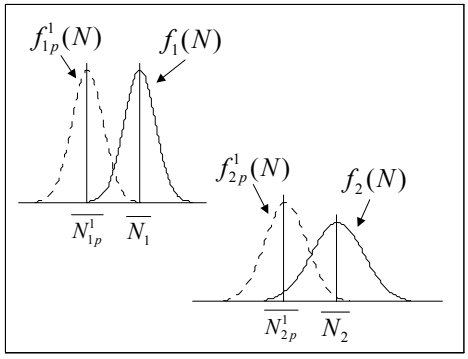
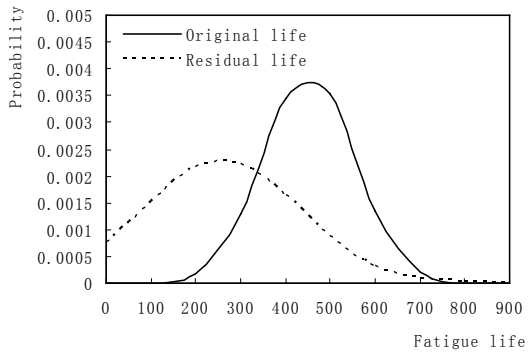
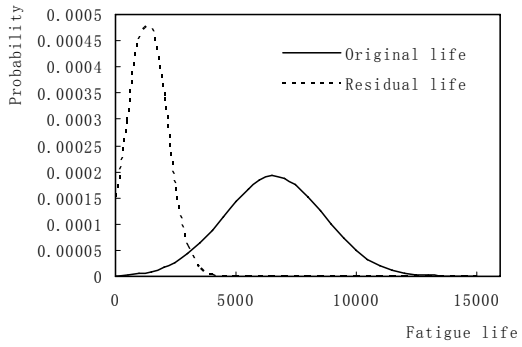


Figure 27.13. Illustration of (residual) life distributions

For the fatigue lives under variable amplitude load conditions, there are investigations (Bahring *et al.* [40] and Choukairi *et al.* [41]) to indicate that the change of residual life distribution is quite complicated. Nevertheless, for the two-level loading condition, an evident tendency can be found in the test results listed in the tables. In conditions of no failure occurrence, if low stress acts first, the standard deviation of the residual life under the subsequent high stress becomes greater, *i.e.,* the standard deviation of the residual life is greater than that of the original fatigue life under the pertinent high stress. If high stress acts first, the standard deviation of the residual life under the subsequent low stress becomes smaller, *i.e.,* the standard deviation of the residual life is less than that of the original life under the pertinent low constant stress. The greater the difference between the amplitudes of the high stress and the low stress is, the greater the change of the standard deviation of the residual life. All in all, the previously applied stress affects both the mean and the standard deviations of the residual fatigue life at subsequent stress (see Figs. 27.14–27.16).



(a) Distribution of the original life under 366 MPa and distribution of residual life under 366 MPa after 75711 cycles (half of the fatigue life under 331 MPa) of the lower stress (331 MPa) of St-45



(b) Distribution of the original life under 309 MPa and distribution of residual life under 309 MPa after 75711 cycles (half of the fatigue life under 331 MPa) of the higher stress (331 MPa) of St-45

Figure 27.14. Original life distribution and residual life distribution

It is shown that after stress σ_1 acts a cycle number n_1, the probability density function of the residual life under stress σ_2 changes from $f_2(N) \sim N(\bar{N}_2, s_2)$ to $f_{2p}^1(N) \sim N(\bar{N}_2 - n_{2d}, s_{2p}^1)$. n_{2d} is the equivalent cycle number of the stress σ_2 to that of the really applied n_1 cycles of σ_1, which is in the sense of mean life and can be estimated by the cumulative fatigue damage rule. The magnitude of the effect depends on the relative stress level of the first stress as well as its cycle number. According to regression analysis of the test data, a linear model can be developed to predict the residual life distribution parameters under two-level stress, and it will be extended to more complicated spectrum loading conditions, as well as variable amplitude loading histories.

Let $\bar{N}_i$ and s_i represent the mean and the standard deviation of the fatigue life under the i^{th} stress ($i = 1, 2$), respectively. The residual life distribution parameters ($\bar{N}_{2p}^1$, s_{2p}^1) under the second stress σ_2, after n_1 cycles of σ_1, can be expressed by the following equations:

$$\bar{N}_{2p}^1 = \bar{N}_2(1 - n_1 / \bar{N}_1) \tag{27.31}$$

$$s_{2p}^1 = s_2 + (s_1 - s_2) n_1 / \overline{N_1} \tag{27.32}$$

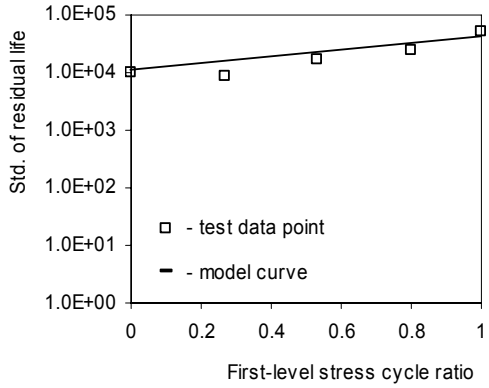
The pdf of the residual life is then:

$$f_{2p}^1(N) \sim N(\bar{N}_{2p}^1, s_{2p}^1) \tag{27.33}$$

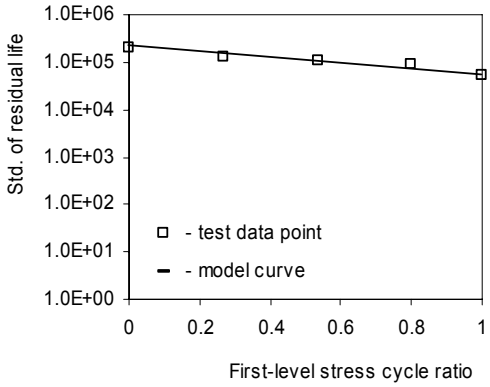
Obviously, (27.31) is equivalent to the well known Miner's rule, and (27.32) is an empirical model developed by the authors, which is taken as a primary approximation of the standard deviation of the residual life. This equation is developed mainly based on the test results listed in Tables 27.1 and 27.2, Figures 27.15 and 27.16 show the test results (denoted by boxes) and the mathematical model (solid line) of carbon steel St-45 and alloy steel 16-Mn. The abscissa stands for cycle ratio of the first level stress and the ordinate stands for the standard deviation of the residual life under the second level stress. Such a model can present the variation of the residual life distribution parameters under variable amplitude loads and can be applied, along with the other equation, to predict fatigue probability under variable amplitude loading.

If there is a third stress level or more, as in the condition of three-level stress or the complex loading spectrum, the residual life distribution parameters $(\bar{N}_{3p}^{12}, s_{3p}^{12})$ at the third stress σ_3, after n_1 cycles of σ_1 and n_2 cycles of σ_2, can be predicted as:

$$\bar{N}_{3p}^{12} = \bar{N}_{3p}^1 (1 - \frac{n_2}{\bar{N}_{2p}^1}) = \bar{N}_3 (1 - \frac{n_1}{\bar{N}_1} - \frac{n_2}{\bar{N}_2}) \tag{27.34}$$



(a) Std. of residual life at high stress



(b) Std. of residual life at low stress

Figure 27.15. Test result and model of std. of residual life of St-45

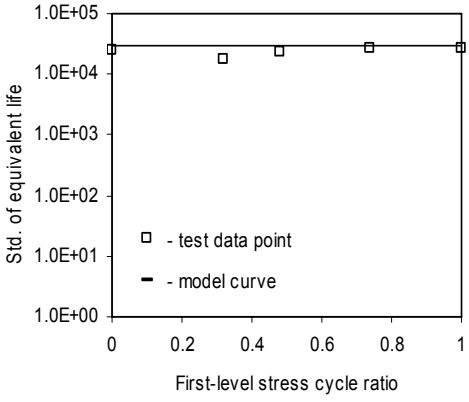
$$s_{3p}^{12} = s_{3p}^{1} + (s_{2p}^{1} - s_{3p}^{1})\frac{n_2}{\bar{N}_{2p}^{1}} = s_3 + (s_1 - s_3)n_1/\bar{N}_1 + (s_2 - s_3)\frac{n_2}{\bar{N}_2} \quad (27.35)$$

The pdf of the residual life is:

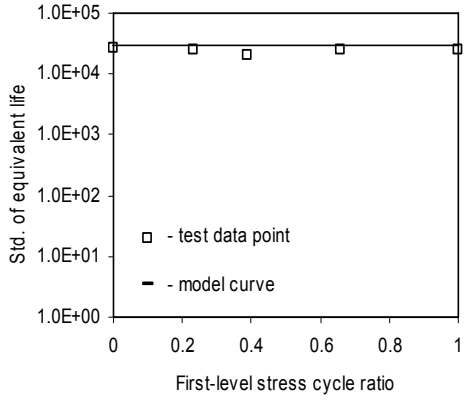
$$f_{3p}^{12}(N) \sim N(\bar{N}_{3p}^{12}, s_{3p}^{12}) \quad (27.36)$$

Similarly, for the i^{th} stress level in condition of multi-level stress or complex loading spectrum, the residual fatigue life distribution parameters $(\bar{N}_{ip}^{12...(i-1)}, s_{ip}^{12...(i-1)})$ can be predicted as:

$$\bar{N}_{ip}^{12...(i-1)} = \bar{N}_i\,(1 - \sum_{j=1}^{i-1} n_j/\bar{N}_j) \quad (27.37)$$



(a) Std. of residual life at the high stress



(b) Std of residual life at the low stress

Figure 27.16. Test result and model of std. of residual life of 16 Mn

$$s_{ip}^{12...(i-1)} = s_i + \sum_{j=1}^{i-1}[(s_j - s_i)(1 - \sum_{k=1}^{j-1}\frac{n_k}{\bar{N}_k})\frac{n_j}{\bar{N}_j}] \quad (27.38)$$

The *pdf* of the residual life is:

$$f_{ip}^{12...(i-1)}(N) \sim N(\bar{N}_{ip}^{12...(i-1)}, s_{ip}^{12...(i-1)}) \quad (27.39)$$

In the equations developed above, the cycle number of the applied stress is assumed to be a deterministic variable. When the cycles of the applied stress is a random variable, the mean of the random variable can be used to predict the residual life distribution parameters for the sake of simplification. The error caused by replacing the random variable with its mean is secondary in comparison with the change in the life distribution parameters caused by the cyclic loading.

When the applied load cycle number is greater than the minimum life, the failure probability is greater than zero (*i.e.,* $P_{fi}(t) > 0$). The *pdf* of the residual life represented in (27.39), (27.36) and (27.33) should be revised as:

$$f_{ipR}^{12...(i-1)}(N) = f_{ip}^{12...(i-1)}/(1 - P_{fi}(t)) \quad (27.40)$$

where $P_{fi}(t) = 1 - \int_0^{+\infty} f_{ip}^{12...(i-1)}(N)dN \quad (27.41)$

27.3.3 Fatigue Failure Probability Under Variable Loading

Let $f(N)$ represent the pdf of fatigue life at a given stress level and $h(n,t)$ the pdf of the applied cycles of the stress (t represents physical time). Obviously, failure occurs when the load cycle number n exceeds the fatigue life N . Fatigue failure probability is defined as:

$$P_f(t) = P(n > N) \quad (27.42)$$

By means of load cycles, fatigue life interference analysis, the fatigue failure probability can be calculated as:

$$P_f(t) = \int_0^{+\infty} h(n,t)[\int_{-\infty}^{n} f(N)dN]dn \quad (27.43)$$

Based on the residual life distribution model developed above (*e.g.*, (27.37) and (27.38)), the load cycles fatigue life interference analysis approach can be used to calculate the fatigue failure probability under variable amplitude loading conditions. For a two-level stress spectrum containing n_1 cycles of σ_1 and n_2 cycles of σ_2, let A_i represent the event of no failure occurrence at the i^{th} stress level ($i=1,2$) and $P(A_i)$ represent its probability. After n_1 cycles of the first-level stress σ_1, the probability of event A_1 (no failure occurrence) equals $P(A_1)$, which can be calculated as:

$$P(A_1)=\int_{n_1}^{+\infty} f_1(N)dN \tag{27.44}$$

Then stress level is transformed to the second stress σ_2. Because of the effect of the first level stress, the residual life distribution under the second stress σ_2 is no longer the same as that of the virgin material. The mean and the standard deviations should be calculated by (27.31) and (27.32), (27.37) and (27.38), respectively. The *pdf* of the residual life at the second-level stress is then presented by (27.33) or (27.39). In the case of the failure probability $P_{f2}(t)=1-\int_{n_1}^{+\infty} f_{2p}^1(N)dN>0$, (27.33) or generally, (27.39) should be modified to (27.40). The probability of no failure occurrence at this stress level, given the condition of no failure at the first stress level, is $P(A_2 \mid A_1)$. This conditional probability should be calculated by the interference relationship between the load cycle n_2 and the residual life N_{2p}^1, *i.e.*,

$$P(A_2 \mid A_1)=\int_{n_2}^{+\infty} f_{2pR}^1(N)dN \tag{27.45}$$

Obviously, the probability of no fatigue failure occurring after n_1 cycles of σ_1 and n_2 cycles of σ_2 equals the probability that the events A_1 and A_2 occur simultaneously. According to the conditional probability algorithm,

$$\begin{aligned} P(A_1A_2) &= P(A_1)P(A_2 \mid A_1) \\ &= \int_{n_1}^{+\infty} f_1(N)dN \int_{n_2}^{+\infty} f_{2pR}^1(N)dN \end{aligned} \tag{27.46}$$

The corresponding fatigue failure probability is

$$P_f(t)=1-\int_{n_1}^{+\infty} f_1(N)dN \int_{n_2}^{+\infty} f_{2pR}^1(N)dN \tag{27.47}$$

If there is a third-level stress in the load spectrum, the pertinent failure probability can be calculated as:

$$\begin{aligned} P_f(t) &= 1-P(A_1A_2A_3) \\ &= 1-P(A_1)P(A_2 \mid A_1)P(A_3 \mid A_1A_2) \end{aligned} \tag{27.48}$$

where, $P(A_3 \mid A_1A_2)=\int_{n_3}^{+\infty} f_{3pR}^{12}(N)dN$ (27.49)

The *pdf* and its parameters involved in (27.49) can be obtained from (27.34)–(27.36) or generally, from (27.37)–(27.39), or by the modified version of (27.36) or (27.39), *i.e.*, from (27.40).

For any complex loading spectrum, fatigue failure probability can be calculated in the same way, using (27.37)–(27.41), *i.e.,*

$$\begin{aligned} P_f(t)=1-&\int_{n1}^{+\infty} f_1(N)dN \int_{n2}^{+\infty} f_{2pR}^1(N)dN\cdots \\ &\int_{ni}^{+\infty} f_{ipR}^{12..(i-1)}(N)dN \end{aligned} \tag{27.50}$$

27.4 Conclusions

Time-dependent and load cycle-dependent reliability models are developed by means of load-strength interference analysis, order statistic theory and probability differential equations. The Poisson stochastic process is used to describe the load action. Both situations with and without strength degradation are taken into account. Time-dependent reliability models of the series system, the parallel system and the *k*-out-of-*n* redundant system are presented. The relationship between component/system reliability and time (or number of load cycles) and that between component failure rate and time (or number of load cycles) are studied, respectively.

The results show that when component strength does not degrade, both the component reliability and the failure rate decrease with time, and

component failure rate takes on the feature of the first two stages of a typical three-stage bathtub curve. If component strength degradation is taken into account, the reliability decreases with time more quickly, while the failure rate first decreases and then increases with time and takes on the whole the feature of a typical bathtub curve.

It can also be concluded that the quick decline of the failure rate in the first stage of a typical bathtub curve can not be merely attributed to a defect in product quality. The relationship between the failure rate and the number of stochastic loads shows that the decline in the failure rate curve is determined by both the strength distribution and the load distribution. For any product, no matter whether the quality is high or low, the failure rate will become lower and lower with the increase of the experienced load history, since once it has survived to a service time t, it will never fail unless a higher load (higher than any of the ones experienced during the time period $0-t$) appears if there is no strength degradation.

In addition to the investigation on strength degradation and its effect on reliability and failure rate, the residual fatigue life distribution is investigated experimentally, and a method is presented to predict fatigue probability under variable amplitude loading histories. For two-level stress, the test results show that when lower stress acts first, the standard deviation of the residual life under the subsequent higher stress becomes greater. That is, the standard deviation of the residual life is greater than that of the fatigue life of the virgin material under the pertinent high stress. When higher stress acts first, the standard deviation of the residual life under the subsequent lower stress becomes less than that of the fatigue life of the virgin material under the pertinent low stress. The greater the differences between the amplitude of the high stress and that of the low stress are, the greater the change of the standard deviation of the residual life.

In one word, previously acting cyclic stress affects both the mean and the standard deviation of the residual life under the following cyclic stress. The effect depends on the relative amplitude of the previously acting cyclic stress as well as its cycle number. A linear model is developed to predict the distribution parameters of residual fatigue life. A method based on such a model and a conditional probability algorithm, is presented to predict fatigue probability under variable amplitude loading condition.

Acknowledgements

The research work was subsidized with the Special Funds for the Major State Basic Research Projects 2006CB605000 and the Hi-Tech Research and Development Program (863) of China grant No. 2006AA04Z408.

References

[1] Li JP, Thompson GA. method to take account of inhomogeneity in mechanical component reliability calculations. IEEE Transactions on Reliability 2005;54(1):159–168.

[2] Moss TR. Mechanical reliability – Research needs. 12th ARTS, Advances in Reliability Technology Symposium, U.K. University of Manchester, April 16–17, 1996.

[3] Crocker J, Kumar UD. Age-related maintenance *versus* reliability centered maintenance: A case study on aero-engines. Reliability Engineering and System Safety 2000; 67:113–118.

[4] Xu H, Rahman S. Decomposition methods for structural reliability analysis. Probabilistic Engineering Mechanics 2005; 20:239–250.

[5] Petryna YS, Pfanner D, Stangenberg F, Kratzig WB. Reliability of reinforced concrete structures under fatigue. Reliability Engineering and System Safety 2002; 77: 253–261.

[6] Murty ASR, Gupta UC, Krishna AR. A new approach to fatigue strength distribution for fatigue reliability evaluation. International Journal of Fatigue 1995; 17(2):91–100.

[7] Roy D, Dasgupta T. A discretizing approach for evaluating reliability of complex systems under stress-strength model. IEEE Transactions on Reliability 2001; 50(2):145–150.

[8] Xie LY, Zhou JY. Load-strength order statistics interference models for system reliability evaluation. International Journal of Performability Engineering 2005; 1: 23–36.

[9] Sun ZL, Chen LY, Zhang Y, *et al*. Reliability model of mechanical transmission system (I). Journal of Northeastern University (Natural Science) 2003; 24 (6):548–551.

[10] Lewis EE. A load-capacity interference model for common-mode failures in 1-out-of-2:G systems. IEEE Transactions on Reliability 2001; 50 (1):47–51.
[11] Knut OR, Larsen GC. Reliability-based design of wind-turbine rotor blades against failure in ultimate loading. Engineering Structures 2000; 22:565–574.
[12] Li B, Meilin Z, Kai X. A practical engineering method for fuzzy reliability analysis of mechanical structures. Reliability Engineering and System Safety 2000; 67:311–315.
[13] Tryon RG, Cruse TA, Mahadevan S. Development of a reliability-based fatigue life model for gas turbine engine structures. Engineering Fracture Mechanics 1996; 53:807–828.
[14] Wasserman GS. Reliability verification, testing, and analysis in engineering design. Marcel Dekker, New York, 2003.
[15] O'Connor PDT. Practical reliability engineering. Wiley, New York, 2002.
[16] Larsen RJ, Marx ML. An introduction to mathematical statistics and its application. Prentice Hall, Englewood Cliffs, NJ, 2001; 180.
[17] Ditlevsen O. Stochastic model for joint wave and wind loads on offshore structures. Structural Safety 2002; 24:139–163.
[18] Li J-P, Thompson G. A method to take account of in-homogeneity in mechanical component reliability calculations. IEEE Transactions on Reliability 2005; 54(1):159–168.
[19] Kececioglu D. Reliability analysis of mechanical components and systems. Nuclear Engineering and Design 1972; 19:259–290.
[20] Witt FJ. Stress-strength interference methods. Pressure Vessel and Piping Technology – A Decade of Progress 1985;761–769
[21] Chen D. A new approach to the estimation of fatigue reliability at a single stress level. Reliability Engineering and System Safety 1991; 33:101–113.
[22] Kam, JPC, Birkinshaw M. Reliability-based fatigue and fracture mechanics assessment methodology for offshore structural components. International Journal of Fatigue 1994; 16(3):183–199.
[23] Kececioglu D, Chester LB, Gardne, EO. Sequential cumulative fatigue reliability. In: Annals of Reliability and Maintainability Symposium 1974; 153–159.
[24] Wirsching PH, Wu YT. Probabilistic and statistical methods of fatigue analysis and design. Pressure Vessel and Piping Technology - A Decade of Progress 1985; 793–819.
[25] Pham H. A new generalized systemability model. Int. J. Performability Engineering 2005;1:145–155.
[26] Soares CG. Reliability of marine structures. Reliability Engineering 1988; 55:513–559.
[27] Lucia AC. Structural reliability: an introduction with particular reference to pressure vessel problems. Reliability Engineering 1988; 55:478–512.
[28] Wirsching PH, Torng TY, Martin WS. Advanced fatigue reliability analysis. International Journal of Fatigue 1991; 13: 389–394.
[29] Connly MP, Hudak, SJ. A simple reliability model for the fatigue failure of repairable offshore structures. Fatigue and Fracture of Engineering Materials and Structures 1993; 16:137–150.
[30] Kopnov VA. Residual life, linear fatigue damage accumulation and optimal stopping. Reliability Engineering and System Safety 1993; 40: 319–325.
[31] Tanaka S, Ichikawa M, Akita S. A probabilistic investigation of fatigue life and cumulative cycle ratio. Engineering Fracture Mechanics 1984; 20: 501–513.
[32] Bahring H, Dunkel, J. The impact of load changing on lifetime distributions. Reliability Engineering and System Safety 1991;31: 99–110.
[33] Choukairi FZ, Barrault J. Use of a statistical approach to verify the cumulative damage laws in fatigue. International Journal of Fatigue 1993; 15:145–149.
[34] Wu YT, Wirsching PH. Advanced reliability method for fatigue analysis. ASCE J. of Engineering Mechanics 1984; 110:536–552.
[35] Wu WF. Computer simulation and reliability analysis of fatigue crack propagation under random loading. Engineering Fracture Mechanics 1993; 45:697–712.
[36] Gauri L, Mi J. Mean residual life and its association with failure rate. IEEE Transactions on Reliability 1999; 48:262–266.
[37] Tang LC, Lu Y, Chew EP. Mean residual life of lifetime distributions. IEEE Transactions on Reliability 1999; 48:73–78.
[38] Camarinopoulos L, Chatzoulis A, Frontistou-Yannas S. Assessment of the time-dependent structural reliability of buried water mains. Reliability Engineering and System Safety 1999; 65: 41–53.
[39] Zuo M, Chiovelli S, Huang J. Reliability evaluation of furnace systems. Reliability Engineering and System Safety 1999; 65:283–287.
[40] Bloch HP, Geitner FK. An introduction to machinery reliability assessment. Gulf Publishing Company, Houston, TX, 1994.
[41] Rausand M, Reinertsen R, Failure mechanisms and life models. Reliability. Quality and Safety Engineering 1996; 3:137–152.

28

New Models and Measures for Reliability of Multi-state Systems

Yung-Wen Liu[1] and Kailash C. Kapur[2]

[1]University of Michigan in Dearborn, Michigan, USA
[2]University of Washington in Seattle, Washington, USA

Abstract: This chapter descibes some new reliability models and measures for multistate systems. Equivalent classes and lower/upper boundary points are used for deriving the structure function for multistate system with multistate components. In addition to the static multistate reliability measures, several dynamic reliability measures are also introduced. Two stochastic models, Markov process and non-homogeneous continuous time Markov process are applied to formulate the probability that the system is in each state. With Non-homogeneous continuous time Markov, the age effect of the system is considered. Utility functions and disutility functions are incorporated with the stochastic models for the customer-centered reliability measures. Couple of potential applications are introduced and used to illustrate these reliability models and measures.

28.1 Introduction

The reliability of a product, process or system is a "time oriented" quality measure, and it must be defined and evaluated by the customer [22] just like any other quality characteristic. In the traditional reliability methods [21] the system and all of its components are assumed to have only two states of working efficiency: working perfectly or not working at all reslting in complete failure. Although this assumption simplifies complicated problems for reliability evaluation, it loses the ability to reflect the reality that most systems actually degrade gradually and have a wide range of states in terms of their function and performance [1, 3, 5, 18, 25, 30]. The degradation of the system and its components over time results in different levels of functional performance of the system, and hence effects the satisfaction of the customer with the system over time. Hence, a good reliability measure should not only capture the state transitions of the multi-state system, but also the customer's total experience with the system over time.

In the literature most of the work on multi-state reliability research makes the assumption that the system and all of its components have the same number of states [3, 30, 33]. This assumption is not realistic because in reality the system and its components have different numbers of states [2, 5, 7, 18]. The reliability measures described in this chapter can better capture the reality of multiple states for the systems and the components.

The degradation of a system is a stochastic process [34]. A customer's experience with the system also changes with this random degradation.

The reliability of a system is evaluated by the customer like any other quality [22]. In order to assess the reliability of the system from the customer's standpoint, we need to capture the customer's total experience with the system over time [7, 28]. Because the customer's experience is a function of the state of the system, we need to understand the degradation processes of the system, and model these underlying stochastic processes. To formulate the customer's total experience, we need to know the customer's utility function and how the utility changes with the transition of the state of the system. The dynamic reliability measures introduced in this chapter use the methodologies of stochastic processes and economic utility functions to capture the customer's total experience with the system.

The applications of these general measures and models include broad problems in

- engineering systems, design and analysis,
- supply chain and logistics,
- general networks for transportation and distribution ,
- computer and communication systems, and
- health systems.

Some of these applications will be described in the following sections.

28.2 Multi-state Reliability Models

For many systems, the binary-state reliability model is insufficient in terms of the evaluation of the system. For example, networks and their components perform their tasks at several levels of performance. Hence, it is necessary to evaluate the performance degradation of the network due to the partial failures of its components over time. In addition, customers experience the degradation of the network over time. To evaluate the system from the customer's standpoint, multi-state reliability modeling and evaluation should be implemented to avoid incorrect decision-making regarding network performance [37].

In this section, we first extend the concepts that are used to generate the structure functions for the binary-state system with binary-state components to develop the structure functions for the multi-state system with n multi-state components. The development of a new structure function for very general systems where the numbers of states of the system as well as of all of its components are different using the concept of lower and upper boundary points is proposed. This is very general and is more realistic than those approaches where the number of the states for the system and its components is the same. This structure function can be used by professionals in the industry for various applications.

It is well known that the development of the expected values of the states of the system using the structure function is a very difficult problem in terms of computational complexity. Hence, the bounds on a measure for reliability in terms of the expected values of the states of the system are also presented.

A numerical example is used to illustrate the structure function, the calculation of the expected value of the states of the system, and the bounds for this reliability measure.

28.2.1 Classification of States

Binary-state Model

Let y be the substitute characteristic [22] for the function of the component and y_0 be the ideal or target value for y. In the binary case, we classify the states of the component into two classes. The system is functioning if $y_0 - \Delta_0 \le y \le y_0 + \Delta_0$, and failed otherwise. The value of Δ_0 is based on the requirements of the customer. Let x_i, $i = 1, \ldots, n$, represent the state of component i for a system with n components. Then

$$x_i = \begin{cases} 1 & \text{if } y_0 - \Delta_0 \le y \le y_0 + \Delta_0 \text{ (component functions)} \\ 0 & \text{otherwise (component has failed)} \end{cases}$$

Multi-state Model

Again, let y be the substitute characteristic for the function of the component. Then the states of a multi-state component are defines as (see also Figure 28.1):

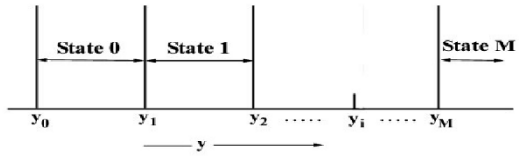


Figure 28.1. State classification

$$x_i = \begin{cases} 0 & \text{if } y_0 \le y < y_1 \\ 1 & \text{if } y_1 \le y < y_2 \\ \vdots & \vdots \\ M & \text{if } y \ge y_M \end{cases}$$

The range of each state can be decided by the reliability engineer based on the physical condition of the system and the customer's preferences.

Notation

n	number of components
(m_i+1)	number of states of component i
$M+1$	number of states of the system
S	$[0,1,\ldots, m_1]$x$[0,1,\ldots, m_2]$x…x$[0,1,\ldots, m_n]$ –
s	component state space $[0,1,\ldots, M]$ – system state space

$\phi(x,t): S \rightarrow s$ is the structure function

28.2.2 Model Assumptions

In a multi-state system with n different components, each component i is assumed to have $(m_i + 1)$ distinct levels of working efficiency called states. If $x_i(t)$ denotes the state for the ith component at time t, then $x_i(t) \in [0,1,\ldots, m_i]$ for $i = 1, 2, \ldots, n$. When $x_i(t) = 0$, the ith component is in the state of total failure at time t. On the other hand, when $x_i(t) = m_i$, the ith component is in the state of perfect functioning at time t. For the static model that considers the working efficiency of the system and its components at a fixed time t, x_i is used instead of $x_i(t)$ to denote the status of working efficiency for the ith component at time t. All the components are assumed to be mutually independent, which means that the working efficiency of each component is not affected by the working efficiency of any other component. The system itself is also assumed to have M+1 different levels of working efficiency. If the structure function of this multi-state system is denoted by $\phi(x,t)$, the status of the working efficiency of this system at some specified time t is given by $\phi(x,t) = k$, where $x = (x_1, x_2,\ldots, x_n)$ is a vector of the states of the n components and $k \in [0, 1,\ldots, M]$.

Therefore, the system is in the state of total failure at time t when $\phi(x,t) = 0$, and it is working perfectly at time t when $\phi(x,t) =$ M. Let $s = [0, 1,\ldots, m_1]\times[0,1,\ldots, m_2]\times\ldots\times[0, 1,\ldots, m_n]$ be the components state space that is the set of all possible states of the components, and $S = [0,1,\ldots,M]$ be the set of all possible states of the system. Then the relationship between the components and system can be expressed as

$$\phi(x,t): S \rightarrow s$$

Again, for the static model, $\phi(x)$ is used instead of $\phi(x,t)$ to denote the status of working efficiency for the system at time t.

Definition 1:

Let $x = (x_1, x_2,\ldots, x_n)$ and $y = (y_1, y_2,\ldots, y_n)$ be two vectors representing the states of the n components of a system. Then we say that $x < y$ if $x_i \le y_i$, for every $i = 1, 2, \ldots, n$, and $x_i < y_i$ for at least one i.

Equivalent Classes

An equivalent class is the collection of all combinations of the states of n components of the system that allows the system to be in state k ($k \in [0, 1,\ldots, M]$), and is defined as:

$$S_k = \{x \mid \phi(x) = k\}, \forall\ k \in [0, 1, 2, ..., M],$$
$$\text{where } x = (x_1, x_2, \cdots, x_n)$$

S_k is known as the equivalent class, the collection of all combinations of states of the n components that make the system to be in state k and S_k's are mutually exclusive, $\bigcup_{i=1}^{M} S_k = S$, where is S the component state space.

Let θ_k be the number of elements in each equivalent class S_k. Of those θ_k different elements, L_k are called "lower boundary points" and U_k are called "upper boundary points".

Definition 2: Lower Boundary Points

$x = (x_1,x_2,\ldots,x_k) \in S_k$ is called a lower boundary point if only if for any $y = (y_1,y_2,\ldots,y_k) < x$, $\phi(y) < k$.

When x is a lower boundary point, any of its component has a change to a lower state will result in a lower state for the system. The collection of all the lower boundary points for the equivalent class k is called the "lower boundary point set", which is denoted as

$$LB(k) = \left(\hat{x}_{(1k)}, \hat{x}_{(1k)}, \cdots, \hat{x}_{(L_k k)}\right) \subset S_k$$

and $\hat{x}_{(ik)}, \forall\, i \in [1, 2, \cdots, L_k]$, is the ith lower boundary point for S_k.

Definition 3: Upper Boundary Points

$x = (x_1, x_2,\ldots, x_k) \in S_k$ is called a upper boundary point if only if for any $y = (y_1, y_2,\ldots, y_k) > x$, $\phi(y) > k$.

When x is an upper boundary point, a change in any of its components to a higher state will result in a higher state for the system.

The collection of all the upper boundary points for the equivalent class k is called the lower boundary point set, which is denoted as

$$UB(k) = \left(\breve{x}_{(1k)}, \breve{x}_{(1k)}, \cdots, \breve{x}_{(L_k k)}\right) \subset S_k$$

and $\breve{x}_{(ik)}, \forall\, i \in [1, 2, \cdots, U_k]$, is the ith upper boundary point for S_k.

From the definition of the lower boundary point, we know that a system is in the state k or higher if x is greater than or equal to at least one lower boundary point in the lower boundary points set LB(k). This can be formulated as

$$\hat{I}(k) = 1 - \prod_{i=1}^{L_k} \left[1 - I(x \geq \hat{x}_{(i,k)})\right]$$

where $I(\,)$ is an indicator function, and its value is 1 if $x \geq \hat{x}_{(i,k)}$ and 0 otherwise.

Figures 28.2 and 28.3 show the concepts of equivalent classes and upper and lower boundary points.

From now on,we will use the notation $I(\,)$ as the indicator function and its value is 1 if the logical expression in $(\,)$ is true, and 0 otherwise. If $\hat{I}(k+1) > \hat{I}(k)$ then we set $\hat{I}(k) = \hat{I}(k+1)$. $k = 0$ means that the system is totally failed, and we let $\hat{I}(0) = 1$. Then the structure function is

$$\phi(x) = \sum_{k=0}^{M} \hat{I}(k) - 1$$

From the definition of the upper boundary point, we know that a system is in the state k or lower if at least one x is less than or equal to all of the upper boundary points in the upper boundary points set UB(k). Define

$$\breve{I}(k) = \prod_{i=1}^{U_k} \left[1 - I(x \leq \breve{x}_{(i,k)})\right]$$

If $\breve{I}(k+1) > \breve{I}(k)$ then we set $\breve{I}(k+1) = \breve{I}(k)$. $k = M$ means that the system is perfectly working, and we let $\breve{I}(M) = 0$. Then the structure function is

$$\phi(x) = \sum_{k=0}^{M} \breve{I}(k)$$

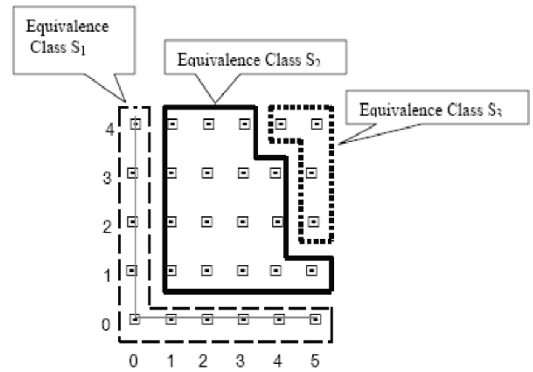


Figure 28.2. Equivalence classes

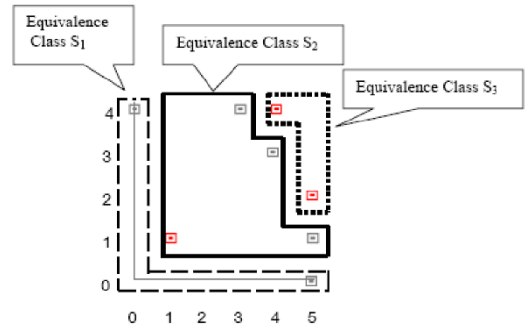


Figure 28.3. Upper/lower boundary points

With the above structure functions, we can find the expected value of the state of the system as follows:

1. With lower boundary points

$$E[\phi(x)] = E\left[\sum_{k=0}^{M} \hat{I}(k) - 1\right] = \sum_{k=0}^{M} E\left[\hat{I}(k)\right] - 1$$

2. With upper boundary points

However, as the number of components and the number of different states of components increase, the calculation of the exact expected state of the system with the method described in the previous section will take a long time due to the computational complexity [6, 19, 25, 41]. Based on the definition of the structure functions, the bounds on the expected value of states for the system are developed as follows:

Lower bounds

Using inclusion/exclusion, we can find bounds on the expected values of state of the system as below. The lower bound is

$$\sum_{l=0}^{M-1} \prod_{k=0}^{l} \prod_{i=1}^{U_k} \left[1 - \prod_{j=1}^{n} \text{Prob}\left(x_j \le \breve{x}_{[(i,k),j]}\right)\right]$$

Upper bounds

The upper bound is

$$M - \sum_{l=0}^{M-1} \prod_{k=M-l}^{M} \prod_{i=1}^{L_k} \left[1 - \prod_{j=1}^{n} \text{Prob}\left(x_j \ge \hat{x}_{[(i,k),j]}\right)\right]$$

Example

Consider a system with two components with m_1 = 3, m_2 = 2 and M = 3. The information on the boundary points is given in Table 28.1, and the information for the component state probabilities is given in the Table 28.2.

To illustrate both the structure functions, let us apply it to x = (2, 1).

Table 28.2. Component-state probability

Component	Component state (x)			
	0	1	2	3
1	0.2	0.4	0.1	0.3
2	0.3	0.2	0.5	

With the lower boundary points,

$\hat{I}(0) = 1$

$\hat{I}(1) = 1$ because $(2,1) \ge (1, 0)$ and $(2,1) \ge (0, 1)$,

$\hat{I}(2) = 1$ because $(2,1) \ge (1, 1)$, and

$\hat{I}(3) = 0$ because $(2,1) < (3, 2)$.

Using the structure function derived from the lower boundary points, for this vector of states of components, the system is in state 2:

$\phi(x) = \sum_{k=0}^{3} \hat{I}(k) - 1 = 2$.

Similarly, with the upper boundary points,

$\breve{I}(0) = 0$ because $(2,1) \ge (0, 0)$

$\breve{I}(1) = 0$ because $(2,1)$ is not less than or equal to either (3, 0) or (0, 2),

$\breve{I}(2) = 1$ because $(2,1) < (2,2)$, and

$\breve{I}(3) = 1$.

Using the structure function derived from the upper boundary points, for this vector of states of components, the system is in state 2:

$\phi(x) = \sum_{k=0}^{3} \breve{I}(k) = 2$.

For this system, we get $E[\phi(x)] = 1.65$, using either the structure function derived from the lower boundary or upper boundary points. Also, bounds on system reliability are $1.54 \le E[\phi(x)] \le 1.75$.

28.3 Measures Based on the Cumulative Experience of the Customer

In traditional binary reliability models, one reliability measure is defined as the probability that a system is functioning perfectly at some point in time $t \in (0, \infty)$. It is denoted by $R(t) = \Pr(\Phi(t) = 1)$, where $\Phi(t)$, the state of the system at time t, is 1 (success) or 0 (failure). In practice, most systems have more than two states of working efficiency (*i.e.,* $\Phi(t) = 0, 1, 2, \ldots, M$, and $M \ge 1$). After being working for some period of time, systems degrade gradually and perform at intermediate states between working perfectly and total failure [5, 7, 15, 25]. Therefore, a reliability measure for multi-state systems should consider all states above some intermediate state. One reliability measure for a

multi-state system is the probability that the system is in some intermediate state k, $k \in [1,\cdots,M]$, or higher at some target usage time t^*, $t^* \in (0,\infty)$. This definition can be expressed as

$$R_k(t^*) = \Pr(\Phi(t^*) \geq k), \forall\ k \in [1,\cdots,M]..$$

The reliability of the system (not repairability or maintainability) is the only concern here. Hence, with time, the system only degrades and does not make transitions to higher states [28, 46, 47]. It is also assumed to be able to degrade directly to any lower state during a transition (see Figure 28.4). With these assumptions and the properties of stochastic processes, models are developed to capture the degradation patterns of the system, and are used to calculate the reliability measures for multi-state systems.

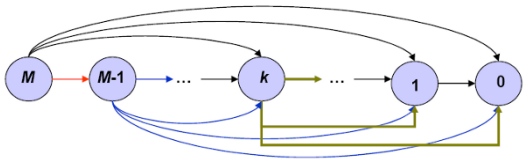


Figure 28.4. Multi-state system degradation

When the degradation pattern of the system is captured, $R_k(t^*) = \Pr(\Phi(t^*) \geq k), \forall\ k \in [1,\cdots,M]$ defines the reliability measure and can be used to evaluate the system at time t^*, $t^* \in (0,\infty)$. A good system should always function at the higher states of working efficiency. For a binary-state system, $R(t) = E[\Phi(t)]$. If the integration of the expected value of the state of this system from 0 to t^* is close to t^*, or if $\frac{1}{t^*}\int_1^{t^*} E[\Phi(t)]dt = \frac{1}{t^*}\int_1^{t^*} R(t)dt$ is close to 1, this system functions perfectly most of time from 0 to t^*.

Similarly, for a multi-state system with M+1 states, if the integration of the expected value of the state of this system from 0 to t^* is closer to Mt^* or $\frac{1}{Mt^*}\int_1^{t^*} E[\Phi(t)]dt = \frac{1}{t^*}\int_1^{t^*} R(t)dt$ is close to 1, this system functions at high levels of working efficiency from 0 to t^*. The advantage of this reliability measure is that with it, different systems can be easily evaluated and compared even though they have different numbers of states of working efficiency. The system with the measure closer to 1 would be considered the better system.

In addition, when evaluating multi-state systems, the customer's preference or utility/ disutility over time should also be taken into account. Some people might prefer a system that works perfectly even though it cannot work for a very long time at that level. However, others might prefer a system that works longer, even though it might not work close to perfection during part of its lifetime.

One numerical example is presented later on to illustrate the calculations and applications of these reliability measures for system performance evaluation.

28.3.1 System Deterioration According to a Markov Process

The degradation of the system from the perfect state, $\Phi(t) = M$, to lower states was first modeled with the Markov process [2, 47] which assumes that the next state of the system depends only on its current state, and that times between transitions follow the stationary exponential distributions. The reliability of the system (not with repairability or maintainability) is the concern here. Hence the system only degrades with time, and does not make transitions to higher states. This can be generalized to consider maintainability. The system is also assumed to be able to degrade directly to any lower state per transition. Models are developed to capture the degradation patterns of the system and are used to calculate the reliability measures for multi-state systems.

For the Markov process, the instantaneous degradation rate from state i to any lower state j is also assumed to be constant and is represented by $\lambda_{i,j}$, where $i > j$ and $i \in [M, M-1,\cdots,1]$. The instantaneous degradation rate matrix Λ summarizes all the instantaneous degradation rates.

$$\Lambda = \begin{bmatrix} \lambda_{M,M-1} & \lambda_{M,M-2} & \cdots & \lambda_{M,1} & \lambda_{M,0} \\ 0 & \lambda_{M-1,M-2} & \cdots & \lambda_{M-1,1} & \lambda_{M-1,0} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \lambda_{1,0} \end{bmatrix}$$

To obtain the reliability measure:

- The probability that the system is in state M at time t is:

$$P(\Phi(t)=M)$$
$$=\exp\left[-\left(\lambda_{M,M-1}+\lambda_{M,M-2}+\cdots+\lambda_{M,1}+\lambda_{M,0}\right)\ t\right]$$
$$=\exp\left[-\left(\sum_{x=0}^{M-1}\lambda_{M,x}\right)\ t\right]$$

- The probability that the system is in state $M-1$ at time t is:

$$P(\Phi(t)=M-1)=\int_0^t \exp[-G_M\tau_1]\lambda_{M,M-1}$$
$$\exp[-G_{M-1}(t-\tau_1)]\,d\tau_1$$
$$=\frac{\lambda_{M,M-1}}{G_M-G_{M-1}}\{\exp(-G_{M-1}t)-\exp(-G_M t)\}$$

- For Pr(Φ(t)=$M-2$), the system can go from M to $M-1$ and then from $M-1$ to $M-2$,

$$P_1(\Phi(t)=M-2)$$
$$=\int_0^t\int_0^{\tau_2}\exp[-G_M\tau_1]\lambda_{M,M-1}\exp[-G_{M-1}(\tau_2-\tau_1)]$$
$$\lambda_{M-1,M-2}\exp[-G_{M-2}(t-\tau_2)]d\tau_1 d\tau_2$$
$$=\frac{\lambda_{M,M-1}\lambda_{M-1,M-2}}{G_M-G_{M-1}}\left\{\frac{\exp(-G_{M-2}t)-\exp(-G_{M-1}t)}{G_{M-1}-G_{M-2}}\right.$$
$$\left.-\frac{\exp(-G_{M-2}t)-\exp(-G_M t)}{G_M-G_{M-2}}\right\}$$

Or the system and go from M to $M-2$ directly.

$$P_2(\Phi(t)=M-2)=\int_0^t\exp[-G_M\tau_2]\lambda_{M,M-2}$$
$$\exp[-G_{M-2}(t-\tau_2)]d\tau_2$$
$$=\frac{\lambda_{M,M-2}}{G_M-G_{M-2}}\{\exp(-G_{M-2}t)-\exp(-G_M t)\}$$

There are two different ways to degrade to the state $M-2$ from the state M (*i.e.*, $M\to M-1\to M-2$ and $M\to M-2$); four different ways to degrade to the state $M-3$ from M (*i.e.*, $M\to M-1\to M-2\to M-3$ and $M\to M-2\to M-3$ and $M\to M-3$); eight different ways to degrade to the state $M-4$ from M. There are $\sum_{r=0}^{M-i-1}\binom{M-i-1}{r}$ ways to go from M to i. With the same logic, the probability that the system is in state i at time t is the sum the following probabilities:

1. From M to i directly (no intermediate states):

$$P_0=\int_0^t\exp[-G_M\tau_1]\lambda_{M,i}\exp[-G_i(t-\tau_1)]\,d\tau_1$$
$$=\frac{\lambda_{M,i}}{G_M-G_i}\{\exp(-G_i t)-\exp(-G_M t)\}$$

2. With one intermediate state

$$P_{1,k}=\lambda_{M,k}\lambda_{k,i}\int_0^t\int_0^{\tau_2}\exp[-G_M\tau_1]\exp[-G_k(\tau_2-\tau_1)]$$
$$\exp[-G_i(t-\tau_2)]\,d\tau_1 d\tau_2$$

where $k=[M-1,\ldots,i+1]$

3. With n intermediate states: $n=2,\ldots,M-i-1$

$$P_n=\lambda_{M,k_1}\left(\prod_{N=1}^{n-1}\lambda_{k_N,k_{N+1}}\right)\lambda_{k_n,i}\times\int_0^t\cdots\int_0^{\tau_2}\exp\ [-G_M\tau_1]$$
$$\left(\prod_{j=1}^{n}\exp\ [-G_{k_j}(\tau_{j+1}-\tau_j)]\right)$$
$$\exp\ [-G_i(t-\tau_{n+1})]\,d\tau_1\cdots d\tau_{n+1}$$

where $k_1=[M-1,\ldots,i+n]$ and $M>k_1>\ldots>k_n>1$, For each n, there are all $\binom{M-i-1}{r}$ combinations of k_1, $k_2,\ldots,k_n$.

28.3.2 System Deterioration According to a Non-homogeneous Markov Process

The assumption for the Markov process that the next state only depends on the current state is applicable only to systems that do not have an age effect such as software engineering systems, supply chains and transportation network systems. Sooner or later most systems wear out after being

used. Hence, the next state of the system and the length of time that a system stays in some state depend not only on the current state but also on how long the system has been in use. In this chapter, a general stochastic model, the non-homogeneous continuous time Markov process (NHCTMP) model, which is a stochastic model with discrete states and continuous time, is described. With this stochastic model, the age effect for the system is incorporated in the modeling of the process [29, 44].

NHCTMP assumes that system's next state depends not only on the current state but also on the time that the system entered the current state. This assumption reflects the age effect that is typical of many systems.

Let $\Phi(t)$ be the state of the system at time t, $\Phi(t) \in [0,1,\ldots,M]$, and $\Phi(t)$ follows NHCTMP. The transition probability from current state i to next state j from time s to time t is denoted by:

$$p_{i,j}(s,t) = \Pr(\Phi(t) = j \mid \Phi(s) = i),$$

$s<t$, $i, j \in [0,1,\ldots,M]$ and $i > j$.

Similar to the Markov process, the non-homogeneous Markov processes can be expressed with the instantaneous degradation rate matrix, $\Lambda(t)$, and

$$\Lambda(t) = \begin{bmatrix} \lambda_{M,M-1}(t) & \lambda_{M,M-2}(t) & \cdots & \lambda_{M,1}(t) & \lambda_{M,0}(t) \\ 0 & \lambda_{M-1,M-2}(t) & \cdots & \lambda_{M-1,1}(t) & \lambda_{M-1,0}(t) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \lambda_{1,0}(t) \end{bmatrix}$$

where

$$\lambda_{i,j}(t) = \lim_{\Delta t \to \infty} \frac{\Pr(\Phi(t+\Delta t) - \Pr(\Phi(t)}{\Delta t}$$

With the known $\Lambda(t)$, we can have the following:

- The probability that the system is in state M at time t is:

$$\Pr(\Phi(t) = M) = \exp[-\int_0^t \sum_{j=0}^{M-1} \lambda_{M,j}(\tau) d\tau]$$

- The probability that the system is in state $M-1$ at time t is:

- For $\Pr(\Phi(t) = M-2)$, the system can go from M to $M-1$ and then from $M-1$ to $M-2$,

$$\Pr_I(\Phi(t) = M-2) = \int_0^t \exp[-\int_0^{\tau_2} \sum_{j=0}^{M-1} \lambda_{M,j}(s) ds] \lambda_{M,M-2}(\tau_2) \exp[-\int_{\tau 2}^t \sum_{j=0}^{M-3} \lambda_{M-2,j}(s) ds] d\tau_2$$

Or the system and go from M to $M-2$ directly.

$$\Pr_{II}(\Phi(t) = M-2) = \int_0^t \int_0^{\tau_2} \exp[-\int_0^{\tau_1} \sum_{j=0}^{M-1} \lambda_{M,j}(s) ds] \lambda_{M,M-1}(\tau_1) \exp[-\int_{\tau 1}^{\tau 2} \sum_{j=0}^{M-2} \lambda_{M-1,j}(s) ds] \lambda_{M-1,M-2}(\tau_2) \exp[-\int_{\tau 2}^t \sum_{j=0}^{M-3} \lambda_{M-2,j}(s) ds] d\tau_1 d\tau_2$$

When the system is in state i at time t the following probabilities should be considered:

1. From M to i directly: (No intermediate states)

$$P_{0,i} = \int_0^t \exp[-\int_0^{\tau_1} \sum_{j=0}^{M-1} \lambda_{M,j}(s) ds] \lambda_{M,i}(\tau_1) \exp[-\int_{\tau 1}^t \sum_{j=0}^{i-1} \lambda_{i,j}(s) ds] d\tau_1$$

2. With only one intermediate state: $l = [M-1,\ldots, i+1]$

$$P_{1,l,i} = \int_0^t \int_0^{\tau_2} \exp[-\int_0^{\tau_1} \sum_{j=0}^{M-1} \lambda_{M,j}(s) ds] \lambda_{M,l}(\tau_1) \exp[-\int_{\tau 1}^{\tau 2} \sum_{j=0}^{l-1} \lambda_{l,j}(s) ds] \lambda_{l,i}(\tau_2) \exp[-\int_{\tau 2}^t \sum_{j=0}^{i-1} \lambda_{i,j}(s) ds] d\tau_1 d\tau_2$$

3. With n intermediate states: ($n = 2,\ldots,M-1$)

$$P_{(n,j),h} = \int_0^t \cdots \int_0^{\tau_2} \exp[-\int_0^{\tau_1} \sum_{j=0}^{M-1} \lambda_{M,j}(s) ds] \lambda_{M,l_1}(\tau_1) \prod_{g=1}^{n-1} \left\{ \exp[-\int_{\tau_N}^{\tau_{g+1}} \sum_{j=0}^{l_{g-1}} \lambda_{l_g,j}(s) ds] \lambda_{l_N,l_{g+1}}(\tau_{g+1}) \right\} \exp[-\int_{\tau_n}^{\tau_i} \sum_{j=0}^{l_{n-1}} \lambda_{l_n,j}(s) ds] \lambda_{l_n,l_i}(\tau_{g+1}) \exp[-\int_{\tau_i}^t \sum_{j=0}^{i-1} \lambda_{i,j}(s) ds] d\tau_1 \cdots d\tau_{n+1}$$

where $h = \binom{M-i-1}{r}$, $l_g = [M-1,\ldots, i+1]$, $M > l_1 > \ldots > l_n > i$, $g = 1, 2, \ldots, n$.

28.3.3 Dynamic Customer-center Reliability Measures for Multi-state Systems

A system might function for a very long time but always with poor efficiency, another might work perfectly in the beginning but then degrade sharply in the short term, and yet another might just degrade very slowly. These three systems may have the same area A in terms of the previous measure and thus are similar, but the customer's satisfaction with these systems may be very different based on their utility over time. This idea can also be visualized using Figure 28.5. Both system I and system II may have the same area, but system II stays in higher states during the early life periods and, of course, system I stays in higher states during the later life periods.

Customers may have different utilities at different life periods. When evaluating multi-state systems, the customer's preference or utility over time should also be considered. To obtain the customer's total experience with the system, we can use the customer's utility function typically used in economics. A utility function, U(x), is the function that transfers customer's preference for some element x to a numerical value. The bigger value indicates that the customer likes the element better [8, 13]. Different customers have different utility functions, and thus different customers will evaluate the same system differently.

With the customer's utility function as a function of the state of the system, we can calculate the customer's expected total utility for experience (ETUE) with the system from time 0 to t*.

$$ETUE = \int_0^{t^*} E[U(\Phi(t))]\, dt$$

$$= \int_0^{t^*} \sum_{\phi=0}^{M} U(\phi) \Pr(\Phi(t) = \phi)\, dt$$

$$= \sum_{\phi=0}^{M} \int_0^{t^*} U(\phi) \Pr(\Phi(t) = \phi)\, dt$$

The greater the ETUE, the better the system from the viewpoint of the customer.

Example

Let us assume that the utility function for a customer for some system is $U(\phi)=\phi^2$. It should also be pointed out that we can very easily use any other utility function. Two systems are evaluated by this customer. Systems I and II are assumed to have the following instantaneous degradation rates matrices:

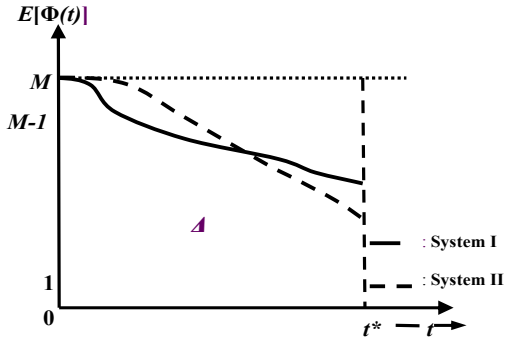


Figure 28.5. Reliability integration for multi-state systems

System I *System II*

$$\Lambda_I = \begin{pmatrix} 0.200 & 0.100 & 0.090 \\ 0 & 0.007 & 0.006 \\ 0 & 0 & 0.008 \end{pmatrix} \quad \Lambda_{II} = \begin{pmatrix} 0.080 & 0.060 & 0.050 \\ 0 & 0.120 & 0.112 \\ 0 & 0 & 0.260 \end{pmatrix}$$

The above two different instantaneous degradation rate matrices indicate that System II will stay at state 3 for longer than System I; System I will stay at states 2 and 1 much longer than system II. However, the accumulated areas from time 0 to 10 under the expected state function are almost the same. For System I, the integral area A_{I} is 16.7830 and for System II, integral area A_{II} is 16.7828. This means that these two system work equally well from time 0 to 10 using the area as a measure. However, this customer may have different experiences with these two systems based on this customer utility function.

The ETUEs show that the total utility that this customer perceives from System I and System II in the last section from time 0 to 10 is:

$$ETUE_I = \int_0^{10} E[U(\Phi(t))]\, dt = \int_0^{10} \sum_{\phi=0}^{3} \phi^2 \Pr(\Phi(t) = \phi)\, dt$$

$$= \sum_{\phi=0}^{3} \int_0^{10} \phi^2 \Pr(\Phi(t) = \phi)\, dt = 22.61 + 14.57 + 1.96$$

$$= 39.14,$$

and

$\text{ETUE}_{\text{II}} = 40.28+4.49+1.11 = 45.88$

The value of $\Pr(\Phi(t)= \phi)$ for this example can be very easily calculated with the equations mentioned in the previous section. Thus, for this example, the customer receives greater ETUE from System II than from System I and hence System II is a better system for the customer for use from 0 to 10 units of time.

Total Experience for the Life Term of the System

Another way to compare two systems is to compare the total utility that the customer receives from using the system until it fails. Thus it would be very interesting to know the expected time that system spends in each state for its whole life term. We can infer that the longer the system spends in higher states, the greater the total utility that will be perceived by the customer.

The expected time that system spends in the state of M for its life term is:

$$E[T_M] = \int_{t=0}^{\infty} P(X(t) = M)dt = \int_{0}^{\infty} \exp(-G_M t)dt = \frac{1}{G_M}$$

The expected time that the system spends in the state of $M-1$ for its life term is:

$$E[T_{M-1}] = \int_{t=0}^{\infty} P(X(t) = M-1)dt$$

$$= \int_{0}^{\infty} \frac{\lambda_{M,M-1}}{G_M - G_{M-1}} \{\exp(-G_{M-1}t) - \exp(-G_M t)\}dt$$

$$= \frac{\lambda_{M,M-1}}{G_M G_{M-1}}$$

Similarly, the expected time that the system spends in the state of $M-2$ for its life term is:

$$E[T_{M-2}] = \int_{t=0}^{\infty} P(X(t) = M-2)dt$$

$$= \frac{\lambda_{M,M-1}\lambda_{M-1,M-2}}{G_M G_{M-1} G_{M-2}} + \frac{\lambda_{M,M-2}}{G_M G_{M-2}}$$

and the expected time that the system spends in the state of i for its life term is:

$$E[T_i] = \int_{t=0}^{\infty} P(X(t) = i)dt = \frac{\lambda_{M,i}}{G_M G_i} + \sum_{k=i+1}^{M-1} \frac{\lambda_{M,k}\lambda_{k,i}}{G_M G_k G_i}$$

$$+ \sum_{n=2}^{M-i-1} \int_{t=0}^{\infty} P_n dt$$

For each n in the last equation, there are $\binom{M-i-1}{r}$ different P_n that can be obtained.

These expected times can be combined with the customer's utility function to develop other customer-centered measures for reliability and safety. A better system should give the customer more utility over time and thus these measures can be used for system design and analysis from the viewpoint of reliability and safety. These models can be generalized for other stochastic processes and we can also incorporate maintainability issues in these models.

28.4 Applications of Multi-state Models

Modern society increasingly relies on infra-structure networks such as the supply chain and logistics [36, 37], transportation networks [4, 9, 10, 20], commodity distribution networks (oil/water/gas distribution networks) [24, 31, 45], and computer and communication networks [23, 40] amongst others. With increasing emphasis on better and more reliable services in competitive global markets, reliability analysis has to be incorporated as an integral part of the planning, design and operations of these infrastructure and related networks. Networks and their components can provide several levels of performance ranging from perfect functioning to complete failure.

In clinical research, patients may experience multiple events that are observed and recorded periodically. For example, in a stroke study [11], patients can be classified into three states based on the Glasgow outcome score (GOS). State 1 is considered the unfavorable state that patients have GOS = 2 or 3. State 2 is considered as the favorable state that patients have GOS = 4 or 5. State 3 represents death. For a diabetes study [1], a patient can be dead or be alive with or without diabetic nephropathy (DN) at some point in time after he/she has been diagnosed with diabetes. To analyze patterns of a disease process, it is desirable

to use those multiple events over time in the analysis.

In order to provide the motivation for applications of the proposed research to potential problems, two examples are presented in the next section: the multi-state flow network reliability and a potential application in measuring the prostate cancer patients' quality of life using the dynamic customer-centered reliability models.

28.4.1 Infrastructure Applications – Multi-state Flow Network Reliability

A network consists of two classes of components: nodes and arcs (or edges). The topology of a network model (see Figure 28.6) can be represented by a graph, $G = (N, A)$ where $N = \{s, 1, 2, \ldots, n, t\}$ is the set of nodes with s as the source node and t as the sink node and $A = \{a_i | 1 \le i \le n\}$ is the set of arcs where an arc ai joins an ordered pairs of nodes $(i, i') \in N \times N$ such that $i \neq i'$. Let $m = \{m_1, m_2, \ldots, m_n\}$ be a vector of maximum capacities for the arcs.

Assume that all the nodes in the network are perfectly reliable. Based on the maximum capacity, we can easily find the maximum flow in the network from node s to node t. This maximum value of flow is equivalent to state M of the system for the development of the structure function, and $0 \le k \le M$. The actual capacity at any time of the arc degrades from m_i, i = 1, …, n, to 0. Let x_i be the actual capacity of the arc a_i, $0 \le x_i \le m_i$, where x_i takes only integer values. This x_i is like the state of the component in the development of the structure function in the Section 28.2.

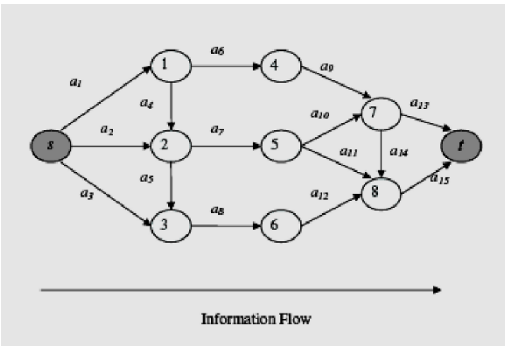


Figure 28.6. Network system

Let E be the node-arc incidence matrix denoted by

$$e(l, a_i) = \begin{cases} 1 & \text{if } l \text{ is the initial node of the arc } a_i \\ -1 & \text{if } l \text{ is the terminal node of the arc } a_i \\ 0 & \text{otherwise} \end{cases}$$

Let e_s be the column vector whose elements are all 0 except the first element, which is is 1; e_t is the column vector whose elements are all 0 except in the last element, where it is 1, and 0 denotes a column vector that has all zero values. The highest state of the network system is the maximum value of the flow, f, which is obtained by solving the following optimization problem:

$Max \;\; f$

$Subject \;\; to$

$Ex^t = (e_s - e_t) f$, E is the node-arc incidence matrix

$x^t \le m^t$

$x^t \ge 0$ and integer

f is the flow, and we want to find probabilities for all the values for the flow in the network to develop measures for reliability. Thus, $S_M = \{x \mid f(x) = M\}$, the equivalence class for the highest value, M, of the state of the system.

Research is under way (through methods in network flow optimization using various labelling algorithms) to generate all the equivalence classes and their boundary points. Then we can apply the methods discussed above to evaluate reliability of the infrastructure networks [38].

28.4.2 Potential Application in Healthcare: Measure of Cancer Patients' Quality of Life

When prostate cancer is diagnosed, the patient is given a stage that indicates the extent of the cancer. Prostate cancer is always categorized into more than two stages based on different staging systems such as Whitmore–Jewett staging and the TNM staging systems.

One of the most popular stage systems developed by the National Cancer Institute categorizes prostate cancer into five stages: 0, I, II, III, and IV (see Table 28.3 for the brief stage

Table 28.3. One definition of prostate cancer stages

Stage	Definition
0	Death
I	Tumors have spread to other parts of body such as bladder, bones, liver or lung
II	Tumors can be found outside of the prostate in nearby tissue
III	Tumors are located only in the prostate but are visible in the image
IV	Tumors are located only in the prostate and not visible in image

definitions). The patient stays in some stage with a lesser extent of cancer for a random period of time and then moves to another stage with more extensive cancer or death (see Figure 28.7). This movement is a stochastic process and it is commonly modeled with a Markov process that assumes that the next stage of cancer only depends on the current stage. In this chapter, we used the NHCTMP model (presented in the previous) to capture the process of the stage changes for the patient. The probability that a patient stays in each stage at some point in time, and the expected time for a patient to be in each stage can be estimated using the stochastic model described in the previous section [also see 12, 14, 16, 42].

Suppose that prostate cancer is categorized by five different stages, $\Phi(t) = 4, 3, 2, 1, 0$, where 4 is the best stage (lesser extent) and 0 is death. A prostate cancer patient can be in stage 4 straight after receiving two different interventions ($t = 0$).

Intervention I makes $\Phi(t)$ follow NHCTMP with instantaneous degradation rates $\lambda_{ij} = \frac{3}{(i-j)^4} t^3, i,$ $j = 4, 3, 2, 1, 0$ and $i > j$ and Intervention II makes $\Phi(t)$ follow NHCTMP with instantaneous degradation rates $\lambda_{ij} = \frac{3}{2(i-j)^2} t$, i, j = 4, 3, 2, 1, 0 and $i > j$.

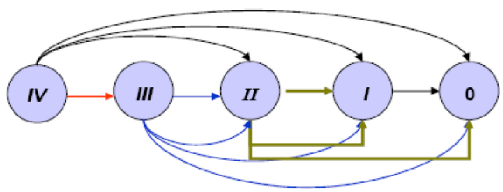


Figure 28.7. Possible stages of prostate cancer movement

We assume that the target or the normalized period of interest from the viewpoint of the patient is [0, 1.85]. Using the equations derived in last section, the probabilities that the patient is in some stage at time 1.85 after receiving two different interventions can be estimated. These are summarized in the Table 28.4.

Quality of life is an important consideration for making a decision about any intervention [14, 17, 26] . The patient's quality of life can reasonably be assumed to change with the stage of his cancer and the types of medical treatment received. With more severe illnesses or more unpleasant side effects from the treatment, the patient's quality of life is likely to be lower.

To measure the decrease in the quality of life, a disutility function can be formulated to measure

Table 28.4. Prostate cancer stage probability at time 1.85

stage (k)	Intervention I	Intervention II
	$Pr_I(\Phi(1.85) = k)$	$Pr_{II}(\Phi(1.85) = k)$
4	0.000	0.026
3	0.001	0.072
2	0.003	0.125
1	0.011	0.165
0	0.985	0.612

how unpleasant or how unsatisfied the patient feels about his illness and medical treatments. The disutility function can be used as one measurement of the patient's quality of life measurement. Disutility functions are commonly used in economics and transportation research [27, 43] and are defined as a function that transfers the customer's dissatisfaction with some item to a numerical value [See also 8, 13, 32, 35, 37]. The greater this numerical value, the more the customer dislikes the item.

A common disutility function in the decision-making literature is the exponential disutility function, which has different forms for different types of risk takers.

I. *Risk Averse*

A risk averse customer might have the disutility function

$$\mathrm{DU}_{ra}(d(t)) = a_1 \exp(\alpha\, d(t)) - a_2$$

a_1, a_2 and α are constant coefficients. a_1 and α show how the patient tolerates his illness. a_2 shows the patient's tolerance toward the side effects of the treatment.

II. *Risk Prone*

A risk prone customer might have the disutility function

$$\mathrm{DU}_{rp}(d(t)) = b_2 - b_1 \exp(-\beta d(t))$$

b_1, b_2 and β are constant coefficients. b_1 and β show how the patient tolerates his illness. b_2 shows the patient's tolerance toward the side effects of the treatment.

III. *Risk Neutral*

A risk neutral customer might have the linear disutility function:

$$\mathrm{DU}_{rn}(d(t)) = c + \gamma\, d(t)$$

c and γ are constant coefficients. $d(t)$ in the above three equations denotes the difference between the stage at time t and the best stage, so $d(t) = M - \Phi(t)$. A greater $d(t)$ results in a greater value of DU.

Suppose this patient is a risk averse patient and his disutility function for interventions is $\mathrm{DU}(\mathrm{d}(t)) = 0.309 \exp(0.289 d(t)) + 2$.

This patient's expected disutility in 1.85 units of time after receiving the two interventions will be:

I.

$$EDU_1(d(1.85)) = \sum_{d=0}^{4} DU(d(1.85)) \Pr_1(d(1.85) = d) = 2.977.$$

II.

$$EDU_{II}(d(1.85)) = \sum_{d=0}^{4} DU(d(1.85)) \Pr_2(d(1.85) = d) = 2.829.$$

This calculation shows that this patient will have greater disutility at time 1.85 after receiving Intervention I. Therefore, from this patient's point of view, Intervention II should be a better choice for him at this time point.

28.5 Conclusions

The traditional binary-state reliability model is insufficient for many systems in the real world, and hence the multi-state reliability models are being developed to meet the needs for real applications.

In this chapter, the development of generic structure functions using equivalent classes and sets of lower/upper boundary points for the multi-state system with multi-state components are presented. The developed structure functions can be applied for general multi-state systems where the numbers of states for the system and for all of its components are different. With the developed structure functions, some multi-state reliability measures can be calculated, such as the probability that the system will be each possible state and the expected value of the state of the system given that the component-state probabilities are known. When the number of components and the state of components and the system increase, the computation of these measures will become time-consuming. Thus, the bounds for the expected

value of the state of the systems are crucial and are also presented here.

The transition of the states of the multi-state system is a stochastic process. The multi-state reliability measure, which is the probability that the system is in state k or higher at some point in time, is first derived using the most commonly used stochastic process, the Markov process. It is reasonable to believe that the probability that some systems degrade from one state to any lower state not only depends on the current state that the system is in but also on the time that the system enters in this state. Therefore, a general stochastic process, NHCTMP, is explored and used to model the degradation of the system. The age effect is considered when estimating the reliability measures using NHCTMP for a multi-state system. With the possible degradation models, the newly accumulated/integrated expected performance is derived and presented.

The development of a new customer-centered dynamic reliability measure that can capture the effect of system degradation on the customer's utility over time is another topic for this chapter. Because the variation of the performance of the system would lower the customer's utility, the integrated variance of the performance over time should be considered in the new customer-centered reliability measure. Utility functions used in portfolio (investment) risk analysis are incorporated with the stochastic models for this purpose.

The potential applications of the multi-state reliability model in infrastructure reliability and in the quality of life measure for patients with multi-stage diseases are also presented to demonstrate the usage of the reliability models described in this chapter.

References

[1] Andersen PK. Multi-state models in survival analysis: A study of nephropathy and mortality in diabetes. Statistics in Medicine 1988; 7: 661–670.

[2] Aven T, Jensen U. Stochastic models in reliability. Springer, New York, 1999.

[3] Barlow RE, Wu AS. Coherent systems with multistate components. Mathematics of Operations Research 1978; 3(4): 275–281.

[4] Bell MGH, Iida Y. Transportation network analysis. Wiley, New York, 1997.

[5] Boedigheimer R, Kapur KC. Customer driven reliability models for multistate coherent systems. IEEE Transactions on Reliability 1994; 43(1): 46–50.

[6] Boutsikas MV, Koutras MV. Generalized reliability bounds for coherent structures. Journal of Applied Probability 2000; 37: 778–794.

[7] Brunelle RD, Kapur KC. Customer-center reliability methodology. Proceedings of the Annual Reliability and Maintainability Symposium, IEEE, New Jersey, 1997; 286–292.

[8] Camerer CF. Recent tests of generalized expected utility theories. In: Edwards W, editor. Utility theories: Measurement and applications. Cambridge University Press, 1992.

[9] Chen A,Yang H, Lo HK, Tang WH. A capacity related teliability for transportation network. Journal of Advanced Transportation. 1999; 33: 183–200.

[10] Chen A, Yang H, Lo HK, Tang WH. Capacity reliability of a road network: An assessment methodology and numerical results. Transportation Research, Part B 2002; 36: 225–252.

[11] Chen P, Bernard EJ, Sen PK. A Markov chain model used in analyzing disease history applied to a stroke study. Journal of Applied Statistics 1999; 26(4): 413–422.

[12] Cowen ME, Chartrand M, Weitzel WF. A Markov model of the natural history of prostate cancer. Journal of Clinical Epidemiology 1994; 47(1): 3–21.

[13] Davis D, Holt C. Experimental economics. Princeton University Press 1993.

[14] Fossa S, Kaasa S, Calais da Silva F, Suciu S, Hengeveld M. Quality of life in prostate cancer patients. Prostate 1992; 4 (Suppl): 145–148.

[15] Fleming TR, Harrington DP. Counting process and survival analysis. Wiley, New York, 1991.

[16] Fowler FJ, Barry MJ, Lu-Yao G, Wasson J, Roman A, Wennberg J. Effect of radical prostatectomy for prostate cancer on patient quality of life: results from a Medicare survey. Urology 1995; 45(6): 905–1089.

[17] Ganz PA, Schag CAC, Lee JJ, Sim MS. The CARES: A generic measure of health-related quality of life for patients with cancer. Quality of Life Research 1992; 1: 19–29.

[18] Hudson JC, Kapur KC. Reliability analysis for multistate systems with multistate components. IIE Transactions 1983; 15(2): 127–135.

[19] Hudson JC, Kapur KC. Reliability bounds for multistate systems with multistate components. Operations Research 1985; 33(1): 153–160.

[20] Iida Y. Basic concepts and future directions of road network reliability analysis. Journal of Advanced Transportation 1999; 32: 125–134.

[21] Kapur KC, Lamberson LR. Reliability in engineering design, Wiley, New York, 1997.

[22] Kapur KC. Quality evaluation systems for reliability. Reliability Review 1986; June, 6(2).

[23] Kim M, Moon J, song H. Techniques improving the transmission reliability in high-rate wireless LANs. IEEE Transactions on Consumer Electronics 2004; 50: 64–72.

[24] Li D, Dolezal T, Haimes YY. Capacity reliability of water distribution networks. Reliability Engineering and System Safety 1993; 42: 29–38.

[25] Lisnianski A, Levitin G. Multi-state system reliability: assessment, optimization and application. World Scientific, Singapore, 2003.

[26] Litwin MS, Hays RD, Fink A, Ganz PA, Leake B, Leach GE, *et al*., Quality-of-life outcomes in men treated for localized prostate cancer. JAMA 1995; 273 (2): 129–135.

[27] Liu H, Ban J, Ran B, Mirchandani P. An analytical dynamic traffic assignment model with stochastic network and travelers' perceptions. Journal of Transportation Research Board 2002; 1783:125–133.

[28] Liu Y, Kapur KC. Reliability measures for dynamic multi-state systems and their applications for system design and evaluation. IIE Transactions 2006;38(6): 511–520.

[29] McClean S, Montgomery E, Ugwuowo F. Non-Homogeneous continuous-time Markov and semi-Markov manpower models. Applied Stochastic Models and Data Analysis 1998;13:191–198.

[30] Natvig B. Two suggestions of how to define a multistate coherent system. Advanced Applied Probability 1982; 14: 434-455.

[31] Natvig B, March HWH. An application of multistate reliability theory to an offshore gas pipeline network. International Journal of Reliability, Quality and Safety Engineering 2003;10:361–381.

[32] Nicholson W. Microeconomics theory: Basic principles and extensions, 7th edition, Dryden Press, Harcourt Brace College Publishers, 1998.

[33] Ross SM. Multivalued state component systems. The Annals of Probability 1979; 7(2):379–383.

[34] Ross SM. Stochastic processes, 2nd edition, Wiley, 1996.

[35] Sargent TJ. Macroeconomics theory, 2nd edition, Academic Press, New York, 1987.

[36] Satitsatian S, Kapur KC. Multi-state reliability model for the evaluation of supply chain network. Proceedings of the International Conference on Manufacturing Excellence, Melboune, Australia, Oct. 13–15, 2003.

[37] Satitsatian S, Kapur KC. Performance evaluation of infrastructure networks with multi-state reliability analysis. International Journal of Performability Engineering 2006; 2(2): 103–121.

[38] Satitsatian S, Kapur KC. An algorithm for lower reliability bounds of multistate two-terminal networks. IEEE Transactions of Reliability 2006; 55(2): 199–206.

[39] Sharp JW. Expanding the definition of quality of life for prostate cancer. Cancer 1993; 71 (Suppl): 1078–1082.

[40] Shooman, M.L. Reliability of computer systems and networks : fault tolerance, analysis and design, Wiley, New York, 2002.

[41] Song, J. and Kiureghian, A.D. Bounds on system reliability by linear programming. Journal of Engineering Mechanics. ASCE. 2003; 129(6), 627–636.

[42] Steinberg GD, Bales GT, Brendler CB. An analysis of watchful waiting for clinically localized prostate cancer. Journal of Urology. 1998; 159(5):1431–1436.

[43] Tatineni M, Boyce DE, Mirchandani P. Comparisons of deterministic and stochastic traffic loading models. Transportation Research Record 1997; 1607: 16–23.

[44] Vassiliou P-CG. The evolution of the theory of non-homogeneous Markov system. Applied Stochastic Models and Data Analysis. 1998; 13: 159–176.

[45] Xu C, Goulter IC. Reliability-based optimal design of water distribution networks. Journal of Water Resources Planning and Management 1999; 125: 352–362.

[46] Xue J, Yang K. Dynamic reliability analysis of coherent multistate systems. IEEE Transactions on Reliability 1995; 44(4): 683–688.

[47] Yang K, Xue J. Dynamic reliability measures and life distribution models for multistate systems. Internaltional Journal of Reliability, Quality and Safety Engineering 1995; 2(1): 79–102.

29

A Universal Generating Function in the Analysis of Multi-state Systems

Gregory Levitin

The Israel Electric Corporation Ltd., P.O. Box 10, Haifa, 31000 Israel

Abstract: Almost all work in reliability theory is based on the traditional binary concept of reliability models allowing only two possible states for a system and its components, *viz*, perfect functionality or complete failure. However, many real-world systems are composed of multi-state components, which have different performance levels and several failure modes with various effects on the system's entire performance. Such systems are called multi-state systems (MSS). For MSS, the outage effect will be essentially different for units with different performance rates. Therefore, the reliability analysis of MSS is much more complex when compared with binary-state systems. The recently emerged universal generating function (UGF) technique allows one to find the entire MSS performance distribution based on the performance distributions of its elements by using algebraic procedures. This chapter presents the generalized reliability block diagram method based on UGF and its combination with random processes methodology for evaluating the reliability of different types of MSS.

29.1 Introduction

Most works on reliability theory are devoted to traditional binary reliability models allowing only two possible states for a system and its components: perfect functionality and complete failure. However many real-world systems are composed of multi-state components, which have different performance levels and several failure modes with various effects on the system's entire performance. Such systems are called multi-state systems (MSS) [1]. Examples of MSS are power systems or computer systems where the component performance is characterized by the generating capacity or the data processing speed, respectively. For MSS, the outage effect will be essentially different for units with different performance rates. Therefore, the reliability analysis of MSS is much more complex when compared with binary-state systems. In real-world problems of MSS reliability analysis, the great number of system states that need to be evaluated makes it difficult to use traditional binary reliability techniques.

The recently emerged universal generating function (UGF) technique allows one to find the entire MSS performance distribution based on the performance distributions of its elements by using algebraic procedures. This technique generalizes the method that is based on using a well-known ordinary generating function. The basic ideas of the method were introduced by Professor I. Ushakov in the mid 1980s [2]. Since then, the method has been considerably expanded [3, 4].

The UGF approach is straightforward. It is based on intuitively simple recursive procedures and provides a systematic method for the system

states' enumeration that can replace extremely complicated combinatorial algorithms used for enumerating the possible states in some special types of system (such as consecutive systems or networks).

The UGF approach is effective. Combined with simplification techniques, it allows the system's performance distribution to be obtained in a short time. The computational burden is the crucial factor when one solves optimization problems where the performance measures have to be evaluated for a great number of possible solutions along the search process. This makes using the traditional methods in reliability optimization problematic. On the contrary, the UGF technique is fast enough to be implemented in optimization procedures.

The UGF approach is universal. An analyst can use the same recursive procedures for systems with a different physical nature of performance and different types of element interaction.

This approach enables one to obtain the performance distribution of complex MSS using a generalized reliability block diagram method (recursively aggregating multi-state elements and their replacement by single equivalent element).

Nomenclature

RBD	reliability block diagram
MSS	multi-state system
u-function	universal generating function
pmf	probability mass function
$\Pr\{e\}$	probability of event e
$E[X]$	expected value of X
$1(x)$	unity function: $1(\text{TRUE}) = 1$, $1(\text{FALSE}) = 0$
n	number of system elements
G_j	random performance of system element j
$\boldsymbol{g}_j$	set of possible realizations of G_j
g_{jh}	hth realization of G_j
p_{jh}	$\Pr\{G_j = g_{jh}\}$
V	random system performance
v_i	ith realization of V
q_i	$\Pr\{V = v_i\}$
ϕ	system structure function: $V=\phi(G_1,\ldots,G_n)$
θ	system demand
$f(V,\theta)$	acceptability function
$R(\theta)$	system reliability: $\Pr\{f(V, \theta^*)=1\}$
$W(\theta)$	conditional expected system performance
$u_j(z)$	u-function representing pmf of G_j
$U(z)$	u-function representing pmf of V
$\otimes_\varphi$	composition operator over u-functions
$\varphi(G_i,G_j)$	function representing performance of pair of elements

29.2 The RBD Method for MSS

29.2.1 A Generic Model of Multi-state Systems

In order to analyze MSS behavior one has to know the characteristics of its elements. Any system element j can have k_j+1 different states corresponding to the performance rates, represented by the set $\boldsymbol{g}_j=\{g_{j0}, g_{j1},\ldots, g_{jk_j}\}$, where g_{jh} is the performance rate of element j in the state h, $h \in \{0, 1, \ldots, k_j\}$. The performance rate G_j of element j at any time instant is a random variable that takes its values from $\boldsymbol{g}_j$: $G_j \in \boldsymbol{g}_j$. The probabilities associated with the different states (performance rates) of the system element j can be represented by the set

$$\boldsymbol{p}_j = \{p_{j0}, p_{j1},\ldots, p_{jk_j}\}, \qquad (29.1)$$

where

$$p_{jh} = \Pr\{G_j = g_{jh}\}. \qquad (29.2)$$

Since the element's states compose the complete group of mutually exclusive events (meaning that the element can always be in one and only in one of k_j+1 states)

$$\sum_{h=0}^{k_j} p_{jh} = 1. \qquad (29.3)$$

Expression (29.2) defines the *pmf* of a discrete random variable G_j. The collection of pairs g_{jh}, p_{jh}, $h = 0, 1,\ldots, k_j$, completely determines the performance distribution of element j.

When the MSS consists of n independent elements, its performance rate is unambiguously determined by the performance rates of these elements. At each moment, the system elements have certain performance rates corresponding to

their states. The state of the entire system is determined by the states of its elements. Assume that the entire system has K+1 different states and that v_i is the entire system performance rate in state $i \in \{0, \ldots, K\}$. The MSS performance rate is a random variable V that takes values from the set $M=\{v_1, \ldots, v_K\}$.

Let $L^n = \{g_{10},\ldots, g_{1k_1}\}\times\ldots\times\{g_{n0},\ldots, g_{nk_n}\}$ be the space of possible combinations of performance rates for all of the system elements and $M = \{v_0, \ldots, v_K\}$ be the space of possible values of the performance rate for the entire system. The transform $\phi(G_1,\ldots,G_n): L^n \to M$, which maps the space of the elements' performance rates into the space of system's performance rates, is named the system structure function.

The generic model of the MSS includes the *pmf* of performances for all of the system elements and system structure function [1]:

$$\boldsymbol{g}_j, \boldsymbol{p}_j, 1 \le j \le n, \tag{29.4}$$

$$V = \phi(G_1,\ldots,G_n). \tag{29.5}$$

From this model one can obtain the *pmf* of the entire system performance in the form

$$q_i, v_i, 0 \le i \le K, \text{ where } q_i = \Pr\{V = v_i\}. \tag{29.6}$$

The acceptability of system state can usually be defined by the acceptability function $f(V,\theta)$ representing the desired relation between the system performance V and some limit value θ named system demand ($f(V,\theta) = 1$, if the system performance is acceptable and $f(V, \theta) = 0$, otherwise). The MSS reliability is defined as its expected acceptability (the probability that the MSS satisfies the demand) [5]. Having the system *pmf* (29.6) one can obtain its reliability as

$$R(\theta) = E[f(V,\theta)] = \sum_{i=1}^{K} q_i f(v_i,\theta). \tag{29.7}$$

For example, in applications where the system performance is defined as a task execution time and θ is the maximum allowed task execution time, (29.7) takes the form

$$R(\theta) = \sum_{i=1}^{K} q_i 1(v_i < \theta), \tag{29.8}$$

in applications where the system performance is defined as system productivity (capacity) and θ is the minimum allowed productivity, (29.7) takes the form

$$R(\theta) = \sum_{i=1}^{K} q_i 1(v_i > \theta). \tag{29.9}$$

For repairable systems, (29.7)–(29.9) can be used for evaluating system availability.

Another important measure of system performance is the conditional expected performance $W(\theta)$. This index determines the system's expected performance given that the system is in acceptable states. It can be obtained as

$$W(\theta) = E[V \mid f(V,\theta) = 1] = \sum_{i=1}^{K} q_i v_i f(v_i,\theta) / R(\theta). \tag{29.10}$$

For some systems an unconditional expected performance $W = E[V] = \sum_{i=1}^{K} q_i v_i$ is of interest.

In order to calculate the indices $R(\theta)$ and $W(\theta)$, one has to obtain the *pmf* of the MSS random performance in the form (29.6) from the model (29.4) and (29.5). The RBD method for obtaining the MSS performance distribution is based on the universal generating function (u-function) technique, which was introduced in [2] and has proven to be very effective for the reliability evaluation of different types of multi-state systems [3, 4].

29.2.2 Universal Generating Function (u-function) Technique

The u-function representing the *pmf* of a discrete random variable Y_j is defined as a polynomial

$$u_j(z) = \sum_{h=0}^{k_j} \alpha_{jh} z^{y_{jh}}, \tag{29.11}$$

where the variable Y_j has k_j+1 possible values and $\alpha_{jh} = \Pr\{Y_j = y_{jh}\}$.

To obtain the u-function representing the *pmf* of a function of n independent random variables $\varphi(Y_1, \ldots, Y_n)$ the following composition operator is used:

$$U(z)=\underset{\varphi}{\otimes}(u_1(z),...,u_n(z))$$

$$=\underset{\varphi}{\otimes}\Big(\sum_{h_1=0}^{k_1}\alpha_{1h_1}z^{y_{1h_1}},...,\sum_{h=0}^{k_n}\alpha_{nh_n}z^{y_{nh_n}}\Big)$$

$$=\sum_{h_1=0}^{k_1}\sum_{h_2=0}^{k_2}...\sum_{h_n=0}^{k_n}\left(\prod_{i=0}^{n}\alpha_{ih_i}z^{\varphi(y_{1h_1},...,y_{nh_n})}\right) \quad (29.12)$$

The polynomial $U(z)$ represents all of the possible mutually exclusive combinations of realizations of the variables by relating the probabilities of each combination to the value of function $\varphi(Y_1, ..., Y_n)$ for this combination.

In the case of MSS u-functions

$$u_j(z)=\sum_{h_j=0}^{k_j}p_{jh_j}z^{g_{jh_j}} \quad (29.13)$$

represent the pmf of random performances of independent system elements. Having a generic model of an MSS in the form of (29.4) and (29.5), one can obtain the measures of system performance by applying the following steps:

1. Represent the *pmf* of the random performance of each system element j in the form of the u-function (29.13).
2. Obtain the u-function of the entire system $U(z)$ which represents the *pmf* of the random variable V by applying the composition operator $\underset{\phi}{\otimes}$ that uses the system structure function ϕ using (29.5).
3. Calculate the MSS performance indices applying (29.7) and (29.10) over system performance *pmf* (29.6) represented by the u-function $U(z)$.

While steps 1 and 3 are rather trivial, step 2 may involve complicated computations. Indeed, the derivation of a system structure function for various types of system is usually a difficult task. As shown in [4], representing the structure functions in the recursive form is beneficial from both the derivation clarity and computational simplicity viewpoints. In many cases, the structure function of the entire MSS can be represented as the composition of the structure functions corresponding to some subsets of the system elements (MSS subsystems).

The u-functions of the subsystems can be obtained separately and the subsystems can be further treated as single equivalent elements with the performance *pmf* represented by these u-functions. The method for distinguishing recurrent subsystems and replacing them with single equivalent elements is based on a graphical representation of the system structure and is referred to as the RBD method. This approach is usually applied to systems with a complex series-parallel configuration.

29.2.3 Generalized RBD Method for Series-parallel MSS

The structure function of complex series-parallel system can always be represented as composition of the structure functions of statistically independent subsystems containing only elements connected in a series or in parallel. Therefore, in order to obtain the u-function of a series-parallel system one has to apply the composition operators recursively in order to obtain u-functions of the intermediate pure series or pure parallel structures. The following algorithm realizes this approach:

1. Find any pair of system elements (i and j) connected in parallel or in series in the MSS.
2. Obtain the u-function of this pair using the corresponding composition operator $\underset{\varphi}{\otimes}$ over two u-functions of the elements:

$$U_{\{i,j\}}(z)=u_i(z)\underset{\varphi}{\otimes}u_j(z)$$

$$=\sum_{h_i=0}^{k_i}\sum_{h_j=0}^{k_j}p_{ih_i}p_{jh_j}z^{\varphi(g_{ih_i},g_{jh_j})}, \quad (29.14)$$

where the function φ is determined by the nature of interaction between elements' performances.

3. Replace the pair with single element having the u-function obtained in step 2.
4. If the MSS contains more than one element return to step 1.

The resulting u-function represents the performance distribution of the entire system.

The choice of the functions φ for series and parallel subsystems depends on the type of system.

For example, in flow transmission MSS, where performance is defined as capacity or productivity, the total capacity of a subsystem containing two independent elements connected in series is equal to the capacity of a bottleneck element (the element with least performance). Therefore, the structure function for such a subsystem takes the form

$$\phi_{\text{ser}}(G_1, G_2) = \min\{G_1, G_2\}. \quad (29.15)$$

If the flow can be dispersed and transferred by parallel channels simultaneously (which provides load sharing), the total capacity of a subsystem containing two independent elements connected in parallel is equal to the sum of the capacities of these elements. Therefore, the structure function for such a subsystem takes the form

$$\phi_{\text{par}}(G_1, G_2) = G_1 + G_2. \quad (29.16)$$

In task processing MSS, where the performance of each element is characterized by its processing speed, different subtasks are performed by different components consecutively. Therefore the time of the entire task completion (reciprocal of the processing speed) is equal to the sum of subtask execution times. In the terms of the processing speeds, one can determine the performance of a subsystem consisting of two consecutive elements as

$$\varphi_{ser}(G_1,G_2)=\text{inv}\,(G_1,G_2) = \frac{1}{1/G_1 + 1/G_2} = \frac{G_1 G_2}{G_1 + G_2}. \quad (29.17)$$

Parallel elements perform the same task starting it simultaneously. The task is completed by a group of elements when it is completed by any element belonging to this group. Therefore, the performance of the group is equal to the performance of its fastest available element. Therefore, for a subsystem of two parallel elements

$$\phi_{\text{par}}(G_1, G_2) = \max\{G_1, G_2\}. \quad (29.18)$$

Example 1

In order to illustrate the reliability block diagram method consider the series-parallel system presented in Figure 29.1A.

First, one can replace series subsystem consisting of elements with the u-functions $u_2(z)$ and $u_3(z)$ with single equivalent element having u-function $[u_2(z) \underset{\phi_{\text{ser}}}{\otimes} u_3(z)]$. By replacing this new element and element with the u-functions $u_4(z)$ with the element having u-function $U_1(z)=[u_2(z) \underset{\phi_{\text{ser}}}{\otimes} u_3(z)] \underset{\phi_{\text{ser}}}{\otimes} u_4(z)$ one obtains a system with the structure presented in Figure 29.1B. This system contains a purely parallel subsystem consisting of elements with the u-functions $U_1(z)$ and $u_5(z)$, which in their turn can be replaced by a single element with the u-function $U_2(z) = U_1(z) \underset{\phi_{\text{par}}}{\otimes} u_5(z)$ (Figure 29.1C). The structure obtained has three elements connected in a series that can be replaced with a single element having the u-function $U_3(z) = [u_1(z) \underset{\phi_{\text{ser}}}{\otimes} U_2(z)] \underset{\phi_{\text{ser}}}{\otimes} u_6(z)$ (Figure 29.1D). The resulting structure contains two elements connected in parallel. The u-function of this structure representing the *pmf* of the entire MSS performance is obtained as $U(z) = U_3(z) \underset{\phi_{\text{par}}}{\otimes} u_7(z)$.

Assume that in the series-parallel system presented in Figure 29.1A all of the system elements can have two states (elements with total failure) and have the parameters presented in Table 29.1.

Each element j has a nominal performance rate g_{j1} in working state and performance rate of zero when it fails. The probability that element j is in working state is p_{j1}.

The process of calculating $U(z)$ for the flow transmission system (for which ϕ_{ser} and ϕ_{par} functions are defined by (29.15) and (29.16), respectively) is as follows:

$$u_2(z) \underset{\min}{\otimes} u_3(z) = (0.8z^3+0.2z^0) \underset{\min}{\otimes} (0.9z^5+0.1z^0)$$
$$= 0.72z^3+0.28z^0;$$
$$U_1(z) = (u_2(z) \underset{\min}{\otimes} u_3(z)) \underset{\min}{\otimes} u_4(z)$$
$$= (0.72z^3+0.28z^0) \underset{\min}{\otimes} (0.7z^4+0.3z^0)$$
$$= 0.504z^3+0.496z^0;$$
$$U_2(z) = U_1(z) \underset{+}{\otimes} u_5(z)$$

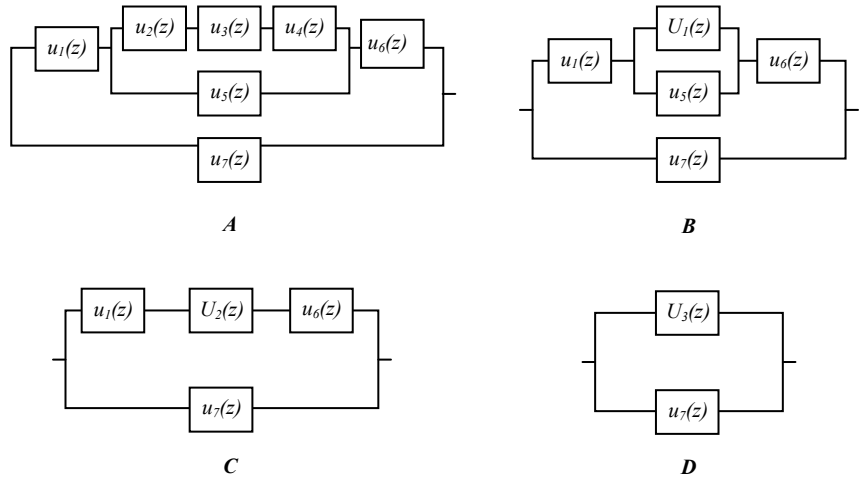


Figure 29.1. Example of RBD method

$= (0.504z^3+0.496z^0) \underset{+}{\otimes} (0.6z^3+0.4z^0)$

$= 0.3024z^6+0.4992z^3+0.1984z^0;$

$u_1(z) \underset{\min}{\otimes} U_2(z) = (0.9z^5+0.1z^0) \underset{\min}{\otimes} (0.3024z^6$

$+0.4992z^3+0.1984z^0)$

$= 0.27216z^5+0.44928z^3+0.27856z^0;$

$U_3(z)=(u_1(z) \underset{\min}{\otimes} U_2(z)) \underset{\min}{\otimes} u_6(z) = (0.27216z^5$

$+0.44928z^3+0.27856z^0) \underset{\min}{\otimes} (0.8z^6+0.2z^0)$

$= 0.217728z^5+0.359424z^3+0.422848z^0;$

$U(z) = U_3(z) \underset{+}{\otimes} u_7(z) = (0.217728z^5+0.359424z^3$

$+0.422848z^0) \underset{+}{\otimes} (0.8z^3+0.2z^0) = 0.1741824z^8$

$+0.2875392z^6+0.0435456z^5+0.4101632z^3$

$+0.0845696z^0.$

Having the system *u*-function that represents its performance distribution one can easily obtain the system expected performance $W = 4.567$. The system reliability for different demand levels can be obtained by applying (29.9) over the system *pmf* represented by the *u*-function $U(z)$:

$R(\theta) = 0.91543$ for $0 < \theta \le 3$;
$R(\theta) = 0.50527$ for $3 < \theta \le 5$;
$R(\theta) = 0.461722$ for $5 < \theta \le 6$;
$R(\theta) = 0.174182$ for $6 < \theta \le 8$;
$R(\theta) = 0$ for $\theta > 8$

The process of calculating $U(z)$ for the task processing system (for which ϕ_{ser} and ϕ_{par} functions are defined by (29.17) and (29.18), respectively) is as follows:

$u_2(z) \underset{\text{inv}}{\otimes} u_3(z)=(0.8z^3+0.2z^0) \underset{\text{inv}}{\otimes} (0.9z^5+0.1z^0)$

$= 0.72z^{1.875}+0.28z^0;$

$U_1(z) = (u_2(z) \underset{\text{inv}}{\otimes} u_3(z)) \underset{\text{inv}}{\otimes} u_4(z)$

$= (0.72z^{1.875}+0.28z^0) \underset{\text{inv}}{\otimes} (0.7z^4+0.3z^0)$

$= 0.504z^{1.277}+0.496z^0;$

$U_2(z)= U_1(z) \underset{\max}{\otimes} u_5(z))$

Table 29.1. Parameters of elements of a series-parallel system

j	1	2	3	4	5	6	7
g_{j1}	5	3	5	4	2	6	3
p_{j1}	0.9	0.8	0.9	0.7	0.6	0.8	0.8

$= (0.504z^{1.277}+0.496z^0) \underset{\max}{\otimes} (0.6z^2+0.4z^0)$

$= 0.6z^2+0.2016z^{1.277}+0.1984z^0;$

$u_1(z) \underset{\text{inv}}{\otimes} U_2(z)=(0.9z^5+0.1z^0) \underset{\text{inv}}{\otimes}$

$(0.6z^2+0.2016z^{1.277}+0.1984z^0)$

$= 0.54z^{1.429}+0.18144z^{1.017}+0.27856z^0;$

$U_3(z) = (u_1(z) \underset{\text{inv}}{\otimes} U_2(z)) \underset{\text{inv}}{\otimes} u_6(z)$

$=(0.54z^{1.429}+0.18144z^{1.017}+0.27856z^0) \underset{\text{inv}}{\otimes}$

$(0.8z^6+0.2z^0) = 0.432z^{1.154}+0.145152z^{0.87}$

$+0.422848z^0;$

$U(z) = U_3(z) \underset{\max}{\otimes} u_7(z) = (0.432z^{1.1}$

$+0.145152z^{0.87}+0.422848z^0) \underset{\max}{\otimes} (0.8z^3+0.2z^0)$

$= 0.8z^3+0.0864z^{1.154}+0.0290304z^{0.87}$

$+0.08445696z^0.$

The main performance measures of this system are:

$W = 2.549;$

$R(\theta) = 0.91543$ for $0 < \theta \le 0.87,$

$R(\theta) = 0.8864$ for $0.87 < \theta \le 1.429$;

$R(\theta) = 0.8$ for $1.429 < \theta \le 3;$

$R(\theta) = 0$ for $\theta > 3.$

The procedure described above recursively obtains the same MSS u-function that can be obtained directly by the operator

$$\underset{\phi}{\otimes}(u_1(z),u_2(z),u_3(z),u_4(z),u_5(z))$$

using the following structure function: $\phi(G_1, G_2, G_3, G_4, G_5, G_6, G_7) = \phi_{\text{par}}(\phi_{\text{ser}}(G_1, \phi_{\text{par}}(\phi_{\text{ser}}(G_2, G_3, G_4), G_5), G_6), G_7)$. The recursive procedure for obtaining the MSS u-function is not only more convenient than the direct one, but, and much more importantly, it allows one to reduce the computational burden of the algorithm considerably. Indeed, using the direct procedure corresponding to (29.12) one has to evaluate the system structure function for each combination of values of random variables $G_1,...,G_7$ ($\prod_{j=1}^{7} k_j$ times, where k_j is the number of states of element j). Using the recursive algorithm one can take advantage of the fact that some subsystems have the same performance rates in different states, which makes these states indistinguishable and reduces the total number of terms in the corresponding u-functions.

In our example, the number of evaluations of the system structure function using directly (29.12) for the system with two-state elements is $2^7 = 128$. Each evaluation requires calculating a function of seven arguments. Using the reliability block diagram method one obtains the system u-function just by 30 procedures of structure function evaluation (each procedure requires calculating simple functions of just two arguments). This is possible because of the reduction in the lengths of intermediate u-functions by the collection of like terms. For example, it can be easily seen that in the subsystem of elements 2, 3 and 4 all eight possible combinations of the elements' states produce just two different values of the subsystem performance: 0 and min (g_{21}, g_{31}, g_{41}) in the case of the flow transmission system, or 0 and $g_{21}g_{31}g_{41}/(g_{21}g_{31}+g_{21}g_{41}+g_{31}g_{41})$ in the case of the task processing system. After obtaining the u-function $U_1(z)$ for this subsystem and collecting like terms one obtains a two-term equivalent u-function that is used further in the recursive algorithm. Such a simplification is impossible when the entire expression (29.12) is used.

29.3 Combination of Random Processes Methods and the UGF Technique

In many cases the state probability distributions of system elements are unknown whereas the state transition rates (failure and repair rates) can be easily evaluated from history data or mathematical models. The Markov process theory allows the analyst to obtain the probability of any system state at any time solving a system of differential equations.

The main difficulty of applying the random processes methods to the MSS reliability evaluation is the "dimension damnation". Indeed, the number of differential equations in the system that should be solved using the Markov approach is equal to the total number of MSS states (product of numbers of states of all of the system elements). This number can be very large even for a relatively

small MSS. Even though the modern software tools provide solutions for high-order systems of differential equations, building the state-space diagram and deriving the corresponding system of differential equations is a difficult non-formalized process that may cause numerous mistakes.

The UGF-based reliability block diagram technique can be used for reducing the dimension of system of equations obtained by the random process method. The main idea of the approach lies in solving the separated smaller systems of equations for each MSS element and then combining the solutions using the UGF technique in order to obtain the dynamic behavior of the entire system. The approach not only separates the equations but also reduces the total number of equations to be solved

The basic steps of the approach are as follows:

1. Build the random process Markov model for each MSS element (considering only state transitions within this element). Obtain two sets $\boldsymbol{g}_j=\{g_{j1},g_{j2},\ldots,g_{jk_j}\}$ and $\boldsymbol{p}_j(t)=\{p_{j1}(t),p_{j2}(t),\ldots,p_{jk_j}(t)\}$ for each element j $(1\le j\le n)$ by solving the system of k_j ordinary differential equations. Note that instead of solving one high-order system of $\prod_{j=1}^{n}k_j$ equations one has to solve n low-order systems with the total number of equations $\sum_{j=1}^{n}k_j$.

2. Having the sets $\boldsymbol{g}_j$ and $\boldsymbol{p}_j(t)$ for each element j define u-function of this element in the form $u_j(z)=p_{j1}(t)z^{g_{j1}}+p_{j2}(t)z^{g_{j2}}+\ldots+p_{jk_j}(t)z^{g_{jk_j}}$.

3. Using the generalized RBD method, obtain the resulting u-function for the entire MSS.

4. Apply the operators (29.7) and (29.10) over the system *pmf* represented by the resulting u-function to obtain the main MSS reliability indices.

Example 2

Consider a flow transmission system (Figure 29.2) consisting of three pipes [1]. The oil flow is transmitted from point A to point B. The pipes performance is measured by their transmission

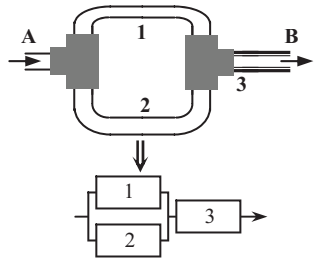


Figure 29.2. Simple flow transmission MSS

capacity (ton per minute). Elements 1 and 2 are binary. A state of total failure for both elements corresponds to a transmission capacity of 0 and the operational state corresponds to the capacities of the elements 1.5 and 2 tons per minute, respectively, so that $G_1(t)\in\{0,1.5\}$, $G_2(t)\in\{0,2\}$. Element 3 can be in one of three states: a state of total failure corresponding to a capacity of 0, a state of partial failure corresponding to a capacity of 1.8 tons per minute and a fully operational state with a capacity of 4 tons per minute so that $G_3(t)\in\{0,1.8,4\}$. The demand is constant: $\theta = 1.0$ ton per minute.

The system output performance rate $V(t)$ is defined as the maximum flow that can be transmitted between nodes A and B. In accordance with (29.15) and (29.16), $V(t)=\min\{G_1(t)+G_2(t),G_3(t)\}$.

The state-space diagrams of the system elements are presented in Figure 29.3. The failure rates and repair rates corresponding to these two elements are

$\lambda_{2,1}^{(1)}=7\,year^{-1},\mu_{1,2}^{(1)}=100\,year^{-1}$ for element 1,

$\lambda_{2,1}^{(2)}=10\,year^{-1},\mu_{1,2}^{(2)}=80\,year^{-1}$ for element 2.

Element 3 is a multi-state element with only minor failures and minor repairs. The failure rates and repair rates corresponding to element 3 are

$\lambda_{3,2}^{(3)}=10\,year^{-1},\lambda_{3,1}^{(3)}=0,\lambda_{2,1}^{(3)}=7\,year^{-1},$

$\mu_{1,3}^{(3)}=0,\mu_{1,2}^{(3)}=120\,year^{-1},\mu_{2,3}^{(3)}=110\,year^{-1}.$

According to the classical Markov approach one has to enumerate all the system states corresponding to different combinations of all possible states of system elements (characterized

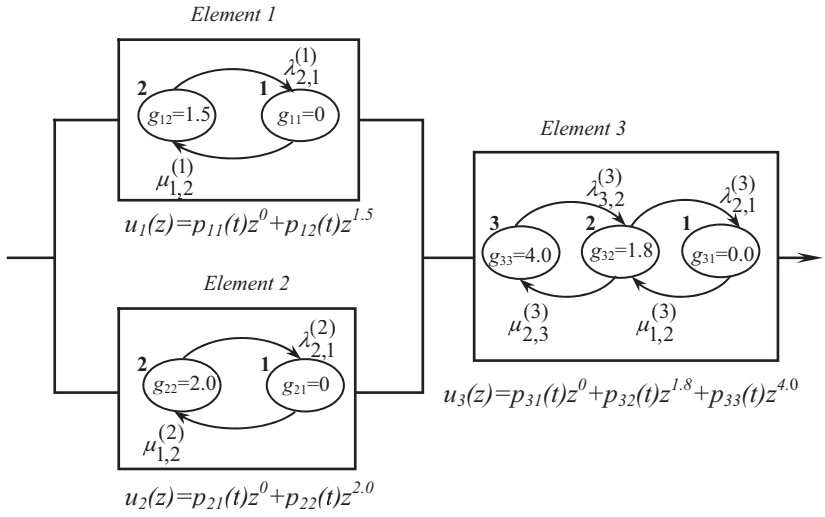


Figure 29.3. State-space diagrams and *u*-functions of system elements

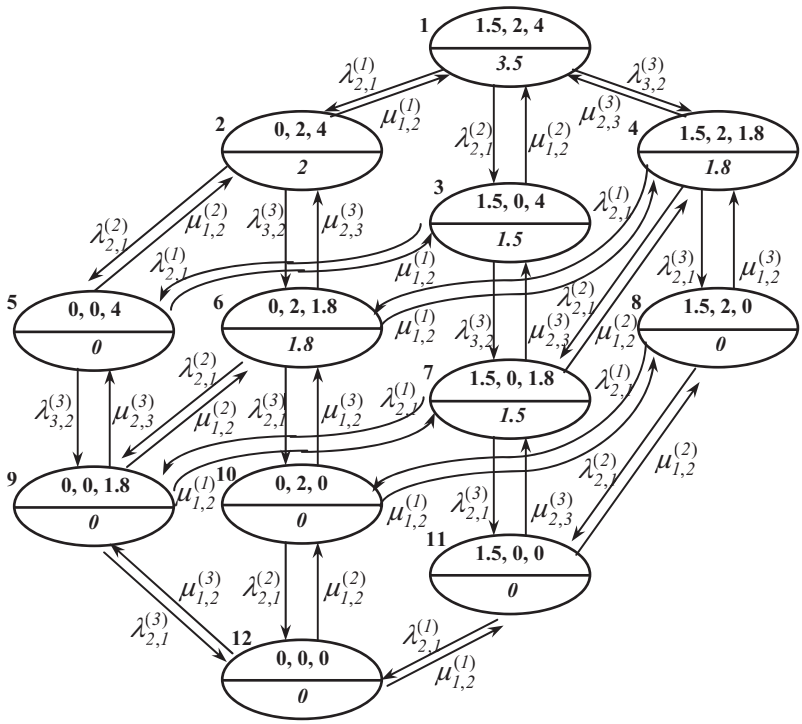


Figure 29.4. State-space diagram for the entire system

by their performance levels). The total number of different system states is $K = k_1k_2k_3 = 2*2*3 = 12$. The state-space diagram of the system is presented in Figure 29.4 (in this diagram the vector of element performances for each state and the corresponding system performance are presented, respectively in the upper and lower parts of the ellipses).

Then the state transition analysis should be performed for all pairs of system states. For example, for the state number 2 where states of the elements are $\{g_{11},g_{22},g_{33}\}=\{2,4,2\}$ the transitions to states 1, 5 and 6 exist with the intensities $\mu_{1,2}^{(1)}, \lambda_{2,1}^{(2)}, \lambda_{3,2}^{(3)}$, respectively.

The corresponding system of differential equations for the state probabilities $p_i(t)$, $2 \le i \le 12$ takes the form:

$$\frac{dp_1(t)}{dt} = -(\lambda_{2,1}^{(1)} + \lambda_{2,1}^{(2)} + \lambda_{3,2}^{(3)})p_1(t) + \mu_{1,2}^{(1)}p_2(t) + \mu_{1,2}^{(2)}p_3(t) + \mu_{2,3}^{(3)}p_4(t),$$

$$\frac{dp_2(t)}{dt} = \lambda_{2,1}^{(1)}p_1(t) - (\mu_{1,2}^{(1)} + \lambda_{2,1}^{(2)} + \lambda_{3,2}^{(3)})p_2(t) + \mu_{1,2}^{(2)}p_5(t) + \mu_{2,3}^{(3)}p_6(t),$$

$$\frac{dp_3(t)}{dt} = \lambda_{2,1}^{(2)}p_1(t) - (\mu_{1,2}^{(2)} + \lambda_{2,1}^{(1)} + \lambda_{3,2}^{(3)})p_3(t) + \mu_{1,2}^{(1)}p_5(t) + \mu_{2,3}^{(3)}p_7(t),$$

$$\frac{dp_4(t)}{dt} = \lambda_{2,3}^{(3)}p_1(t) - (\mu_{2,3}^{(3)} + \lambda_{2,1}^{(1)} + \lambda_{2,1}^{(2)} + \lambda_{2,1}^{(3)})p_4(t) + \mu_{1,2}^{(1)}p_6(t) + \mu_{1,2}^{(2)}p_7(t) + \mu_{1,2}^{(3)}p_8(t),$$

$$\frac{dp_5(t)}{dt} = \lambda_{2,1}^{(2)}p_2(t) + \lambda_{2,1}^{(1)}p_3(t) - (\mu_{1,2}^{(2)} + \mu_{1,2}^{(1)} + \lambda_{3,2}^{(3)})p_5(t) + \mu_{2,3}^{(3)}p_9(t),$$

$$\frac{dp_6(t)}{dt} = \lambda_{3,2}^{(3)}p_2(t) + \lambda_{2,1}^{(1)}p_4(t) - (\mu_{2,3}^{(3)} + \mu_{1,2}^{(1)} + \lambda_{2,1}^{(2)} + \lambda_{2,1}^{(3)})p_6(t) + \mu_{1,2}^{(2)}p_9(t) + \mu_{1,2}^{(3)}p_{10}(t),$$

$$\frac{dp_7(t)}{dt} = \lambda_{3,2}^{(3)}p_3(t) + \lambda_{2,1}^{(1)}p_4(t) - (\mu_{2,3}^{(3)} + \mu_{1,2}^{(2)} + \lambda_{2,1}^{(1)} + \lambda_{2,1}^{(3)})p_7(t) + \mu_{1,2}^{(1)}p_9(t) + \mu_{1,2}^{(3)}p_{11}(t),$$

$$\frac{dp_8(t)}{dt} = \lambda_{2,1}^{(3)}p_4(t) - (\mu_{1,2}^{(3)} + \lambda_{2,1}^{(1)} + \lambda_{2,1}^{(2)})p_8(t) + \mu_{1,2}^{(1)}p_{10}(t) + \mu_{1,2}^{(2)}p_{11}(t),$$

$$\frac{dp_9(t)}{dt} = \lambda_{3,2}^{(3)}p_5(t) + \lambda_{2,1}^{(2)}p_6(t) + \lambda_{2,1}^{(1)}p_7(t) - (\mu_{2,3}^{(3)} + \mu_{1,2}^{(2)} + \mu_{1,2}^{(1)} + \lambda_{2,1}^{(3)})p_9(t) + \mu_{1,2}^{(1)}p_{10}(t) + \mu_{1,2}^{(3)}p_{12}(t),$$

$$\frac{dp_{10}(t)}{dt} = \lambda_{2,1}^{(3)}p_6(t) + \lambda_{2,1}^{(1)}p_8(t) - (\mu_{1,2}^{(3)} + \mu_{1,2}^{(1)} + \lambda_{2,1}^{(2)})p_{10}(t) + \mu_{1,2}^{(2)}p_{12}(t),$$

$$\frac{dp_{11}(t)}{dt} = \lambda_{2,1}^{(3)}p_7(t) + \lambda_{2,1}^{(2)}p_8(t) - (\mu_{1,2}^{(3)} + \mu_{1,2}^{(2)} + \lambda_{2,1}^{(1)})p_{11}(t) + \mu_{1,2}^{(1)}p_{12}(t),$$

$$\frac{dp_{12}(t)}{dt} = \lambda_{2,1}^{(3)}p_9(t) + \lambda_{2,1}^{(2)}p_{10}(t) + \lambda_{2,1}^{(1)}p_{11}(t) - (\mu_{1,2}^{(3)} + \mu_{1,2}^{(2)} + \mu_{1,2}^{(1)})p_{12}(t).$$

Solving this system with the initial conditions $p_1(0) = 1$, $p_i(0) = 0$ for $2 \le i \le 12$ one obtains the probability of each state at time t.

According to Figure 29.4, in different states MSS has the following performance rates: in the state 1 $v_1 = 3.5$, in the state 2 $v_2 = 2.0$, in the states 4 and 6 $v_4 = v_6 = 1.8$, in the states 3 and 7 $v_3 = v_7 = 1.5$, in the states 5, 8, 9, 10, 11 and 12 $v_5 = v_8 = v_9 = v_{10} = v_{11} = v_{12} = 0$. Therefore,

$\Pr\{V=3.5\} = p_1(t)$,

$\Pr\{V=2.0\} = p_2(t)$,

$\Pr\{V=1.8\} = p_4(t)+p_6(t)$,

$\Pr\{V=0\}=p_5(t)+p_8(t)+p_9(t)+p_{10}(t)+p_{11}(t)+p_{12}(t)$.

For the constant demand level $\theta = 1$, one obtains the MSS instantaneous availability as a sum of states probabilities where the MSS output performance is greater than or equal to 1. The states 1, 2, 3, 4, 6 and 7 are acceptable. Hence $A(t) = p_1(t) + p_2(t) + p_3(t) + p_4(t) + p_6(t) + p_7(t)$. The MSS instantaneous expected performance is: $W(t) = \sum_{i=1}^{12} p_i(t)v_i$.

Solving the system of 12 differential equations is quite a complicated task that can only be solved numerically. Applying the combination of Markov

and UGF techniques, one can drastically simplify the calculations and even obtain an analytical solution for the reliability and expected performance of the given system. One should proceed as follows:

1. According to the Markov method build the following systems of differential equations for each element separately (using the state-space diagrams presented in Figure 29.3):
For element 1:

$$\begin{cases} dp_{11}(t)/dt = -\mu_{1,2}^{(1)} p_{11}(t) + \lambda_{2,1}^{(1)} p_{12}(t) \\ dp_{12}(t)/dt = -\lambda_{2,1}^{(1)} p_{12}(t) + \mu_{1,2}^{(1)} p_{11}(t) \end{cases}$$

The initial conditions are $p_{12}(0) = 1$, $p_{11}(0) = 0$.

For element 2:

$$\begin{cases} dp_{21}(t)/dt = -\mu_{1,2}^{(2)} p_{21}(t) + \lambda_{2,1}^{(2)} p_{22}(t) \\ dp_{22}(t)/dt = -\lambda_{2,1}^{(2)} p_{22}(t) + \mu_{1,2}^{(2)} p_{21}(t) \end{cases}$$

The initial conditions are: $p_{21}(0) = 1$, $p_{22}(0) = 0$.

For element 3:

$$\begin{cases} dp_{31}(t)/dt = -\mu_{1,2}^{(3)} p_{31}(t) + \lambda_{2,1}^{(3)} p_{32}(t) \\ dp_{32}(t)/dt = \lambda_{3,2}^{(3)} p_{33}(t) - (\lambda_{2,1}^{(3)} + \mu_{2,3}^{(3)}) p_{32}(t) \\ \quad + \mu_{1,2}^{(3)} p_{31}(t) \\ dp_{33}(t)/dt = -\lambda_{3,2}^{(3)} p_{33}(t) + \mu_{2,3}^{(3)} p_{32}(t) \end{cases}$$

The initial conditions are: $p_{31}(0) = p_{32}(0) = 0$, $p_{33}(0) = 1$.

After solving the three separate systems of differential equations under the given initial conditions, we obtain the following expressions for state probabilities:

For element 1:

$$p_{11}(t) = \lambda_{2,1}^{(1)}/\omega^{(1)} - (\lambda_{2,1}^{(1)}/\omega^{(1)}) e^{-\omega^{(1)} t},$$

$$p_{12}(t) = \mu_{1,2}^{(1)}/\omega^{(1)} + (\lambda_{2,1}^{(1)}/\omega^{(1)}) e^{-\omega^{(1)} t},$$

For element 2:

$$p_{21}(t) = \lambda_{2,1}^{(2)}/\omega^{(2)} - (\lambda_{2,1}^{(2)}/\omega^{(2)}) e^{-\omega^{(2)} t},$$

$$p_{22}(t) = \mu_{1,2}^{(2)}/\omega^{(2)} + (\lambda_{2,1}^{(2)}/\omega^{(2)}) e^{-\omega^{(2)} t},$$

where $\omega^{(i)} = \mu_{1,2}^{(i)} + \lambda_{2,1}^{(i)}$.

For element 3:

$$p_{31}(t) = A_1 e^{\alpha t} + A_2 e^{\beta t} + A_3,$$

$$p_{32}(t) = B_1 e^{\alpha t} + B_2 e^{\beta t} + B_3,$$

$$p_{33}(t) = C_1 e^{\alpha t} + C_2 e^{\beta t} + C_3, \text{ where}$$

$$\alpha = -\eta/2 + \sqrt{\eta^2/4 - \zeta}, \ \beta = -\eta/2 - \sqrt{\eta^2/4 - \zeta},$$

$$A_1 = \frac{\lambda_{2,1}^{(3)} \lambda_{3,2}^{(3)}}{\alpha(\alpha - \beta)}, \ A_2 = \frac{\lambda_{2,1}^{(3)} \lambda_{3,2}^{(3)}}{\beta(\beta - \alpha)}, \ A_3 = \frac{\lambda_{2,1}^{(3)} \lambda_{3,2}^{(3)}}{\zeta},$$

$$B_1 = \frac{(\mu_{1,2}^{(3)} + \alpha)\lambda_{3,2}^{(3)}}{\alpha(\alpha - \beta)}, \ B_2 = \frac{(\mu_{1,2}^{(3)} + \alpha)\lambda_{3,2}^{(3)}}{\beta(\beta - \alpha)},$$

$$B_3 = \frac{\mu_{1,2}^{(3)} \lambda_{3,2}^{(3)}}{\zeta}, \ C_1 = \frac{(\mu_{1,2}^{(3)} + \alpha)\lambda_{3,2}^{(3)} \mu_{2,3}^{(3)}}{\alpha(\alpha - \beta)(\alpha + \lambda_{3,2}^{(3)})},$$

$$C_2 = \frac{(\mu_{1,2}^{(3)} + \beta)\lambda_{3,2}^{(3)} \mu_{2,3}^{(3)}}{\beta(\beta - \alpha)(\beta + \lambda_{3,2}^{(3)})},$$

$$C_3 = \frac{\mu_{1,2}^{(3)} \mu_{2,3}^{(3)} (\beta + \lambda_{3,2}^{(3)}(\lambda_{3,2}^{(3)} - \alpha))}{\alpha\beta(\alpha + \lambda_{3,2}^{(3)})(\beta + \lambda_{3,2}^{(3)})},$$

$$\eta = \lambda_{2,1}^{(3)} + \lambda_{3,2}^{(3)} + \mu_{1,2}^{(3)} + \mu_{2,3}^{(3)},$$

$$\zeta = \lambda_{2,1}^{(3)} \lambda_{3,2}^{(3)} + \mu_{1,2}^{(3)} \mu_{2,3}^{(3)} + \mu_{1,2}^{(3)} \lambda_{3,2}^{(3)}.$$

After determining the state probabilities for each element, we obtain the following performance distributions:

For element 1:

$\boldsymbol{g}_1 = \{g_{11}, g_{12}\} = \{0, \ 1.5\}$,

$\boldsymbol{p}_1(t) = \{p_{11}(t), p_{12}(t)\}$.

For element 2:

$\boldsymbol{g}_2 = \{g_{21}, g_{22}\} = \{0, \ 2.0\}$,

$\boldsymbol{p}_2(t) = \{p_{21}(t), p_{22}(t)\}$.

For element 3:

$\boldsymbol{g}_3 = \{g_{31}, g_{32}, g_{33}\} = \{0, \ 1.8, \ 4.0\}$,

$\boldsymbol{p}_3(t) = \{p_{31}(t), p_{32}(t), p_{33}(t)\}$.

2. Having the sets $\boldsymbol{g}_j$, $\boldsymbol{p}_j(t)$ for $j = 1,2,3$ obtained in the first step we can define the *u*-functions of the individual elements as:

$u_1(z) = p_{11}(t)z^{g_{11}} + p_{12}(t)z^{g_{12}} = p_{11}(t)z^0 + p_{12}(t)\, z^{1.5}$.

$u_2(z) = p_{21}(t)z^{g_{21}} + p_{22}(t)z^{g_{22}} = p_{21}(t)z^0 + p_{22}(t)z^2$.

$u_3(z) = p_{31}(t)z^{g_{31}} + p_{32}(t)z^{g_{32}} + p_{33}(t)\, z^{g_{33}} = p_{31}(t)z^0 + p_{32}(t)z^{1.8} + p_{33}(t)z^4$.

3. Using the composition operators for flow transmission MSS we obtain the resulting u-function for the entire series-parallel MSS $U(z)=[u_1(z) \underset{+}{\otimes} u_2(z)] \underset{\min}{\otimes} u_3(z)$ by the following recursive procedure:

$u_1(z) \underset{+}{\otimes} u_2(z)) = [p_{11}(t)z^0 + p_{12}(t)z^{1.5}] \underset{+}{\otimes} [p_{21}(t)z^0$

$+p_{22}(t)z^2] = p_{11}(t)p_{21}(t)z^0 + p_{12}(t)p_{21}(t)z^{1.5} + p_{11}(t)p_{22}(t)$ $z^2 + p_{12}(t)p_{22}(t)z^{3.5}$.

$U(z) = u_3(z) \underset{\min}{\otimes} [u_1(z) \underset{+}{\otimes} u_2(z)] = [p_{31}(t)z^0 + p_{32}(t)z^{1.8}$

$+p_{33}(t)z^4] \underset{\min}{\otimes} p_{11}(t)p_{21}(t)z^0 + p_{12}(t)p_{21}(t)z^{1.5}$

$+p_{11}(t)p_{22}(t)z^2 + p_{12}(t)p_{22}(t)z^{3.5}) = p_{31}(t)p_{11}(t)p_{21}(t)z^0$
$+p_{31}(t)p_{12}(t)p_{21}(t)z^0 + p_{31}(t)p_{11}(t)p_{22}(t)z^0$
$+p_{31}(t)p_{12}(t)p_{22}(t)z^0 + p_{32}(t)p_{11}(t)p_{21}(t)z^0$
$+p_{32}(t)p_{12}(t)p_{21}(t)z^{1.5} + p_{32}(t)p_{11}(t)p_{22}(t)z^{1.8}$
$+p_{32}(t)p_{12}(t)p_{22}(t)z^{1.8} + p_{33}(t)p_{11}(t)p_{21}(t)z^0$
$+p_{33}(t)p_{12}(t)p_{21}(t)z^{1.5} + p_{33}(t)p_{11}(t)p_{22}(t)z^2$
$+p_{33}(t)p_{12}(t)p_{22}(t)z^{3.5}$.

Taking into account that $p_{31}(t)+p_{32}(t)+p_{33}(t) = 1$, $p_{21}(t)+p_{22}(t)=1$ and $p_{11}(t)+p_{12}(t)=1$, we obtain the u-function that determines the performance distribution $\boldsymbol{v}$, $\boldsymbol{q}(t)$ of the entire MSS in the following form $U(z)= \sum_{i=1}^{5} q_i(t)z^{v_i}$ where

$v_1=0$,
$q_1(t)= p_{11}(t)p_{21}(t)+p_{31}(t)p_{12}(t)+p_{31}(t)p_{11}(t)p_{22}(t)$,
$v_2=1.5$ tons/min,
$q_2(t)= p_{12}(t)p_{21}(t)[p_{32}(t)+p_{33}(t)]$,
$v_3=1.8$ tons/min, $q_3(t)= p_{32}(t)p_{22}(t)$,
$v_4=2.0$ tons/min, $q_4(t)= p_{33}(t)p_{11}(t)p_{22}(t)$,
$v_5=3.5$ tons/min, $q_5(t)= p_{33}(t)p_{12}(t)p_{22}(t)$.

4. Based on the entire MSS u-function $U(z)$ we obtain the MSS reliability indices:

The instantaneous MSS availability for different demand levels θ takes the form

$A(t) = q_2(t) + q_3(t) + q_4(t) + q_5(t)$ for $0 < \theta \le 1.5$;

$A(t) = q_3(t) + q_4(t) + q_5(t)$ for $1.5 < \theta \le 1.8$;

$A(t) = q_4(t) + q_5(t)$ for $1.8 < \theta \le 2$;

$A(t) = q_5(t)$ for $2 < \theta \le 3.5$;

$A(t) = 0$ for $3.5 < \theta$.

The instantaneous expected performance at any instant $t > 0$ is

$W(t) = \sum_{i=1}^{5} q_i(t)v_i$

$=1.5q_2(t)+1.8q_3(t)+2q_4(t)+3.5q_5(t)$.

The obtained function $W(t)$ is presented in Figure 29.5.

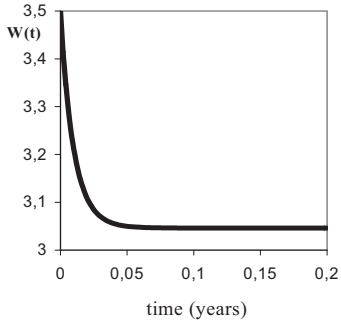


Figure 29.5. System instantaneous expected performance

29.4 Combined Markov-UGF Technique for Analysis of Safety-critical Systems

The UGF technique can be used not only in the cases when different element's states are characterized by quantitative measures of their performance. For example, in analysis of safety-critical systems the dangerous and non-dangerous failures are distinguished, that correspond to failure-safe and failure-dangerous states of the system.

The following section presents a Markov-UGF-based method for evaluating the probabilities of failure-safe and failure-dangerous states for arbitrary complex series-parallel systems with imperfect diagnostics and imperfect periodic inspections and repairs of elements [6]. Each kind of element failure whether failure-safe or failure-dangerous can be either detected or undetected.

29.4.1 Model of System Element

The model of any system element is based on the following assumptions:

1. A system is composed of elements and each element can experience two categories of failures: dangerous and non-dangerous, corresponding, respectively, to failure-dangerous and failure-safe events. Failure-dangerous and failure-safe events are independent.
2. Both categories of failures can be detected and undetected.
3. Detected and undetected failures constitute independent events.
4. Failure rates for both kinds of failures are constant.
5. The element is in operation state if no failure event (detected or undetected) has occurred.
6. The element is in failure-safe state if at least one non-dangerous failure (detected or undetected) has occurred and no dangerous failure has occurred.
7. The element is in failure-dangerous state if at least one dangerous failure (detected or undetected) has occurred.
8. The elements are independent and can undergo periodic inspections at different times.
9. The state of any composition of elements is unambiguously defined by the states of these elements and the nature of the interaction of the elements in the system.
10. The elements' interaction is represented by a series-parallel block diagram.

The safety-critical system is composed of elements to which diagnosis and periodic inspection and repair are applied. Failure-safe or failure-dangerous events can occur independently. The failure category depends on the effects of a fault occurrence. For example, if a failure results in the shutdown of a properly operating process, it is of the failure-safe (FS) type. This type of failure is referred to in a variety of ways as false trip and false alarm. However, if a safety-critical system fails in an operation that is required to shut down a process, this may cause hazardous results, such as the failure of a monitor that is applied to control an important process. This type of failure is generally called failure-dangerous (FD).

Both FS and FD events can be detected or undetected. The detected failure can be detected instantly by diagnostic devices. An imperfect diagnosis model presumes that a fraction d of detected failures can be detected instantaneously by diagnostic devices. Whenever the failure of this kind is detected, the on-line repair is initiated. The failures that cannot be detected by diagnostic devices or remain undetected because of imperfect diagnosis are considered to be undetected failures. These failures can be found only by the proof-test (periodical inspection) just after the end of a proof-test interval. We assume that failure rates of detected failure-safe and failure-dangerous (λ_{sd} and λ_{dd}, respectively) event, as well as undetected failure-safe and failure-dangerous (λ_{su} and λ_{du}, respectively) events can be calculated or elicited from tests.

The state of any single element can be represented as the combination of two independent states corresponding to detected and undetected failures. Each of the two failures can be in the three different states of no failure (state O), failure of the FS category, and failure of the FD category. According to assumptions 5–7, the state of each element can be determined based on each combination of states of failures using Table 29.2.

The state of each element j can be represented by a discrete random variable G_j that takes values from the set {O, FS, FD}. In order to obtain the element state distribution $p_{jO} = \Pr(G_j = \mathrm{O})$, $p_{jFS} = \Pr(G_j = \mathrm{FS})$ and $p_{jFD} = \Pr(G_j = \mathrm{FD})$, one should summarize the probabilities of any combination of states of detected and undetected failures that results in the element states O, FS and FD, respectively. Based on element state transition analysis, one can obtain the Markov state transition diagram presented in Figure 29.6. In this diagram, each possible combination of the states of detected and undetected failures (marked inside the ellipses) belongs to one of the three sets corresponding to three different states of element defined according to Table 29.2.

Practically, no repair action is applied to the undetected failure until the next proof-test. In general, periodic inspection and repair take a very

Table 29.2. States of single elements

		Detected failure		
		O	FS_d	FD_d
Undetected failure	O	O	FS	FD
	FS_u	FS	FS	FD
	FD_u	FD	FD	FD

short time when compared to the proof-test interval T_1, and the whole system stops operating during the process of periodic inspection and repair. Therefore, it is reasonable to set repair rates for undetected failures $\mu_{du} = \mu_{su} = 0$ when analyzing the behavior of a safety-critical system within the proof-test interval.

According to Figure 29.6, the following group of equations describes an element's behavior:

$$\boldsymbol{P}'(t) = \boldsymbol{P}(t)\,\boldsymbol{\Lambda}_j \qquad (29.19)$$

where, $\boldsymbol{P}(t) = (p_{j1}(t), p_{j2}(t), \ldots, p_{j9}(t))$ is the vector of state probabilities, $\boldsymbol{P}'(t)$ is derivative of $\boldsymbol{P}(t)$ with respect to t, and $\boldsymbol{\Lambda}_j$ is transition rate matrix presented in Figure 29.7.

According to Table 29.2, state 1 in the Markov diagram corresponds to state O of the element, states 2–4 correspond to state FS of the element and states 5–9 correspond to state FD of the element. Having the solution $\boldsymbol{P}(t)$ of (29.19) for any element j, one can obtain $p_{jO} = p_{j1}$, $p_{jFS} = p_{j2} + p_{j3} + p_{j4}$ and $p_{jFD} = p_{j5} + p_{j6} + p_{j7} + p_{j8} + p_{j9}$. The solution of (29.19) can be expressed as

$$\boldsymbol{P}_j(t) = \boldsymbol{P}_j(0) \cdot \exp(\boldsymbol{\Lambda}_j\, t), \quad \text{for } t \geq 0; \qquad (29.20)$$

$$\boldsymbol{P}_j(t) = \boldsymbol{P}_j(n\,T_1^+)\exp(\boldsymbol{\Lambda}_j\,(t - n\,T_1)),$$

$$\text{for } n\,T_1^+ \leq t \leq (n+1)\,T_1^+,\ n = 0, 1, 2, \ldots$$

According to imperfect inspection and repair model, the undetected fault cannot be repaired as good as new and some faults may still exist after

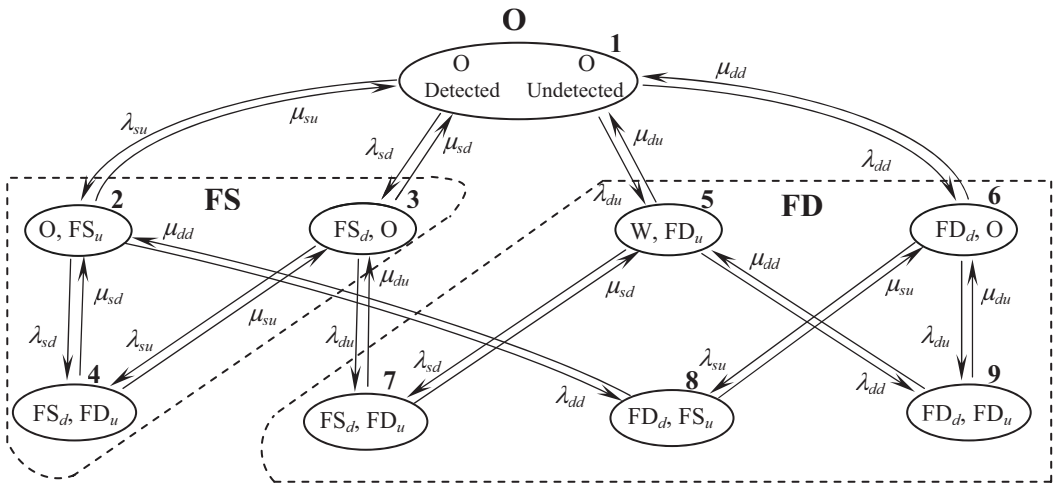


Figure 29.6. Markov state transition diagram used for calculating state distribution of a single element

$$\boldsymbol{\Lambda}_j = \begin{bmatrix}
-\lambda_{sd}-\lambda_{dd}-\lambda_{su}-\lambda_{du} & \lambda_{su} & \lambda_{sd} & \lambda_{du} & \lambda_{dd} & 0 & 0 & 0 & 0 \\
0 & -\lambda_{sd}-\lambda_{dd} & 0 & 0 & 0 & \lambda_{sd} & 0 & \lambda_{dd} & 0 \\
\mu_{sd} & 0 & -\lambda_{su}-\lambda_{du}-\mu_{sd} & 0 & 0 & \lambda_{su} & \lambda_{du} & 0 & 0 \\
0 & 0 & 0 & -\lambda_{sd}-\lambda_{dd} & 0 & 0 & \mu_{sd} & 0 & \mu_{dd} \\
\mu_{dd} & 0 & 0 & 0 & -\lambda_{su}-\lambda_{du}-\mu_{dd} & 0 & 0 & \lambda_{su} & \lambda_{du} \\
0 & \mu_{sd} & 0 & 0 & 0 & -\mu_{sd} & 0 & 0 & 0 \\
0 & 0 & 0 & \mu_{sd} & 0 & 0 & -\mu_{sd} & 0 & 0 \\
0 & \mu_{dd} & 0 & 0 & 0 & 0 & 0 & -\mu_{dd} & 0 \\
0 & 0 & 0 & \mu_{dd} & 0 & 0 & 0 & 0 & -\mu_{dd}
\end{bmatrix}$$

Figure 29.7. Transition rate matrix

inspection and repair. A matrix $\boldsymbol{M}_{ji}$ is used to describe this behavior. Each element of the matrix $\boldsymbol{M}_{ji}$ describes the transition rate of probability from one state to another. Thus, we have

$$\begin{aligned}
&\boldsymbol{P}_j(T_1^+)=\boldsymbol{P}_j(T_1)\,\boldsymbol{M}_{j1}=\boldsymbol{P}_j(0)\exp(\Lambda_j T_1)\boldsymbol{M}_{j1};\\
&\boldsymbol{P}_j(2T_1^+)=\boldsymbol{P}_j(2T_1)\boldsymbol{M}_{j2}\\
&=\boldsymbol{P}_j(0)\exp(\Lambda_j T_1)\boldsymbol{M}_{j1}exp(\Lambda_j T_1)\,\boldsymbol{M}_{j2};\\
&\boldsymbol{P}_j(nT_1^+)=\boldsymbol{P}_j(nT_1)\boldsymbol{M}_{jn}=\boldsymbol{P}_j((n-1)T_1^+)\exp(\Lambda_j T_1)\boldsymbol{M}_{jn}\\
&=\boldsymbol{P}_j((n-2)T_1^+)\exp(\Lambda_j T_1)\boldsymbol{M}_{j(n-1)}\exp(\Lambda_j T_1)\boldsymbol{M}_{jn}\\
&=\boldsymbol{P}_j(0)\exp(\Lambda_j T_1)\boldsymbol{M}_{j1}\exp(\Lambda_j T_1)\boldsymbol{M}_{j2}\times\ldots\\
&\times\exp(\Lambda_j T_1)\,\boldsymbol{M}_{j(n-1)}\exp(\Lambda_j T_1)\boldsymbol{M}_{jn}\ \text{for } n=3,4,\ldots
\end{aligned} \tag{29.21}$$

where n represents the number of proof-test intervals and $\boldsymbol{M}_{ji}$ (i=1,…,n) is matrix associated with the ith proof-test.

29.4.2 State Distribution of the Entire System

In order to obtain the state distribution of the entire system one can represent the performance distribution of the basic element j (*pmf* of the discrete random variable G_j) as

$$u_j(z)=\sum_{k=1}^{3} p_{jk} z^{g_{jk}}\ , \tag{29.22}$$

where g_{j1} = FD, g_{j2} = FS, g_{j3} = O for any j.

The structure functions ϕ_{ser} and ϕ_{par} for pairs of elements connected in parallel and in series should be defined for any specific application based on analysis of the system functioning. For example, in the widely applied conservative approach the following assumptions are made. Any subsystem consisting of two parallel elements is in the failure-dangerous state if at least one element is in the failure-dangerous state and it is in the operational state if at least one element is in the operational state. In all other cases, the subsystem is in the failure-safe state. This can be expressed by the structure function ϕ_{par} presented in Table 29.3.

Table 29.3. Structure function ϕ_{par}

		Element 1		
		O	FS	FD
Element 2	O	O	FS	FD
	FS	O	O	FD
	FD	O	FS	FD

Table 29.4. Structure function ϕ_{ser}

		Element 1		
		O	FS	FD
Element 2	O	FS	FD	FD
	FS	FS	FD	FD
	FD	FD	FD	FD

A subsystem consisting of two elements connected in series is in the operational state if both elements are in the operational state, whereas it is in the failure-dangerous state if at least one element is in the failure-dangerous state. In all other cases, the subsystem is in the failure-safe state. This can be expressed by the structure function ϕ_{ser} presented in Table 29.4.

In the numerical realization of the composition operators, we can encode the states O, FS and FD by integer numbers 3, 2 and 1, respectively, such that $g_{jk} = k$ for any j. It can be seen that in this case the functions ϕ_{ser} and ϕ_{par} defined above take the form:

$$\phi_{\text{par}}(g_{jk}, g_{ih}) = \begin{cases} \max(g_{jk}, g_{ih}), & \text{if } \min(g_{jk}, g_{ih}) > 1 \\ 1, & \text{if } \min(g_{jk}, g_{ih}) = 1 \end{cases}$$

and $\phi_{\text{ser}}(g_{jk}, g_{ih}) = \min(g_{jk}, g_{ih})$.

Note that the nine possible different combinations of element states produce only three possible states of the subsystem. Applying the RBD technique one obtains the u-function representing the state distribution of the entire system (the system has also three distinguished states O, FS and FD).

With the state probabilities of each element in the form of functions of time, one can use the RBD technique to obtain the probability values corresponding to any given time. Finally, the entire system state probabilities and the overall system safety (defined as the sum of operational probability and failure-safe state probability) as functions of time can be obtained.

Example 3

Consider a combined-cycle power plant with two generating units [6]. Each unit consists of gas turbine blocks and fuel supply systems. The fuel to each turbine block can be supplied by two parallel systems. The simplified RBD of the plant is presented in Figure 29.8.

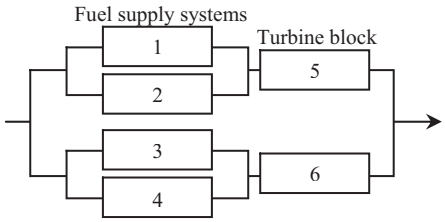


Figure 29.8. RBD of combine cycle power plant

Each fuel supply system as well as each turbine can experience both safe and dangerous failures (detected and undetected).

The parameters of fuel supply systems are: $\lambda_{sd} = 2.56\times10^{-5}$, $\lambda_{su} = 10^{-5}$, $\lambda_{dd} = 8.9\times10^{-6}$, $\lambda_{du} = 1\times10^{-6}$, $\mu_{sd} = 0.25$; $\mu_{dd} = 0.0833$, $\mu_{su} = \mu_{du} = 0$; $d = 0.99$; $T_1 = 1.5$ years. The fuel supply systems are statistically identical, but the inspection times of systems 2 and 4 are shifted 0.5 year earlier relatively to inspection times of systems 1 and 3.

The matrices $\boldsymbol{M}_{ji}$ associated with any system element take the form

$$\boldsymbol{M}_{ji} = \begin{array}{c} \begin{matrix} p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 & p_9 \end{matrix} \\ \begin{bmatrix} 1.0 & 0 & 0 & 0 & & & & & \\ \alpha & 1-\alpha & 0 & 0 & & & & & \\ 1 & 0 & 0 & 0 & \mathbf{0_9} & \mathbf{0_9} & \mathbf{0_9} & \mathbf{0_9} & \mathbf{0_9} \\ \beta & 0 & 0 & 1-\beta & & & & & \\ \mathbf{1_5} & \mathbf{0_5} & \mathbf{0_5} & \mathbf{0_5} & & & & & \end{bmatrix} \end{array},$$

where $\mathbf{0_k}$ and $\mathbf{1_k}$ are zero and unit column vectors of size $k\times1$ respectively. For the fuel supply systems: for $\boldsymbol{M}_{11}$ $\alpha = 0.9$ and $\beta = 0.8$; for $\boldsymbol{M}_{12}$ $\alpha = 0.88$ and $\beta = 0.776$; for $\boldsymbol{M}_{13}$ $\alpha = 0.85$ and $\beta = 0.747$; for $\boldsymbol{M}_{14}$ $\alpha = 0.808$ and $\beta = 0.711$.

The turbine blocks are also statistically identical. The parameters of the turbine blocks are: $\lambda_{sd} = 2.56\times10^{-5}$, $\lambda_{su} = 6.540\times10^{-6}$, $\lambda_{dd} = 7.9\times10^{-6}$, $\lambda_{du} = 7.8\times10^{-7}$; $\mu_{sd} = 0.25$, $\mu_{dd} = 0.0625$, $\mu_{su} = \mu_{du} = 0$; $d = 0.99$; $T_1 = 2$ years. The parameters of matrices $\boldsymbol{M}_{ji}$ for the turbine blocks are: for $\boldsymbol{M}_{21}$ $\alpha = 0.92$ and $\beta = 0.85$; for $\boldsymbol{M}_{22}$ $\alpha = 0.804$ and $\beta = 0.832$; for $\boldsymbol{M}_{23}$ $\alpha = 0.882$ and $\beta = 0.81$.

The probabilities of working, failure-safe and failure-dangerous states were obtained numerically using the combined Markov-UGF procedure for a time period of 65000 hours. The obtained system safety (the probability that the system does not enter the failure-dangerous state) as the function of time is presented in Figure 29.9.

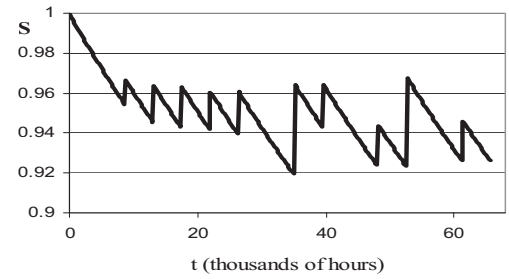


Figure 29.9. Overall system safety

29.5 Conclusions

The universal generating function technique is powerful computationally efficient tool for the reliability analysis of complex multi-state systems. It can be directly applied for calculating system reliability and performance indices based on the generalized reliability block diagram approach (recursively aggregating multi-state elements and replacing them by single equivalent ones). It can also be combined with the Markov random process technique to reduce drastically the dimension of differential equations to be solved.

The UGF approach is based on intuitively simple recursive procedures and provides a systematic method for the enumeration of the system states, which can replace extremely complicated combinatorial algorithms. The same recursive procedures can be used for systems with a different physical nature of the characteristics of elements' states and different types of element interaction. This provides the universality of the UGF method. The applications of the method can be found in fields such as internet services [7], communication networks [8], control and image processing [9], software systems [5], quality control and manufacturing [10], defense [11], and many other areas [4].

The reliability of multi-state systems is a recently emerging field at the junction of classical binary reliability and performance analysis. As a

relatively new discipline, it still has much to accomplish. Many promising directions for further research can be formulated.

The generic model of MSS provides a wide perspective for defining different new classes of systems. Various technical systems in combination with various failure criteria can produce new types of MSS models. Some of them can be extensions of corresponding binary models while others may not have any analogs.

In some cases, the system and its elements are characterized by several measures of functionality (for example, multiple product production systems). In these cases, the performance is a complex (usually vector) index. The extension of MSS models to the multi-performance case is necessary for the study of such systems.

In some systems, the effectiveness of their functioning cannot be measured numerically. Such measures as customer satisfaction or the safety level are usually represented and estimated using the fuzzy set approach. Integration of MSS and the fuzzy set techniques is a promising direction in the analysis of this type of system.

MSS models can be used for studying systems in which the performance of elements is influenced by factors such as deterioration, fatigue, learning, adaptation, *etc*. These factors should be considered in system design and in planning maintenance actions. For example, by incorporating dependencies of the elements failure rates on performance levels into MSS models one can determine the optimal load levels for the entire system or the optimal load distribution among system elements.

The combination of various types of multi-state systems with different criteria and constraints can produce many different interesting optimization problems. For example, incorporating economical indices associated with different levels of system performance provides a wide range of models in which design, maintenance activity, warranty policy, *etc*., are optimized.

When optimizing MSS, one deals with different measures of its reliability and efficiency. Some of these measures are contradictory. For example, a tradeoff usually exists between the availability of MSS and its performance deficiency. In this situation the problems of MSS optimization become multi-objective by their nature. The combination of algorithms for solving multi-objective problems with realistic formulations of MSS optimization problems with multiple criteria can be very fruitful in many applications.

When determining the maintenance of complex systems consisting of elements with different reliability and performance rates one can use the MSS models for estimating the effect of the technological changes on the replacement decisions, for determining the optimal number of spare parts and the optimal inventory management, replacement rules of the system components, the cannibalization policy, the scheduling of maintenance jobs, *etc*. Algorithms of the complex periodic inspection/replacement policies for MSS that maximize the maintenance efficiency are still to be developed.

The recent developments in sensors and measuring techniques have facilitated the continuous monitoring of the performance of systems and their elements. This has led to the development of a predictive maintenance approach. The development of decision rules in the predictive maintenance of MSS is a challenging task.

Since computers are used in almost every system, software reliability has become an important issue attracting the interest of researchers. Many software failures cause not only system failure, but also deterioration of the system performance (usually computational time), which is caused by restarts, self-testing, *etc*. Therefore, in order to assess the reliability indices of complex systems consisting of software and hardware components, one has to develop multi-state models. Further research is needed to estimate the influence of the resource distribution during the software development and testing on the system's reliability. In this research, software reliability models should be incorporated into the MSS paradigm.

References

[1] Lisnianski A, Levitin G. Multi-state system reliability. Assessment, optimization and applications. World Scientific, Singapore, 2003.

[2] Ushakov I. Optimal standby problems and a universal generating function. Soviet Journal of Computer Systems Science 1987; 25:79–82.
[3] Levitin G, Lisnianski A, Beh-Haim H, Elmakis D. Redundancy optimization for series-parallel multi-state systems. IEEE Transactions on Reliability 1998; 47:165–172.
[4] Levitin G. Universal generating function in reliability analysis and optimization. Springer, London, 2005.
[5] Levitin G. Optimal version sequencing in fault-tolerant programs. Asia-Pacific Journal of Operational Research 2005; 22(1):1–18.
[6] Levitin G, Zhang T, Xie M. State probability of a series-parallel repairable system with two types of failure states. International Journal of Systems Science 2006; 37(14):1011-1020.
[7] Levitin G, Dai Y, Ben-Haim H, Reliability and performance of star topology grid service with precedence constraints on subtask execution. IEEE Transactions on Reliability 2006; 55(3): 507–515.
[8] Levitin G. Reliability evaluation for acyclic transmission networks of multi-state elements with delays. IEEE Transactions on Reliability 2003; 52(2):231–237.
[9] Levitin G. Threshold optimization for weighted voting classifiers. Naval Research Logistics 2003; 50 (4):322–344.
[10] Levitin G. Linear multi-state sliding window systems. IEEE Transactions on Reliability 2003; 52 (2): 263–269.
[11] Levitin G. Optimal defense strategy against intentional attacks. IEEE Transactions on Reliability 2007; 56(1):148–157.

30

New Approaches for Reliability Design in Multistate Systems

Jose Emmanuel Ramirez-Marquez

Stevens Institute of Technology,
Babbio Bldg. #537, Hoboken, NJ 07030, USA

Abstract: This chapter presents a new algorithm that can be applied to solve multi-state reliability allocation problems, namely: capacitated multistate and multistate with multistate components. The optimization problem solved considers the maximization of the system design reliability subject to known constraints on resources (cost and weight) by assuming that the system contains a known number of subsystems connected in series and for each of these subsystems a known set of functionally equivalent component types (with different performance specifications) can be used to provide redundancy. This is the first time an optimization algorithm for multistate systems with mutistate components has been proposed. The algorithm is based on two major steps that use a probabilistic discovery approach and Monte Carlo simulation to generate solutions to these problems. Examples for different series-parallel system behaviors are used throughout the chapter to illustrate the approach. The results obtained for these test cases are compared with other methods to show how the algorithm can generate good solutions in a relatively small amount of time. Although developed for series-parallel system reliability optimization, the algorithm can be applied in other system structures as long as minimal cut sets are known.

30.1 Introduction

The optimal design of systems is a classical optimization problem in the area of system reliability engineering [1]. In general, the objective of these problems is to optimize a function-of-merit of the system design (reliability, cost, mean time to failure, *etc*.) subject to known constraints on resources (cost, weight, volume, *etc.*) and/or system performance requirements (reliability, availability, mean time to failure, *etc*.).

To optimize this specific function, it is generally assumed that the system can be decomposed into a system that contains a known number of subsystems connected in series and for each of these subsystems a known set of functionally equivalent components types (with different performance specifications) can be used to provide redundancy. This problem is referred to as the series-parallel component reliability allocation problem (RAP) and in this chapter the objective of the problem is to maximize system reliability subject to resource constraints.

30.1.1 Binary RAP

Currently, most methods developed for the solution of the series-parallel RAP work under the

assumption that the system and its components are of a binary nature. That is, the system and its components are either perfectly working or completely failed. Whenever this assumption holds, the most common approach to solve RAP has been to restrict the search space and to prohibit the mixture of different components within a subsystem [2].

Ghare and Taylor [3] demonstrated that for, problems with nonlinear but separable constraints, many variations of the problem can be transformed into an integer programming model. A knapsack formulation using alternate constraints was proposed by Bulfin and Liu [4]

The problem of mixing functionally equivalent components within subsystems has been addressed by Coit and Smith [5]. In their study, it has been recognized that allowing mixing of components can yield a better solution to the problem since the solution space is expanded. They successfully obtained solutions for many problems to demonstrate the advantages of genetic algorithms (GA).

The use of GA requires problem-specific coding and parameter tuning, and the development of adequate initial solutions so that the converged solution is near optimal. Thus, researchers have analyzed other techniques to solve mixing components in RAP that include surrogate approaches allowing transforming the problem into a linear program. The max-min method proposed by Ramirez-Marquez *et al*. [6] transforms the original system RAP into a problem of the maximization of the minimum subsystem reliability. This new formulation allowed for the first time, the use of commercially available linear programming software for RAP with component mixture. In this respect, Lee *et al.* [7] have compared the max-min method with the Nakagawa and Nakashima approach [8] for various test cases concluding that the former generally out-performed the latter with respect to system reliability design.

More recently, Coit and Konak [9] presented an extension of the max-min method using a multiple weighted objectives heuristic, which involves the transformation of a single objective problem into one with multiple objectives.

30.1.2 Multistate RAP

For some systems, a binary assumption fails to recognize the true nature of the system performance. An incorrect binary state assumption could potentially overestimate system reliability leading to incorrect results and poor system design. Furthermore, this assumption imposes a restriction on both the type of system that can be designed and on the types of components that can be used. Namely, that the different component types that can be used to provide a defined function, contribute to the system performance in equal terms (*i.e.*, no difference in the nominal performance of the components of the system exists).

In practice, there are different component versions with known cost and reliability that can yield different system performance levels; measured as a capacity of system requirement. As an example, consider an electric distribution system [10] where a particular component type may be able to provide 100% of the daily demand, yet a different type of component could just supply 80% of the same demand level or yet, another component may be able to supply 90%, 50% or nothing, depending on its functional behavior.

Recognition of these performance considerations for system configuration is important due to the significant impact that component performance can have in an optimal system design.

These considerations have been recognized in the area of multi-state system reliability [11–16]; an area, concerned with the analysis of systems that have various performance levels and for which, performance is usually associated with the ability of the system to supply a known demand. In this respect, systems can be broadly categorized in one of two categories:

1. Systems that consist of binary capacitated components (*i.e.*, components that either work at a known nominal performance levels or that are completely failed), where in a given time interval, the system can have a range of different demands (*i.e.,* multi-state) depending on the performance levels of the selected components and their operating state [11, 13].

2. Systems for which a specific performance level must be guaranteed and where such performance is dictated by components that have multiple performance levels (*i.e.*, multistate components) [12, 14, 16].

For series-parallel RAP in the multi-state case, most studies have been concern with systems that fall into the first category. Such problem has been studied and analyzed by Levitin *et al.* [13], Lisnianski *et al.* [15], and Ramirez-Marquez and Coit [12]. These researchers developed heuristic approaches to solve the problem of minimizing system cost subject to a reliability or availability constraint. These methods do not guarantee an optimal solution although they have been demonstrated to yield very good results.

The GA developed in [13, 15] requires that the universal generating function method (an implicit enumeration method [16]) be used for solution representation and decoding procedure for calculating multistate system reliability. Furthermore, these methods require the development, coding and testing of a problem specific GA, complicating the solution process and are highly dependent on the quality of initial solutions.

In the second category, there are currently no algorithms that can be used to provide a solution for the series-parallel RAP. Similarly, it should be noted that there is no general approach that can be used for solving any of the multi-state problems. That is, the algorithms developed for a specific case of RAP cannot be immediately applied in other cases.

The remainder of the chapter is organized as follows. Section 2 presents the general series-parallel system reliability computation problem for each of the cases discussed. In Section 3, the heuristic approach is developed for solving the RAP for general series-parallel systems. Finally, Section 4 considers different literature examples to illustrate the proposed method and illustrate its efficiency and accuracy.

30.1.3 Notation

$\mathbf{X}$	System design vector $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$
$\mathbf{x}_i$	Subsystem design vector $\mathbf{x}_i = (x_{i11}, x_{i12}, \ldots, x_{i1u}, x_{i21}, \ldots, x_{i2u}, \ldots, x_{im1}, \ldots, x_{imu})$
x_{ijk}	Binary decision variable defining if the kth type j component in subsystem design vector $\mathbf{x}_i$ is present or not. k=1,…u
$R(\mathbf{x})$	Series-parallel reliability under design vector $\mathbf{x}$
$P(\varphi_i(\mathbf{x}) \geq d_v)$	Probability the supply of the ith subsystem is greater than or equal to d_v
d_v	Demand for the vth operating interval
$g_l(\mathbf{x})$	Value of the lth constraint under design vector $\mathbf{x}$
G_l	The lth constraint value, l=1,…,L
$\mathbf{x}_i^h$	The hth potential solution , h=1,…,DESIGN $\mathbf{x}_i^h = (x_{i11}^h, x_{i12}^h, \ldots, x_{i1u}^h, x_{i21}^h, \ldots, x_{i2u}^h, \ldots, x_{ijk}^h, \ldots, x_{im1}^h, \ldots, x_{imu}^h)$
$\boldsymbol{\gamma}_i$	Vector of probabilities, $\boldsymbol{\gamma}_i = (\gamma_{i11}, \gamma_{i12}, \ldots, \gamma_{i1u}, \gamma_{i21}, \ldots, \gamma_{i2u}, \ldots, \gamma_{ijk}, \ldots, \gamma_{imu}, \ldots, \gamma_{imu})$
γ_{ijk}	Defined as $P(x_{ijk}=1)$
$\mathbf{b}_{ij}$	Possible states for the jth component type in the ith subsystem. $\mathbf{b}_{ij}=(b_{ij1}, b_{ij2}, \ldots, b_{ijz})$
$\mathbf{p}_{ij}$	State probability vector for the jth component type in the ith subsystem. $\mathbf{p}_{ij}=(p_{ij1}, p_{ij2}, \ldots, p_{ijz})$
$\mathbf{y}_i$	Subsystem state vector $\mathbf{y}_i=(y_{i11}, y_{i12}, \ldots, y_{i1u}, \ldots, y_{ij1}, y_{i21}, \ldots, y_{i2u}, \ldots, y_{ijk}, \ldots, y_{im1}, \ldots, y_{imu})$
p_{ijw}	Defined as $p_{ijw}=P(y_{ijk}=b_{ijw})$
$\Delta_l(\mathbf{x}^h)$	The lth penalty function for the hth potential solution
$\overline{R}(\mathbf{x}^h)$	Penalized reliability for the hth potential solution
S	A subset of solutions
λ	Indexes the number of generations in the global and local cycles
$\mathbf{x}^*$	Optimal system design vector

30.1.4 Acronyms

RAP	Reliability allocation problem
MC	Monte Carlo
GA	Genetic algorithm
LOLP	Loss of load probability

30.1.5 Assumptions

1. Component characteristics are known.
2. Failures of individual components are *s*-independent.
3. All redundancy is active.
4. Component failures do not manage the system and no repair or maintenance is considered.

30.2 General Series-parallel Reliability Computation

For general series-parallel systems, the loss of load probability (LOLP) index can be used as a measure of system reliability. LOLP can be understood as the probability the system cannot supply a given demand load. Based on this index, for an operating period that is divided into V operating intervals with duration T_v and demand level d_v, the probability of system success at a given demand level is given by:

$$R(\mathbf{x}) = T_1' \prod_{i=1}^{n} P\left(\varphi_i(\mathbf{x}) \geq d_1\right) + T_2' \prod_{i=1}^{n} P\left(\varphi_i(\mathbf{x}) \geq d_2\right) + \ldots + T_V' \prod_{i=1}^{n} P\left(\varphi_i(\mathbf{x}) \geq d_V\right) = \sum_{v=1}^{V} T_v' \prod_{i=1}^{n} P\left(\varphi_i(\mathbf{x}) \geq d_v\right) \tag{30.1}$$

where $$T_v' = \frac{T_v}{\sum_{v=1}^{V} T_v}.$$

In the binary case, (30.1) would revert to the well-known series-parallel formulation if only one operating interval, a demand equal to 1 and binary (0, 1) component states are considered.

For the multistate cases, (30.1) can be solved either using the universal generation function approach presented by Levitin and Lisnianski [11] or by using a minimal cut/path vector approach [14]. Figure 30.1 illustrates the differences that are present in each of the series-parallel systems cases.

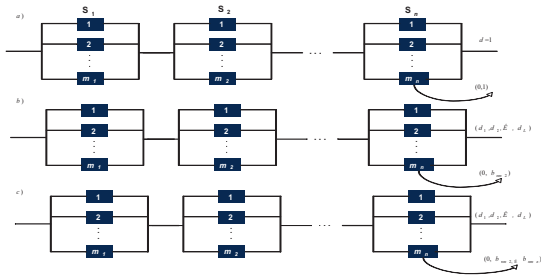


Figure 30.1. Series-parallel systems: **(a)** binary, **(b)** capacitated multistate and (**c**) multistate components

For the binary case, the demand is defined to be one unit and that each component in the subsystems can "process" one unit if it is working and nothing if it is failed. For case b, the system can experience different demands at different time intervals but the components either work at a nominal capacity or fail. Finally, the last case considers that components can have multiple capacities ranging from the nominal capacity to the complete failure.

30.3 Algorithm for the Solution of Series-parallel RAP

The mathematical model to be optimized in this chapter is presented in model 1. The objective of this model is to maximize the reliability of general series-parallel systems subject to a known number of constraints on resources. It is assumed that the system contains n subsystems connected in series and, for each of these subsystems a known set of functionally equivalent components types (with different performance specifications) can be used to provide redundancy.

Model 1

$$\text{Max} \sum_{v=1}^{V} T_v' \prod_{i=1}^{n} P\left(\varphi_i(\mathbf{x}) \geq d_v\right)$$

subject to

$g_l(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n) \le G_l \; \forall \; l=1,\ldots L$

$x_{ijk} \in Z^+$ (x_{ijk} the kth type j component in subsystem design vector $\mathbf{x}_i$).

30.3.1 Algorithm

The algorithm to solve model 1 uses two optimization cycles termed global and local. The global cycle contains three interrelated steps that are based on MC simulation, the cut sets of general series-parallel systems, the max-flow min-cut theorem [17], and a new method to select potential optimal system designs.

In the design development step, the first of the three steps of the global cycle, MC simulation is used to generate a specified number of potential system designs based on the probabilities defined by the vector $\boldsymbol{\gamma}_i$. This vector defines the probability that a specific component type will be present in the final system design and its level of redundancy. This step also contains the stopping rule of the algorithm. In essence, the rule dictates that the algorithm be stopped once the vector $\boldsymbol{\gamma}_i$ will no longer change (*i.e.*, all initial "appearance" probabilities are either zero or one).

Following this step, for each of the previously generated potential system designs, the second step simulates the performance behavior for each of the k possible component types in each subsystem (*i.e.*, generates a subsystem state vector $\mathbf{y}_i$). It is important to notice that the index k defines the maximum level of redundancy allowed for any given component. Once vector $\mathbf{y}_i$ is obtained, it is used along with the potential subsystem design obtained in Step 1 and with the max-flow min-cut theorem to generate an estimate of the system design reliability.

The final step in the global cycle penalizes the reliability of potential system designs both when the solutions exceed and when they fall short of the exact value of the constraints. The solutions are then ranked in decreasing order with respect to the penalized reliability. The best solution is stored and then a subset of size S of the whole set of solutions (a set of size DESIGN), is used to update the probabilities defined by the vector $\boldsymbol{\gamma}_i$. This new vector is sent to Step 1 to check for termination or for solution discovery.

The pseudo code of the global cycle optimization follows:

Global Cycle Optimization

Initialize: DESIGN, RUNS, S, h, $\boldsymbol{\gamma}_i$, λ=1, u,

Step 1:
(Design Development)
For h =1,…, DESIGN
For i= 1,..,n generate a subsystem design $\mathbf{x}_i$, as dictated by vector $\boldsymbol{\gamma}_i$

$$\mathbf{x}_i^h = \left(x_{i1}^h, x_{i12}^h, \ldots, x_{i1u}^h, x_{i21}^h, \ldots, x_{i2u}^h, \ldots, x_{ijk}^h, \ldots, x_{im1}^h, \ldots, x_{imu}^h\right)$$

and

$$\boldsymbol{\gamma}_i = \left(\gamma_{i11}, \gamma_{i12}, \ldots, \gamma_{i1u}, \gamma_{i21}, \ldots, \gamma_{i2u}, \ldots, \gamma_{ijk}, \ldots, \gamma_{im1}, \ldots, \gamma_{imu}\right)$$

where, $\gamma_{ijk}=P(x_{ijk}=1)$;

$\mathbf{x}^h = \left(\mathbf{x}_1^h, \mathbf{x}_1^h, \ldots, \mathbf{x}_i^h, \ldots \mathbf{x}_n^h\right)$; $h \rightarrow h+1$;

if ($\gamma_{ijk}=1 \vee \gamma_{ijk}=0 \; \forall$ i, j and k) Stop.

$\mathbf{x}_i^* = \arg\max\left\{R\left(\mathbf{x}^h\right), R\left(\overline{\mathbf{x}}^\lambda\right)\right\} \quad \forall i, \lambda \; \forall \; i$

Go to local cycle.
Else go to Step 2.

Step 2:
(Component State Simulation)
For h= 1,..,DESIGN
While ($t \le$ RUNS)
For i= 1,..,n generate a subsystem state vector $\mathbf{y}_i$ as dictated by vectors $\mathbf{b}_{ij}$ and $\mathbf{p}_{ij}$

$\mathbf{y}_i = (y_{i11}, y_{i12}, \ldots, y_{i1u}, \ldots, y_{ij1}, y_{i21}, \ldots, y_{i2u}, \ldots, y_{ijk}, \ldots, y_{im1}, \ldots, y_{imu})$

$\mathbf{b}_{ij}=(b_{ij1}, b_{ij2}, \ldots, b_{ijz})$ and $\mathbf{p}_{ij}=(p_{ij1}, p_{ij2}, \ldots, p_{ijz})$ where $p_{ijw}=\mathrm{P}(y_{ijk}=b_{ijw})$

(Design Reliability Analysis)
For i= 1,..,n calculate:

$$\Omega_i = \sum_{j=1}^{m} \sum_{k=1}^{u} x_{ijk}^h y_{ijk}$$

If $\Omega_i \ge d \; \forall \; i$:
$Q \rightarrow Q$; $t \rightarrow t+1$
Else
$Q \rightarrow Q+1$; $t \rightarrow t+1$;
$R(\mathbf{x}^h)=1-(Q/\mathrm{RUNS})$;

Step 3:
(Solution Discovery)
For h=1,…,DESIGN and l=1,…,L compute:

$$\Delta_l(\mathbf{x}^h)=\begin{cases}\max_h\left\{R(\mathbf{x}^h)-\dfrac{g_l(\mathbf{x}^h)}{\max_l\{g_l(\mathbf{x}^h)\}}\right\} & g_l(\mathbf{x}^h)>G_l\\ \dfrac{g_l(\mathbf{x}^h)}{G_l} & \text{o.w.}\end{cases};$$

$$\overline{R}(\mathbf{x}^h)=\begin{cases}R(x^h)\max_l\{\Delta_l(\mathbf{x}^h)\} & \Delta_l(\mathbf{x}^h)\le 1\,\forall l\\ R(x^h)\min_l\{\Delta_l(\mathbf{x}^h)\} & \text{o.w.}\end{cases};$$

List $\overline{R}(\mathbf{x}^h)$ by decreasing order of magnitude:

$$\overline{R}(\mathbf{x}^{(1)})\ge\overline{R}(\mathbf{x}^{(2)})\ge\cdots\ge\overline{R}(\mathbf{x}^{(h)})\ge\cdots\ge\overline{R}(\mathbf{x}^{(\mathrm{GEN})})$$

$$\overline{\mathbf{x}}_i^{\lambda}=\mathbf{x}_i^{(1)}\ \forall i;\ \overline{\mathbf{x}}^{\lambda}=(\overline{\mathbf{x}}_1^{\lambda},\overline{\mathbf{x}}_2^{\lambda},\ldots,\overline{\mathbf{x}}_n^{\lambda});\ \lambda\to\lambda+1;$$

For i= 1,..,n update vector $\boldsymbol{\gamma}_i$ as follows:

$$\gamma_{ijk}=\frac{\sum_{s=1}^{S}x_{ijk}^{(s)}}{S}\ \text{where } S\ll\text{DESIGN}$$

Go to Step 1.

Once the global cycle stops, the algorithm recognizes that the solution maybe improved by iteratively applying the global cycle to a reduced RAP based on the best subsystem designs previously obtained.

These new iterations start by ordering the subsystems obtained from the optimal solution by increasing unreliability. Then any slack in the constraints is proportionally assigned (based on a normalized unreliability) to each of the subsystems. The current values of the constraints for the least unreliable subsystem are updated and a new subsystem solution is obtained based on the global cycle. If the new solution is better, the system design is updated otherwise the design suffers no transformation.

The local cycle continues by proportionally assigning any slack in the constraints to the second least unreliable system until all subsystems have been reanalyzed.

The pseudo code for the local optimization cycle follows.

Local Cycle Optimization

For $i \notin$ A and $i\le n$;
List 1-$R_i(\mathbf{x}_i^*)$ by increasing order of magnitude;

$$a=\arg\min_i\left(1-R_i(\mathbf{x}_i^*)\right)$$

Compute: $S_l=g(\mathbf{x}^*)-G_l\quad\forall\quad l$ and

$$\vartheta_a=\frac{1-R_a(\mathbf{x}_a^*)}{\sum_{\substack{i\notin A\\ i\le n}}\left(1-R_i(\mathbf{x}_i^*)\right)}$$

Use global optimization cycle to solve sub-model:

$$\text{Max}\ \sum_{v=1}^{V}T_v'P(\varphi_a(\mathbf{z}_a)\ge d_v)$$

s.t.

$$g_l(\mathbf{z}_a)\le g_l(\mathbf{x}_a^*)+S_l\vartheta_a$$

$z_{ajk}\in Z^+$ (z_{ajk} the kth type j component of subsystem design vector $\mathbf{x}_a$)

Step 2.
Update $\mathbf{x}_a^*$ if needed; A→A∪{a};
Go to Step 1.

30.4 Experimental Results

In this section, three different RAP for series-parallel systems have been solved to illustrate the simplicity and power of the algorithm.

The first of three problems, considers a binary system and is used to illustrate how the algorithm can be used immediately used for these problems. The remaining exampless belong to the multistate case; the second one, introduced by Levitin *et al*. [15] and, the last one, a multistate system with multistate components for the first time solved in the area of multistate reliability.

All the examples were solved with a Pentium R laptop at 238 Mhz and 512 Mb of RAM.

30.4.1 Binary System

This first example was initially presented by Sung and Cho [18] and later analyzed by Ramirez-Marquez and Coit [6]. This problem has three

subsystems connected in series with three components to provide redundancy. The problem is to obtain a solution for RAP assuming reliability is to be maximized subject to cost and weight constraints with values of 17 and 30, respectively.

This RAP was solved using the proposed algorithm and presents a good example for illustration purposes. Table 30.1 presents data associated with the components reliability and resource characteristics. Table 30.2 illustrates the global cycle of the algorithm as the solution converges.

For this problem the initial potential system design probability defined by vector γ_i equals 0.5. After 14 generations, these initial probabilities have converged to a final solution. Notice how the algorithm immediately identifies the third choice in subsystem 3 as a very poor choice.

Table 30.1. Binary RAP component data

	Subsystem 1		
Choice	Reliability	Cost	Weight
1	0.99	4	2
2	0.95	13	3
3	0.92	7	5
	Subsystem 2		
Choice	Reliability	Cost	Weight
1	0.98	8	3
2	0.8	3	3
3	0.9	3	9
	Subsystem 3		
Choice	Reliability	Cost	Weight
1	0.98	11	4
2	0.92	5	6
3	0	100	100

Table 30.3 illustrates the solutions obtained for this same problem when different initial potential system design probabilities γ_i, are used. The solution for $\gamma_1 = 0.5$ corresponds to the generations described in Table 30.2 and is the optimal solution presented in previous studies [6, 18].

Table 30.2. Component appearance probability convergence by subsystem

Subsystem (λ_1)				Subsystem (λ_7)			
i	1	2	3	i	1	2	3
x_{i1}	0.5	0.5	0.5	x_{i1}	0.33	0.57	0
x_{i1}	0.5	0.5	0.5	x_{i1}	0.73	0	0.57
x_{i1}	0.5	0.5	0.5	x_{i1}	0.23	0	0.27
x_{i2}	0.5	0.5	0.5	x_{i2}	0	0.27	0.13
x_{i2}	0.5	0.5	0.5	x_{i2}	0	0.1	0.13
x_{i2}	0.5	0.5	0.5	x_{i2}	0	0.7	0.07
x_{i3}	0.5	0.5	0.5	x_{i3}	0.07	0	0
x_{i3}	0.5	0.5	0.5	x_{i3}	0	0.03	0
x_{i3}	0.5	0.5	0.5	x_{i3}	0	0	0
Subsystem (λ_3)				Subsystem (λ_{12})			
i	1	2	3	i	1	2	3
x_{i1}	0.53	0.5	0.37	x_{i1}	0.13	1	0
x_{i1}	0.57	0.37	0.57	x_{i1}	1	0	1
x_{i1}	0.3	0.3	0.5	x_{i1}	0.87	0	0
x_{i2}	0.33	0.27	0.4	x_{i2}	0	0.03	0
x_{i2}	0.2	0.4	0.4	x_{i2}	0	0.2	0
x_{i2}	0.3	0.6	0.47	x_{i2}	0	0.77	0
x_{i3}	0.3	0.3	0	x_{i3}	0	0	0
x_{i3}	0.03	0.5	0	x_{i3}	0	0	0
x_{i3}	0.3	0.6	0	x_{i3}	0	0	0
Subsystem (λ_5)				Subsystem (λ_{14})			
i	1	2	3	i	1	2	3
x_{i1}	0.57	0.5	0.17	x_{i1}	0	1	0
x_{i1}	0.67	0.07	0.5	x_{i1}	1	0	1
x_{i1}	0.33	0.03	0.43	x_{i1}	1	0	0
x_{i2}	0.07	0.23	0.13	x_{i2}	0	0	0
x_{i2}	0	0.3	0.3	x_{i2}	0	0	0
x_{i2}	0.07	0.43	0.17	x_{i2}	0	1	0
x_{i3}	0.1	0.03	0	x_{i3}	0	0	0
x_{i3}	0	0.17	0	x_{i3}	0	0	0
x_{i3}	0.07	0.23	0	x_{i3}	0	0	0

Table 30.3. System design as a function of initial appearance probabilities

Initial probability = 0.80			
	Choice		
Subsystem	1	2	3
1	2	0	0
2	1	1	0
3	1	0	0
R=0.9785	C=30	W=14	T=29
Initial probability = 0.75			
	Choice		
Subsystem	1	2	3
1	1	0	0
2	0	3	0
3	0	1	0
R=0.9072	C=18	W=16	T=34
Initial probability = 0.65			
	Choice		
Subsystem	1	2	3
1	2	0	0
2	1	1	0
3	1	0	0
R=0.9785	C=30	W=14	T=39
Initial probability = 0.60			
	Choice		
Subsystem	1	2	3
1	1	0	0
2	2	1	0
3	0	1	0
R=0.9156	C=28	W=17	T=33
Initial probability = 0.50			
	Choice		
Subsystem	1	2	3
1	2	0	0
2	1	1	0
3	1	0	0
R=0.9785	C=30	W=14	T=24

For this specific example the local cycle was not implemented since the rationale was to understand how the global optimization cycle behaved with different initial probabilities. In this respect, it is important to note that for all the experiments run the initial probabilities always converged although not to the optimal solution. Moreover, the algorithm does not require the use of initial solutions

30.4.2 Multistate System with Binary Capacitated Components

The example in this section considers a multi-state system with binary capacitated components. This problem initially presented by Levitin *et al*. [13] was solved under the assumption that cost needed to be minimized subject to a reliability constraint. In order to apply the proposed algorithm to this problem, the minimum cost found by Levitin *et al*. [13] has been used as a constraint and reliability has been maximized.

Although the solutions are not equal, the purpose is to show how the algorithm can be used to generate very good solutions for this highly involved problem.

Table 30.4 presents data associated to the components reliability, nominal capacity and resource characteristics. During a specific time interval the system design must be able to provide 20% of the time 100% of the nominal system demand, 30% of the time 80% of the nominal system demand and the remaining time, 40% of the nominal system demand. A maximum cost of 6.924 is allowed for the system design.

Table 30.5 illustrates the solution obtained through the global and local cycles. The global cycle converged after 31 generations but for this example, the top solution in generation 20 yielded the best solution.

Finally, Figure 30.2 illustrates how the reliability and cost for the top solution converge as a function of the generations in the global cycle.

Table 30.4. Binary capacitated component data

Component Type 1			
Subsystem	K	R	C
1	0.5	0.97	0.52
2	0.2	0.967	0.516
3	0.6	0.959	0.214
4	0.25	0.989	0.683
Component Type 2			
Subsystem	K	R	C
1	0.8	0.964	0.62
2	0.5	0.914	0.916
3	0.9	0.97	0.384
4	0.25	0.979	0.645
Component Type 3			
Subsystem	K	R	C
1	0.8	0.98	0.72
2	0.5	0.96	0.967
3	1.8	0.959	0.534
4	0.3	0.98	0.697
Component Type 4			
Subsystem	K	R	C
1	1	0.969	0.89
2	0.5	0.953	1.367
3	2	0.96	0.614
4	0.7	0.96	1.19
Component Type 5			
Subsystem	K	R	C
1	1.5	0.96	1.02
2	-	-	
3	2	0.97	0.783
4	0.7	0.98	1.26
Component Type 6			
Subsystem	K	R	C
1	-	-	
2	-	-	
3	2.4	0.96	0.813
4	-	-	

Table 30.5. Solutions for the binary capacitated multistate problem

Global cycle								
Subsystem	Design choice						Total	
	1	2	3	4	5	6	C	R
1	0	0	0	0	1	0	1.020	0.9600
2	0	3	0	0	0	0	2.748	0.9893
3	4	0	0	0	0	0	0.856	0.9999
4	0	0	1	0	1	0	1.957	0.9704
T = 279	System						6.581	0.9215
Local cycle								
Subsystem	Design choice						Total	
	1	2	3	4	5	6	C	R
1	1	0	1	0	0	0	1.240	0.9830
2	0	2	1	0	0	0	2.799	0.9940
3	4	0	0	0	0	0	0.856	0.9999
4	0	0	1	0	1	0	1.957	0.9704
T = 142	System						6.852	0.9481

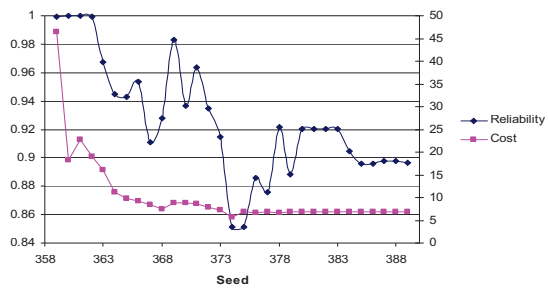


Figure 30.2. Reliability and cost convergence for optimal solution

30.4.3 Multistate System with Multistate Components

The remaining example constitutes the first time the RAP is considered for multistate series-parallel systems with multistate components. This problem was randomly generated assuming a demand of 10 units and a maximum cost of 60 units. Table 30.6 presents component states and cost while, Table 30.7 component states probability.

Table 30.8 illustrates the global and final solution design obtained from the algorithm. These solutions were obtained after 33 generations developed by the global cycle.

Table 30.6. Components states and cost

Subsystem	State choice 1				Cost
1	0	1	2	5	4
2	0	2	3	4	7
3	0	1	2	3	2
4	0	1	3	5	4
Subsystem	State choice 2				Cost
1	0	2	5	7	3
2	0	1	3	4	4
3	0	1	4	6	4
4	0	1	3	6	5
Subsystem	State choice 3				Cost
1	0	1	2	3	3
2	0	2	3	5	3
3	0	1	3	4	5
4	0	1	3	4	5
Subsystem	State choice 4				Cost
1	0	1	2	4	4
2	0	1	3	5	4
3	0	1	2	5	3
4	0	2	3	6	3

Table 30.7. Component state probabilities

Subsystem	State probabilities Choice 1			
1	0.05	0.20	0.10	0.65
2	0.10	0.15	0.10	0.65
3	0.08	0.10	0.15	0.67
4	0.06	0.10	0.10	0.74
Subsystem	State probabilities State choice 2			
1	0.05	0.10	0.15	0.70
2	0.02	0.10	0.10	0.78
3	0.01	0.10	0.10	0.79
4	0.01	0.05	0.10	0.84
Subsystem	State probabilities State choice 3			
1	0.02	0.10	0.10	0.78
2	0.01	0.10	0.20	0.69
3	0.05	0.05	0.10	0.80
4	0.01	0.10	0.20	0.69
Subsystem	State probabilities State choice 4			
1	0.01	0.05	0.15	0.79
2	0.02	0.10	0.20	0.68
3	0.01	0.05	0.10	0.84
4	0.05	0.05	0.15	0.75

Table 30.8. Converged and best solution designs

Converged solution subsystem	Design choice			
	1	2	3	4
1	1	2	0	1
2	0	0	3	1
3	1	2	0	1
4	1	1	1	2
R=0.9669	C= 60		T= 234.8	
Best solution subsystem	Design choice			
	1	2	3	4
1	0	3	0	1
2	0	0	3	1
3	2	2	0	1
4	0	1	1	3
R=0.9845	C= 59		T= 234.8	

Finally, Tables 30.9 and 30.10 illustrate four generations that represent how the initial probabilities, γ_i, = 0.5, changed as the solution converged. Similarly, they present the top four solutions, with respective reliability and cost, for each generation λ.

Table 30.9. Solution convergence for generations λ = 4 and 12

λ_4	Subsystem			
i	1	2	3	4
x_{i1}	0.5	0.5	0.5	0.5
x_{i1}	0.5	0.5	0.5	0.5
x_{i1}	0.5	0.5	0.5	0.5
x_{i2}	0.5	0.5	0.5	0.5
x_{i2}	0.5	0.5	0.5	0.5
x_{i2}	0.5	0.5	0.5	0.5
x_{i3}	0.5	0.5	0.5	0.5
x_{i3}	0.5	0.5	0.5	0.5
x_{i3}	0.5	0.5	0.5	0.5
x_{i4}	0.5	0.5	0.5	0.5
x_{i4}	0.5	0.5	0.5	0.5
x_{i4}	0.5	0.5	0.5	0.5
R	0.9910	0.9801	0.954	0.9551
C	80	79	76	79

Table 30.9. (continued)

λ_{12}	Subsystem			
i	1	2	3	4
x_{i1}	0.13	0	0.73	0.07
x_{i1}	0.57	0.2	0.53	0.07
x_{i1}	0.1	0	0.43	0.47
x_{i2}	0.8	0	0.83	0.37
x_{i2}	1	0.37	0.83	0
x_{i2}	0.47	0.27	0.23	0.17
x_{i3}	0.27	0.7	0	0.73
x_{i3}	0	0.97	0	0
x_{i3}	0.03	0.53	0	0.3
x_{i4}	0.17	0.2	0.33	0.6
x_{i4}	0.33	0	0.13	0.3
x_{i4}	0.23	0.77	0.2	0.83
R	0.9722	0.9568	0.9184	0.9414
C	60	60	60	58

Table 30.10. Solution convergence for generations $\lambda = 16$ and 28

λ_{16}	Subsystem			
i	1	2	3	4
x_{i1}	0	0	0.77	0.07
x_{i1}	0.27	0	0.43	0
x_{i1}	0	0	0.3	0.27
x_{i2}	1	0	1	0.3
x_{i2}	1	0.5	0.93	0
x_{i2}	0.2	0.1	0	0.17
x_{i3}	0.4	0.93	0	0.63
x_{i3}	0	1	0	0
x_{i3}	0	0.63	0	0.43
x_{i4}	0.13	0.43	0.73	0.5
x_{i4}	0.53	0	0.03	0.73
x_{i4}	0.13	1	0	1
R	0.9577	0.9739	0.9679	0.9642
C	59	58	58	58

Table 30.10. (continued)

λ_{28}	Subsystem			
i	1	2	3	4
x_{i1}	0	0	0.53	0
x_{i1}	1	0	0.4	0
x_{i1}	0	0	0.07	0.93
x_{i2}	1	0	1	0
x_{i2}	1	0	1	0
x_{i2}	0	0	0	0.4
x_{i3}	0.13	1	0	0.93
x_{i3}	0	1	0	0
x_{i3}	0	1	0	0.33
x_{i4}	0	0.03	1	0.03
x_{i4}	1	0	0	1
x_{i4}	0	1	0	1
R	0.978	0.9745	0.9701	0.9694
C	60	60	60	60

References

[1] Kuo W, Prasad V, Tillman F, Hwang C. Optimal reliability design: Fundamentals and applications. Cambridge University Press, 2000.

[2] Fyffe D, Hines W, Lee NK. System reliability allocation and a computational algorithm. IEEE Transactions on Reliability 1968; R-17: 64–69.

[3] Ghare P, Taylor R. Optimal redundancy for reliability in series system. Operations Research 1969;17:838–847.

[4] Bulfin R, Liu C. Optimal allocation of redundant components for large systems. IEEE Transactions on Reliability 1985; R-34, 241–247.

[5] Coit D, Smith A. Reliability optimization of series-parallel systems using a genetic algorithm. IEEE Transactions on Reliability 1996; R-45:254–266.

[6] Ramirez-Marquez, J, Coit D, Konak A. Reliability optimization of series-parallel systems using a max-min approach. IIE Transactions 2004; 36:891–898.

[7] Lee H, Kuo W, Ha C. Comparison of max-min approach and NN method for reliability optimization of series-parallel system. Journal of System Science and Systems Engineering 2003; 12, 39–48.

[8] Nakagawa Y, Nakashima K. A heuristic method for determining optimal reliability allocation. IEEE Transaction on Reliability 1977; R- 26:156–161.
[9] Coit D, Konak A. Multiple weighted objectives heuristic for the redundancy allocation problem. IEEE Transactions on Reliability 2006.
[10] Billinton R, Zhang W. State extension for adequacy evaluation of composite power systems-applications. IEEE Transactions on Power Systems 2000; 15:427–432.
[11] Levitin G, Lisnianski A. Multi-state system reliability. Series on Quality, Reliability and Engineering Statistics. World Scientific Publishing, Singapore 2003; 6.
[12] Ramirez-Marquez JE, Coit D. A heuristic for solving the redundancy allocation problem for multistate series-parallel systems. Reliability Engineering and System Safety 2004; 83:341-349.
[13] Levitin G, Lisnianski A, Ben-Haim, H, Elmakis D. Redundancy optimization for series-parallel multi-state systems. IEEE Transactions on Reliability 1998; R-47:165–172.
[14] Ramirez-Marquez J, Coit D, Tortorella M. A generalized multistate based path vector approach for multistate two-terminal reliability. IIE Transactions 2006; 38: 477–488.
[15] Lisnianski A, Levitin G, Ben-Haim H, Elmakis D. Power system structure optimization subject to reliability constraints. Electric Power Systems Research 1996; 39:145–152.
[16] Yeh W. Multistate node acyclic network reliability evaluation. Reliability Engineering and System Safety 2002; 78:123–129.
[17] Ford L. Fulkerson D. Flows in networks. Princeton University Press, Princeton, NJ, 1962.
[18] Sung S, Cho Y. Branch and bound redundancy optimization for a series system with multiple-choice constraints. IEEE Transactions on Reliability 1999; R-48:108–117.

31

New Approaches to System Analysis and Design: A Review

Hong-Zhong Huang[1], Liping He[2]

[1]School of Mechatronics Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, 610054, China
[2]School of Mechanical Engineering, Dalian University of Technology, Dalian, Liaoning, 116023, China

Abstract: Engineering design under uncertainty has gained considerable attention in recent years. A variety of reliability analysis strategies and methodologies are taken into account and applied increasingly to accommodate uncertainties. There exist two different types of uncertainties in practical engineering application: aleatory uncertainty, which is classified as objective and irreducible uncertainty with sufficient information on input uncertainty data and epistemic uncertainty, which is a subjective and reducible uncertainty that stems from a lack of knowledge on input uncertainty data. The nature of uncertainty depends on the mathematical theory within which problem situations are formalized. When sufficient data is available, probability theory is very effective to quantify uncertainty. However, when data is scarce or there is lack of information, the probabilistic methodology may not be appropriate. Among several alternative tools, possibility theory and evidence theory have proved to be computationally efficient and stable tools for reliability analysis under aleatory and/or epistemic uncertainty involved in engineering systems. Thus this chapter first attempts to give a better understanding of uncertainty in engineering design with a holistic view of its classifications, theories and design consideration, and then discusses general topics of foundations and applications of possibility theory and evidence theory. The overview includes theoretical research, computational development and performability improvement about possibilistic and evidential methodologies in the area of reliability during recent years, and it especially reveals the capability and characteristics of quantifying uncertainty from different angles. Finally, perspectives on future research directions are stated.

31.1 Introduction

One of the greatest challenges in engineering design is uncertainty, which can be observed from both epistemological and methodological angles in various environments. There has been an ever-increasing tendency to take uncertainty qualification analysis into account over the last two decades. In fact, uncertainty is associated with both qualitative and quantitative characteristics of design problems. The nature of uncertainty depends on the mathematical theory within which problems are formalized [1], and each method emphasizes a different paradigm [2]. The more general the theory is, the more types of uncertainty can be described by it. Mainly in response to criticism on the credibility of standard probabilistic analysis, the theories and methodologies that we summarize to deal with

uncertainty will shed light on practical problems in engineering design to be dealt with later.

31.1.1 Definitions and Classifications of Uncertainty

People often use different terms as synonyms of uncertainty: indefiniteness, unpredictability, indeterminacy, changeability, irregularity, arbitrariness, ambiguity, vagueness, randomness, variability and haphazardness, *etc*. [3], although each term has some specific nuances in meaning.

Uncertainty has several definitions. To a certain degree, it is associated with phenomena that are questionable, problematical, not definite or not determined, or not having certain knowledge, or even liable to change or to vary. The word uncertainty often refers to random variability. Uncertainty is also connected with the degree of belief in the validity of a particular proposition or datum [3]. Uncertainty can be categorized as aleatory uncertainty, epistemic uncertainty and error [4], [5], and [6], as illustrated in Figure 31.1.

In view of descriptions of the degree of uncertainty and simplifications of systems, uncertainty can naturally be categorized according to different meanings, as seen in Figure 31.2, which plays a fundamental role in the relevant theories between uncertainty and information [2].

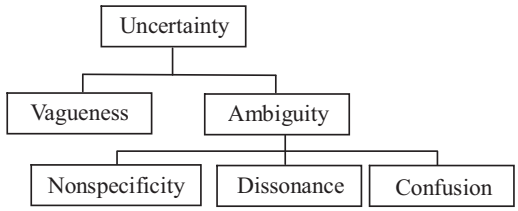


Figure 31.2. A semantic classification of uncertainty [2]

31.1.2 Theories and Measures of Uncertainty

There is an abundant collection of theories for modeling all types of uncertainty. Before fuzzy measure was proposed by Sugeno [7], probability theory was the dominant way to model uncertainty, especially for stochastic uncertainty when there is sufficient information supplied. However, this theory is not appropriate for reducible uncertainty and error because the additivity axioms, which the

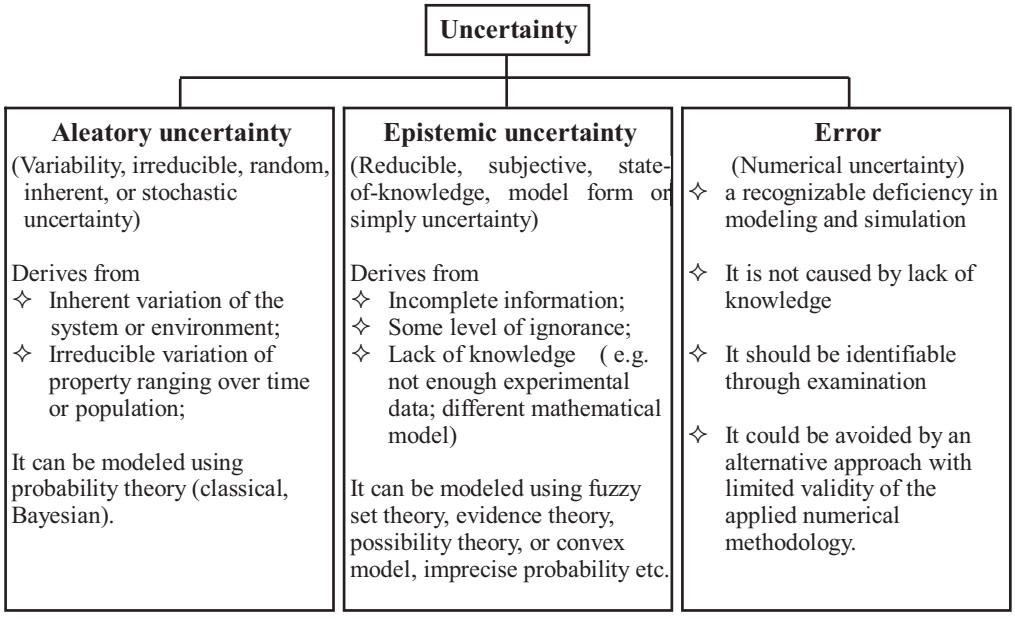


Figure 31.1. A well-known classification of uncertainty [4], [5], and [6]

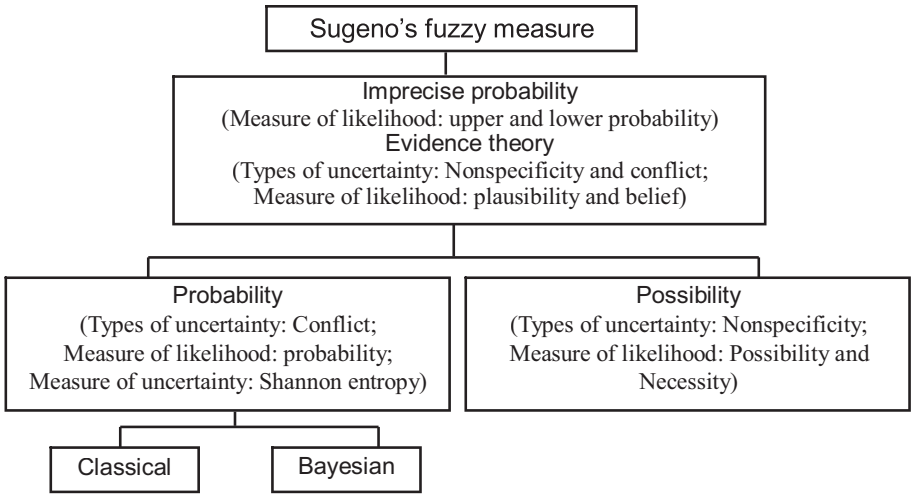


Figure 31.3. Families of theories of uncertainty [8]

probability theory relies on, are unable to express the lack of knowledge in scarce-data situations. Therefore, alternative uncertainty analysis tools such as imprecise probability and evidence theory, have been developed, which can be combined with probability theory to develop a framework in a specific field [8], *e.g.*, risk assessment of systems. And these theories are flexible enough to model both non-specificity and conflict types of uncertainty (see the classification in Figure 31.2.). A family of theories of uncertainty is presented in Figure 31.3.

After viewing the various types of uncertainty, Klir investigated their relation to information and complexity [1], [2], by the reason that each type of uncertainty requires a distinct framework within which appropriate measures of the corresponding type of uncertainty must be formulated. The understanding that measures are related to types of uncertainty has been widely accepted. The formulae are shown in Table 31.1.

Table 31.1. A Summary of measures of uncertainty by Klir [2]

Type	Name	Formula	Notation
Classical	Hartley information	$I(N)=\log_2 N$	U: a universal domain A: a crisp set of U N : cardinality of a crisp set P: probability distribution $P=(p_1,p_2,\cdots,p_n)$ Π: possibility distribution $\Pi=(\pi_1,\pi_2,\cdots,\pi_n)$ $\mu_A(u)$:membership function C :fuzzy complement m : a basic probability assignment (a mass function) **F** : set of focal elements $B_{el}(\cdot)$: belief measure $P_l(\cdot)$: plausibility measure
	Shannon entropy	$H(P)=-\sum_{i=1}^{n} p_i \log_2 p_i$	
General	U-uncertainty	$U(\Pi)=\sum_{i=1}^{n}(\pi_i-\pi_{i+1})\log_2 i$	
Vagueness	Measure of fuzziness	$f_C(A)=\lvert X\rvert-\sum_{u\in U}\lvert\mu_A(u)-C(\mu_A(u))\rvert$	
Ambiguity	Measure of non-specificity	$V(m)=\sum_{A\in\mathbf{F}} m(A)\log_2\lvert A\rvert$	
	Measure of dissonance	$E(m)=-\sum_{A\in\mathbf{F}} m(A)\log_2 P_l(A)$	
	Measure of confusion	$C(m)=-\sum_{A\in\mathbf{F}} m(A)\log_2 B_{el}(A)$	

31.1.3 Uncertainty Encountered in Design

In complicated situations of reliability analysis and engineering design, we encounter many indeterminable factors, both during the early stages of design, and in the manufacturing processes and use, due to lack of knowledge or the incomplete information. Common reasons for the lack of statistical data include the increased complexity of large-scale systems, the collection of statistical data being difficult and/or costly, the rarity of failures in some highly reliable systems, and data being imprecise or unavailable under various testing conditions.

The characteristics and formalisms of uncertainty have to be mathematically quantified, before a designer can seek the optimum design. A design or decision problem should take into account the main types of uncertainties arising during the design (manufacturing tolerances, uncontrollable variations in external operating conditions), uncertainties in decision making (vagueness in conflicting objectives), modeling and simulation [6]. Moreover, the experience and subjective assessment of experts is often given in natural language, which introduces vagueness and impreciseness [9], [10] and [11] Furthermore, in the investigation of complex man-made systems and multi-state systems, inaccuracy caused by human errors or poor definitions of failure should also be considered. It is inappropriate to represent all of them solely by probabilistic properties and the uncertainties in such cases are typically referred to as epistemic.

The aim of this chapter is to present a holistic view on reliability analysis and optimization methods in the context of possibility theory and evidence theory in engineering area when data is insufficient, mainly under epistemic uncertainty.

The outline of the remaining part of this chapter is as follows. Section 31.2 deals with the fundamentals of possibility theory and evidence theory and their applications. Sections 31.3 to 31.5 address various applications of possibility theory and evidence theory in engineering design, illustrating their superiority in handling epistemic uncertainty information especially for reliability analysis. Section 31.6 provides an indication of application of possibility theory and evidence theory to engineering designs. Concluding remarks are provided in the last section of the chapter.

31.2 General Topics of Applications of Possibility Theory and Evidence Theory

31.2.1 Basics of Possibility Theory and Evidence Theory

As one of three constituents of fuzzy theory (the others are fuzzy set theory and fuzzy logic, respectively) [12], possibility theory was originally introduced by Zadeh [13] to express the intrinsic fuzziness of natural languages as well as uncertainty information. Among all the multifarious interpretations of possibility theory, the fuzzy set interpretation is well-known and prominent. Possibility theory may be viewed as a special branch of fuzzy measure theory, which is based upon two dual fuzzy measures, *possibility measure* and *necessity measure*.

Compared with probability theory, possibility theory is similar to the former because it is a tool to represent uncertainty based on set functions. The difference between them, in the aspect of the axiom, is that probability is additive whereas possibility is subadditive [8]; with a view to information involved, probability is a quantitative ratio scale of uncertainly while possibility can be considered as a quasi-qualitative ordinal scale [4].

Evidence theory (or Dempster–Shafer theory) may be viewed as a branch of mathematics considering the combination of empirical evidence to construct a coherent picture of reality [14]. Compared with Bayesian theory, evidence theory is generally felt to be closer to our human perception and reasoning processes [15]. There have been many interpretations of evidence theory and also closely related developments. The most influential version is still Shafer's presentation in his book [16].Two large classes of fuzzy measures, referred to as *belief measure* and *plausibility measure*, respectively, characterize the theory of evidence. In fact, the classical probability theory is a subset of the possibility theory, which in turn, is

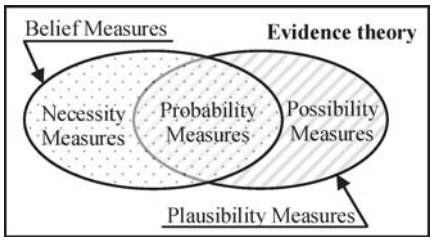


Figure 31.4. A pictorial description of uncertainty classification based on fuzzy measures

a subset of the evidence theory [2], seen in Figure 31.4.

31.2.2 Introduction to General Applications

Both possibility theory and evidence theory have been used recently in reliability analysis and uncertainty handling.

Possibility theory has been applied in many areas, including artificial intelligence, approximate reasoning, decision making, and data fusion [17]. It is usually used to quantify only epistemic uncertainty if there is no conflicting evidence among experts [18]. In the area of reliability engineering, the reliability estimation and design was investigated by Möller *et al.* [19], Kozine *et al*. [20], Mourelatos [21], and Huang *et al.* [22], and [23]. Besides reliability engineering, the application areas also cover civil (or structural) engineering engineering [19], computational mechanics, military, energy, forestry, aerospace and automobile engineering, and others.

As a more general uncertainty analysis tool, evidence theory has also been applied in many areas, including artificial intelligence [8] and [24], object detection and approximate reasoning [25] and [26], design optimization [27], uncertainty quantification [24], risk and reliability evaluation, pattern recognition and image analysis, decision making [28], data fusion [29], and fault diagnosis [30] and [31]. However, the popularity of evidence theory has remained low because evidence theory requires epistemological assumptions that are at odds with those underlying classical and Bayesian probability theories [14].

There is a tendency to use not only one framework to deal with complicated and changeful environments, *e.g*., integration of probabilistic approach and possibilistic approaches, of probabilistic and evidential approaches, *etc*.

The existing applications and developments of possibility theory and evidence theory, on the subject of uncertainty and reliability analysis of recent works, mainly focus on the following two aspects: theoretic development, which is related to the fundamentals or foundation of reliability theory, *e.g*., fuzzy reliability and imprecise reliability and computational (or algorithmic) development, which particularly emphasizes the analysis and design method, *e.g*., data fusion technology applied in reliability assessment and optimum design methods.

31.3 Theoretical Development in the Area of Reliability

31.3.1 Fuzzy Reliability

One tool to cope with the imprecision of available information in reliability analysis is fuzzy reliability theory, which was proposed by Cai [32]–[34] and has been developed by several other researchers [35]–[38], [39], who employed possibility theory as uncertainty analysis tools.

31.3.1.1 Motivation and Classifications

The origin of fuzzy reliability theory comes from the consideration of reliability aspects in gracefully degradable computing systems, where system states cannot be simply classified as failed or functioning. In addition to the nature of performance degradation, a failure does not necessarily occur at random.

Various forms of fuzzy reliability theories, including profust reliability theory [34], [37], posbist reliability theory [32], [40], and posfust reliability theory, have been proposed based on new assumptions of fuzzy state or possibility measure in place of the binary state and probability assumptions. The structure of fuzzy reliability theory is illustrated as Figure 31.5.

Possibility theory-based reliability theory can be classified as not only a member of fuzzy reliability theory, but also a member of non-

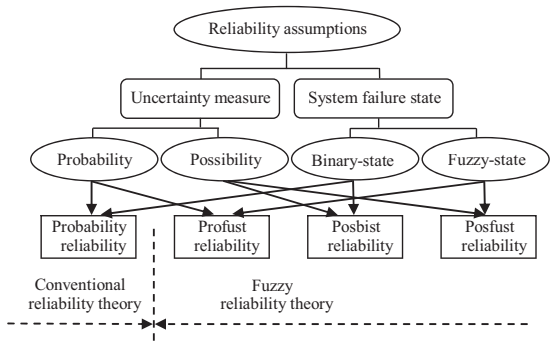


Figure 31.5. Reliability theories based on various fundamental assumptions

probabilistic or imprecise reliability theory. The former classification is due to the theoretic background of fuzzy set theory, while the latter classification is due to the non-statistical characteristics of the information involved.

31.3.1.2 Present Status and Challenging Problems

To date, most existing works are in theoretic construction and modification [39], [35]–[42], or practical connections in engineering [18], [19], [24] and [43]. Cai *et al.,* considered posbist reliability theory of typical systems, such as series, parallel, *k*-out-of-*n* systems [32], and cold and warm redundant systems [38]. Utkin *et al.* [44] provided an analysis of typical repairable systems in the possibility context. Aiming at more changeful systems, Utkin *et al.* [40] proposed a general formal approach to analyze the posbist reliability behavior of arbitrary systems by a system of functional equations, on the basis of a state transition diagram, which can avoid the extremely difficult time-domain analysis of the reliability behaviour.

Systematic work on maintenance policy and FTA in the presence of fuzzy state assumption has only been partially done. Huang and Tong [45] have developed a new model of fault tree analysis corresponding to posbist reliability theory to evaluate system reliability and safety when the statistical data is scarce or the failure probability is extremely small. With the concept of possibilistic logic proposed by Dubois and Prade [46], a new knowledge-based solution enables possibility theory to achieve wider applications in artificial intelligence or data fusion domain, compared with probability theory and evidence theory.

The exploration of fuzzy reliability theory itself and its extensions is not enough. Some difficulties are seen by practitioners in that this theory does not cover a large variety of possible judgments in reliability [47]. In some real cases, there does not exist a certain type of possibility distribution that is reasonably consistent with statistical data. A clear interpretation of the possibility distribution is further expected.

31.3.2 Imprecise Reliability

31.3.2.1 Origin and Objectives

In order to overcome the forementioned difficulties, the theory of imprecise probabilities and its analogs (the theory of *interval statistical models* and the theory of *interval probability*) [47] have been used as a unified tool for reliability and risk analysis. Here, the term imprecise probabilities is used as a generic one to cover mathematical models such as *upper and lower probabilities*, *upper* and *lower previsions* (or *expectations*), *possibilities* and *necessities*, *belief* and *plausibility* functions, and other qualitative models [20].

The general motivation for imprecise probabilities is that the confidence of a decision maker mainly depends on the evidence on which a probability estimate is based. Mathematical assumptions can lead to imprecision and further sources of uncertainty. Hence a main objective of imprecise reliability is to use only available information without additional assumptions or, even with a minimal number of assumptions to obtain the component reliability level and the best possible reliability bound. Furthermore, the effects of any possible imprecision of initial information can be reflected *via* the imprecision of resulting system reliability measures [47]. Conventional reliability models can be classified as a special case of imprecise models.

31.3.2.2 Development and Directions

Imprecise probabilities have been used in practical reliability and risk analysis by characterizing the state-of-knowledge uncertainty with intervals of probabilities. There are several theories of imprecise probabilities, including evidence theory and possibility theory. Moreover, recently a theory of *coherent imprecise probabilities* has been developed by Walley [48].

The coherent imprecise probability theories [48] are based on a behavioral interpretation and three fundamental principles, *i.e*., avoiding sure loss, coherence and natural extension. The basic concept associated with the behavioral interpretation is the concept of a gamble, which is a bounded real-valued function defined on domain Ω and which should be interpreted as a reward whose value depends on the uncertain state, each belongs to the domain Ω , in the context of decision theory and utility theory. The coherent imprecise probability theories are also based on two probabilistic models: *lower previsions* (or expectations) and *upper previsions*. In reliability and risk analysis problems, we will consider a particular case of gamble for which the reward can be either 0 or 1. In this case, lower and upper previsions are called *lower* and *upper probabilities*, respectively, just as the name means.

The combinative rules of multi-source information discriminate between consistent and inconsistent judgments (or models). The former contains the conjunction rule, which combines lower and upper previsions for the two consistent judgments; the latter includes an alternative one called the unanimity rule. These rules were obtained based on the concept of desirability and preference [48].

Kozine and Filimomov [20] developed imprecise probabilities as a particularly advantageous way of handling indeterminacy and summarized their experiences in dealing with the evidence theory relating to reliability assessments. With practical system reliability assessments for serial, parallel and general reliability structures, they demonstrated the advances in the application of the theory of coherent imprecise probabilities for system reliability assessments.

Aughenbaugh *et al.* [49] considered imprecise probabilities to express clearly the precision with which something is known, on the hypothesis that it is valuable to represent this imprecision by using imprecise probabilities in engineering design. Then, the example of the pressure vessel design problem was presented using two approaches, both variations of utility-based decision making. The computational experiments demonstrated that when designers only have access to a small set of sample data, a probability bounds analysis (PBA) approach that uses imprecise probabilities to model uncertainty can lead, on average, to better designs than a purely probabilistic approach.

Coolen [50] discussed a variety of issues (involving advantages and disadvantages) and reviewing the issues suggested applications of imprecise probability in reliability. A recently developed statistical approach, called *non-parametric predictive inference* (NPI), to reliability has been introduced as a coherent framework offering exciting opportunities when data is scarce, where inferences are directly on future observable random quantities such as the random time to failure of the next system. In this approach, imprecision depends on the available data in an intuitive way, as it decreases if information is added. Applications with regard to replacement and maintenance decisions were also presented.

Hall and Lawry [51] introduced a new method for constructing an imprecise limit state function from scarce data based on minimal assumptions about the underlying system behavior. A case study of reliability analysis has demonstrated how this conventional approach can be extended to handle imprecise knowledge about the system state variables, represented in general as random sets, in order to generate bounds on the probability of failure. The approach has provided new insights into the sources of uncertainty and the assumptions implicit in the conventional probabilistic approach.

We can conclude from those results that it is valuable to explicitly represent the imprecision in the available characterization of uncertainties with imprecise probabilities. A further introduction and examples of imprecise reliability analysis can be found in [8].

Although the applications of imprecise probability methods in reliability have shed light on many interesting research problems, some unsatisfactory points have been criticized (*e.g.,* difficulties of evidence combinations, diversity of judgments admitted in elicitation, *etc*.). By far the main difficulty in imprecise reliability is computation for imprecise probability. Recent work by Utkin and co-authors [47] has provided great progress in this aspect, yet much more needs to be done. Another topic that has not yet been studied is the design of experiments with uncertainty quantified *via* imprecise probabilities [8] and [50]. From this perspective, further research in this field may be of great benefit in future.

31.4 Computational Developments in the Reliability Area

To a certain extent, reliability analysis using the proposed possibilistic and evidential methods cannot be completely separated from reliability-based design optimization (RBDO).

Design optimization is now a mainstream discipline in high technology product development and a natural extension of the ever-increasing analytical abilities of computer-aided engineering [52]. The process of obtaining optimal designs with the availability of complex simulation models of actual systems is known as design optimization. It assumes a decision-making paradigm for the design process in the form of mathematical programming and the main criteria used to measure the effectiveness in a practical engineering optimization problem are cost and performance.

The presence of uncertainties in engineering practice complicates a the design problem of a system. Although the RBDO approach has a more consistent description of the safety of designs, it has a higher computational cost and the calculations may not always converge. Hence design methods considering uncertainty have been increasingly applied and various specialized optimization methodologies have been proposed in areas where it is not possible to obtain accurate statistical data due to restriction of resources or conditions (such as budgets, facilities, time, human factors, *etc*.).

The concrete design optimization methods can be categorized as the parallel-loop method, the serial-loop method, the single-loop method, and the adaptive-loop method. Because they are based on theories of uncertainty, these methods can be classified as the *probabilistic* (or statistical) approach and the *possibilistic* approach. The former approach includes *asymptotic reliability analysis*, *the first-order reliability method* (FORM), *the second-order reliability method* (SORM), Monte Carlo simulation (MCS), and the Bayesian method, *etc*.. The second approach involves interval analysis, convex modeling, and fuzzy modeling [39]. In addition, a unified approach integrates the two methods in a general framework. There have been some advances in exploring decomposition strategies or approximation concepts, as discussed next.

31.4.1 Possibility-based Design Optimization (PBDO)

The general PBDO can be formulated as

$$\begin{aligned} &\min \quad Cost(\mathbf{d}, \mathbf{Y}) \\ &\text{s.t.} \quad \Pi\left(G_i\left(\mathbf{d}(\mathbf{Y})\right) > 0\right) \le \alpha_{t_i},\ i = 1, 2, \cdots, np \\ &\mathbf{d}^L \le \mathbf{d} \le \mathbf{d}^U,\ \mathbf{d} = \mu(\mathbf{Y}) \in \mathbb{R}^n,\ \mathbf{Y} = [Y_i]^T \in \mathbb{R}^{nr} \end{aligned} \tag{31.1}$$

where $\mathbf{d}$ and $\mathbf{Y}$ are the design vector and the fuzzy random vector, respectively, while α_t is a target failure possibility. Moreover, n, nr, np are the number of design variables, the number of fuzzy random variables, and the number of possibility constraints, respectively.

Compared to other methods, the fuzzy (or possibilistic) analysis method is a very useful tool with the following main advantages: (1) It preserves the intrinsic random nature of physical variables through their membership functions. (2) The extended fuzzy operations are simpler than those using probability. (3) It yields a more conservative design than the probabilistic design method in terms of a confidence level. (4) It provides a system-level possibility different from reliability analysis. For numerical methods of fuzzy analysis, some reported methods [39], [50] are listed as: *the vertex method*, *the discretization method*, *the level-cuts (α-cuts) method*, *the*

Table 31.2. Comparison of PMA in RBDO and PBDO

Issues	PMA in RBDO	PMA in PBDO
Formulation	$\min \quad Cost(\mathbf{d};\mathbf{X})$ s.t. $G_{pi}(\mathbf{d}(\mathbf{X})) \le 0,(i=1,2,\cdots,np)$ $\mathbf{d}^L \le \mathbf{d} \le \mathbf{d}^U$	$\min \quad Cost(\mathbf{d};\mathbf{Y})$ s.t. $G_{\pi i}(\mathbf{d}(\mathbf{Y})) \le 0,(i=1,2,\cdots,np)$ $\mathbf{d}^L \le \mathbf{d} \le \mathbf{d}^U$
Objective and constraints	$Cost(\mathbf{d})$: Deterministic material cost, random quality loss and random manufacturing cost. G_{pi} : the ith probabilistic constraints	$Cost(\mathbf{d})$: Deterministic material cost, random quality loss and random manufacturing cost. $G_{\pi i}$: the ith possibilistic constraints
Evaluation of constraints	$\min \ G(\mathbf{U})$ s.t. $\|\mathbf{U}\|_2 \le \beta_t$	$\min \ G(\mathbf{V})$ s.t. $\|\mathbf{U}\|_\infty \le 1-\alpha_t$
Variables and parameters	$\mathbf{X}$: random variable $\mathbf{U}$: standard normal random variable $\mathbf{d}$: design variable. $\mathbf{d}=\mu(\mathbf{X}) \in R^n$ β_t : target reliability index or target reliability level	$\mathbf{Y}$: non-interactive fuzzy variables $\mathbf{V}$: fuzzy variable with isosceles triangular membership $\mathbf{d}$: design variable, $\mathbf{d}=\{\max[\Pi_{Y_i}(y_i)]\}$ α_t : target failure possibility

multilevel-cut method, *the possibility index approach*, *the performance measure approach* (PMA), *the most probable point* (MPP) *search* and *maximal possibility search* (MPS), *etc*.

In practical engineering design, the vertex method is popular but rather expensive and may yield inaccurate results of fuzzy analysis in the case when an output response has a maximum or minimum within the input range. A level-cuts method has been used to overcome the difficulties of non-linear problems using various design levels. Recently, a multilevel-cut method has been developed to improve the accuracy of the vertex method for non-linear structural design, but it is also very expensive to carry out PBDO with this method. However, PMA has been successfully applied with its advantages of numerical efficiency and stability in PBDO [50], [53].

Both RBDO and PBDO employ PMA to improve numerical efficiency, stability and accuracy. The difference of PMA in the reliability analysis [50], [53] and in fuzzy analysis [39] is illustrated in Table 31.2.

The fuzzy analysis method is different from reliability analysis in the following two aspects. Firstly, MPP in reliability analysis based on FORM results in a first order approximation, whereas MPP in fuzzy analysis is exact along with the related possibility. Secondly, their search domain is different, *i.e*., an *nr*-dimensional sphere in reliability analysis but an *nr*-dimensional hyper-cube in fuzzy analysis, thus leading to simpler computation in fuzzy analysis [54].

At present, one of the main concerns related to PBDO research is how to improve numerical efficiency, accuracy and stability during the optimization process. PMA is such a method satisfying the requirement, by replacing the probabilistic constraint with the performance measure under a specified reliability level [53], [55]. Choi *et al.* [54] provided a new formulation of PBDO using PMA to improve numerical efficiency, stability, and accuracy. They also proposed a new MPS method to resolve disadvantages of the vertex method and the multilevel-cut method, by evaluating possibility

constraints efficiently and accurately for non-linear structural applications. Youn and Choi [56] presented an integrated design platform of both RBDO and PBDO using PMA when modeling physical uncertainty with insufficient information. Mourelatos and Zhou [21] presented a hybrid optimization approach for calculation of the confidence level of fuzzy response efficiently. Although PMA is less expensive when the reliability index is very high, Tu and Choi [57] revealed that it might require more computations when the reliability index is lower than the required reliability level.

In order to improve computational efficiency and stability, the *enriched performance measure approach* (PMA+) has been proposed as an extension of PMA. It combines four key ideas [55]: a way to launch RBDO at a deterministic optimum design, a probabilistic feasibility check, an enhanced *hybrid-mean value* (HMV+) method, and a fast reliability analysis under the condition of design closeness.

Another concern of the extension of PBDO is to provide a general framework integrating various proposed design optimization methodologies such as RBDO, PBDO *etc*., under aleatory uncertainty or epistemic uncertainty, or both of them.

Researchers [8], [39] also consider the PBDO problem of design for maximal safety under uncertainty. It is shown that more conservative results are obtained with PBDO that may be appropriate especially for design against catastrophic failure compared with the probability-based design in reliability assessment. The existing work related to PBDO revealed the characteristics and advantages of the possibility theory for coherent systems; but a general solution (not only referring to method or algorithms) of all uncertainty-based optimization under diverse uncertainties is still needed, which could be the future direction of research.

31.4.2 Evidence-based Design Optimization (EBDO)

Recently, evidence theory has shown its qualitative value and computational efficiency in engineering design if limited and even conflicting information is provided from expert elicitation or experiments, by means of combining aleatory and epistemic uncertainty in a straightforward way.

However, to the best of our knowledge, reported exploration of evidence theory in engineering design is fairly limited, and even much less in a design optimization framework. It is only recently that evidence-based methods have been used to propagate epistemic uncertainty [52], [58]. One of the major difficulties of applications may be their high computational cost. Bae *et al.* [18], [58] adopted *multi point approximation* (MPA) to alleviate these difficulties. In their work, compared with the sampling method and the vertex method, the proposed MPA method enhanced its accuracy through local approximation, focusing the computational recourses on the failure region. Then the *two-point adaptive non-linear approximate* (TANA2) method was selected, evaluating the belief and plausibility functions without sacrificing the accuracy. Basic belief assignment (BBA) expressed the degree of confidence in a proposition. The detailed flow diagram is shown in Figure 31.6.

Although such a cost-effective algorithm is demonstrated by two structural examples [18], it is not an issue as to which one takes design problem

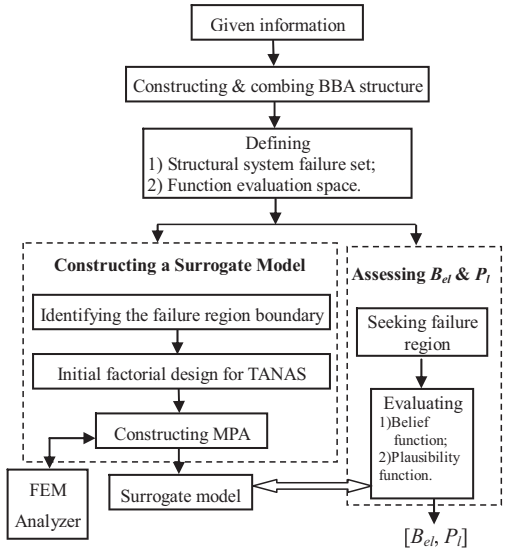


Figure 31.6. An uncertainty qualification approximation algorithm using evidence theory

into account. The study of design optimization that propagates epistemic uncertainty using evidence theory was first carried out by Agarwal *et al.* [6], who calculated optimum designs for multi-disciplinary systems. Since the belief functions are discontinuous to formulate non-deterministic constraints in this research, Agarwal *et al*., employed a trust region sequential approximate optimization method to drive the optimization process with surrogate models representing the uncertain measures as continuous functions. Their work is significant in throwing light on the use of evidence theory for optimization under uncertainty.

Mourelatos and Zhou [27] continued the research of EBDO and proposed an optimization method that can handle a mixture of aleatory and epistemic uncertainties efficiently in the formulation as follows,

$$\begin{aligned} &\min \ f\left(\mathbf{d}, \mathbf{X}^N, \mathbf{P}^N\right) \\ &\text{s.t.} \ P_f\left(G_i\left(\mathbf{d}(\mathbf{X})\right) > 0\right) \le p_{f_i},\ i = 1,2,\cdots,np \\ &\quad \mathbf{d}^L \le \mathbf{d} \le \mathbf{d}^U,\ \mathbf{X}_L^N \le \mathbf{X}^N \le \mathbf{X}_U^N \\ &\quad \mathbf{d} \in \mathbb{R}^n,\ \mathbf{X} \in \mathbb{R}^{nr},\ \mathbf{P} \in \mathbb{R}^q \end{aligned} \tag{31.2}$$

where **d**, **X** and **P** are the vectors of deterministic design variables, uncertain design variables and uncertain design parameters, respectively. Here *n*, *nr*, *q* are the numbers of the above variables or parameters, respectively, and *np* is the number of constraints. p_{f_i} is a prescribed probability value and the superscript "*N*" indicates the nominal value of each variable or parameter.

After a geometrical interpretation of the EBDO problems, a computationally efficient solution was presented to demonstrate the proposed EBDO method in [27]. The algorithm quickly identified the vicinity of the optimal point by a derivative-free optimizer calculating the evidence-based optimum, starting from the close-by RBDO optimum and moving a hyper-ellipse in the original design space. Moreover, only the identified active constraints were considered for local surrogate models. All these aspects keep the computational cost desirably low [27].

It is also shown that EBDO is conservative compared with all RBDO designs obtained with different probability distributions, but it is usually less conservative compared with the PBDO designs. It provides the possibility to investigate design optimization from a more broadened and general point of view, if the uncertainty representation tools can be further improved.

31.4.3 Integration of Various Approaches to Design Optimization

In recent years, more attention has been paid to the integrated framework of uncertainty analysis and optimization methods. The representative, but not exhausitive, work is illustrated below.

31.4.3.1 Integration of PBDO and RBDO

A design platform integrating both RBDO and PBDO when modeling physical uncertainty with insufficient information has been presented using PMA to improve numerical efficiency and stability in PBDO with MPS for highly non-linear and monotonic performance response in RBDO [56]. Such a structure is shown in Figure 31.7.

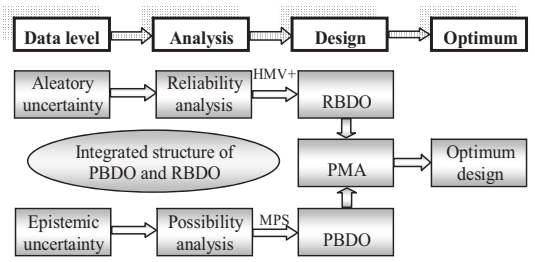


Figure 31.7. An integration of PBDO and RBDO by the PMA method [56]

Other integrating work has been done on the probabilistic and possibilistic methods. Although these two methods have tended to develop independently, with specialized algorithms for the implementation of each technique, it is possible to encompass them by a single mathematical algorithm according to the relation between them. Langley [59] realized the fact and then provided a unified approach to the assessment of structural integrity, for example, existing codes for FORM and SORM can potentially be employed for other methods in terms of a constrained minimization problem. Moreover, a second common algorithm

has been derived to assess the system reliability under a specified uncertainty or to derive the maximum tolerances for a reliability level.

31.4.3.2 Integrated Framework of Aleatory Uncertainty and Epistemic Uncertainty

In considering the integration of various design optimization methodologies under aleatory uncertainty or epistemic uncertainty, or both, a method called the *adaptive-loop* method has been explored [60]. It aims at improving numerical efficiency as well as maintaining numerical stability and accuracy.

The adaptive-loop method is composed of three phases of optimization. Deterministic design optimization is employed at the beginning of the process with the additional improvement of numerical efficiency by reducing the design iterations. Then the parallel-loop method is expedited addressing numerical convergence and statistical feasibility using PMA+. The last step uses the single-loop method, checking the design closeness and improving computational efficiency. Such an integrated framework is typical as an organic structure for uncertainty design optimization, as illustrated in Figure 31.8.

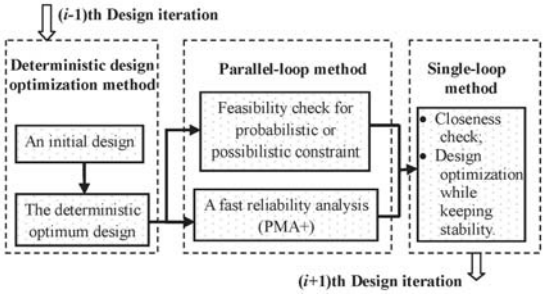


Figure 31.8. An adaptive-loop design optimization method [60]

31.4.3.3 Integration of Robust Design and PBDO

Considering the fact that, for epistemic uncertianties, PBDO deals with the failure rate, while a robust design optimization minimizes the product quality loss, researchers are interested in integration work for epistemic uncertainty. Since there is no metric for product loss defined under epistemic uncertianty, Youn and Choi [61] proposed a new framework integrating PBDO and a robust design optimization with a new metric of product quality loss by means of three different types of robust objectives for epistemic uncertainty. Such *possibility-based robust design optimization* (PBRDO) can be formulated as

$$\begin{aligned} &\min \quad Cost(\mathbf{d}, \mathbf{V}) \\ &\text{s.t.} \quad \Pi\left(G_i\left(\mathbf{d}(\mathbf{V})\right) > 0\right) \le \alpha_t,\ i = 1,2,\cdots,np \\ &\mathbf{d}^L \le \mathbf{d} \le \mathbf{d}^U,\ \mathbf{d} = m(\mathbf{V}) \in \mathbb{R}^{ndv}, \mathbf{V} = [V_i]^T \in \mathbb{R}^{nrv} \end{aligned} \tag{31.3}$$

where the design vector $\mathbf{d}$ is the maximum likely value of the fuzzy random vector and $\mathbf{V}$ is the fuzzy random vector. *np*, *ndv* and *nrv* are the number of possibilistic constraints, the number of design variables, and the number of fuzzy random variables, respectively.

Then MPS and PMA+ are employed to more effectively estimate possibilistic constraints and conducting the design optimization, respectively.

Actually, robust design can be integrated into any of uncertainty-based design optimization with the result of enhancing the product quality as well as the confidence level (*e.g.*, reliability). Du *et al.* [62] integrated robust design and RBDO in an inverse reliability strategy and gave a new search algorithm for the *most probable point of inverse reliability* (MPPIR), evaluating the performance robustness. Their engineering example of a vehicle combustion engine piston design illustrated the effectiveness of the method, solving the tradeoff problem encountered in the integration simultaneously, which has always been the difficulty in uncertainty handling.

31.4.4 Data Fusion Technology in Reliability Analysis

Along with optimization approaches, fusion technologies are necessary in reliability assessment and engineering design of complex large scale systems. As two of the most important fusion methods, the evidence method and the possibility method have been widely used recently. Data fusion is now a formal framework and tools for the

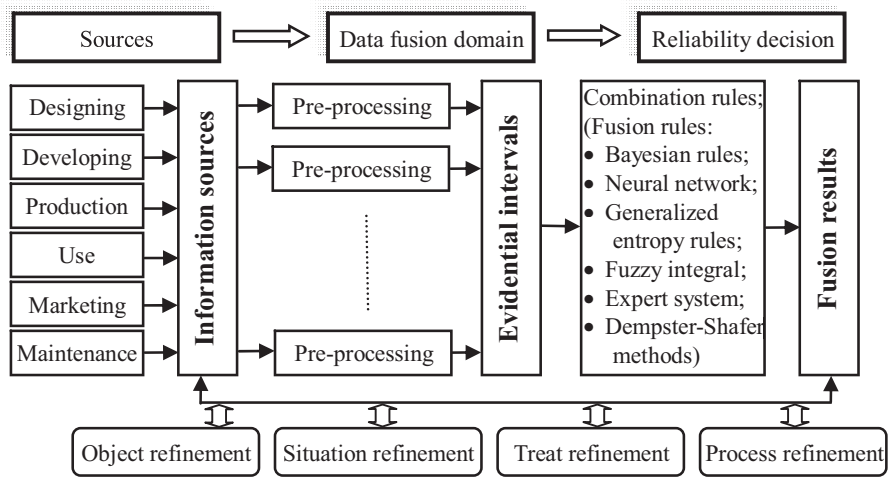


Figure 31.9. Dempster-Shafer methods as a part of reliability information fusion model

alliance of data originate from different sources of different nature. It aims at obtaining information of greater quality. If the information in the fusion process involves not only data, but also image, sensor and classifier, *etc*., the concept of data fusion can be extended, and the application area can also been extended. A fusion system is usually multi-leveled, e.g. from fixed level to feature level and then to decision level [63].

In the framework of possibility theory, the information available is represented by a possibility distribution corresponding to an interval (or a set). The fusion of uncertain information is equivalent to finding a compromise between a too accurate result which is certainly false and a sure result which is too imprecise.

Evidence theory allows the handling of non-exclusive and non-singleton events. Each measure attaches a probability to any element of the power set of the set of discernment [63]. The Dempster–Shafer rule is used to aggregate these input mass functions. Different modes of decision allow us to handle the compromise information. Based on this knowledge, with information theory, the D-S fusion method in reliability engineering can be illustrated as in Figure 31.9.

The essential strategy should be considered as combining fusion technology into a comprehensive approach. In the reliability assessment process, fusion technologies may be first applied to subsystems, then synthesizes all combine proper results together [64], as showed in Figure 31.10. More information about principles and applications can be found in reference [30],[31].

31.5 Performability Improvement on the Use of Possibility Theory and Evidence Theory

As far as we know, besides theoretical and computational developments by the means of possibilistic and evidential approaches, some physical problems have also been solved in the area of perfomability, which includes quality, reliability, maintenance and safety and risk. Physical problems such as failure mechanisms and detective methods are related to *system failure engineering*, which in some sense can be viewed as a part of operational research [66]. From this point of view, fuzzy (possibilistic) methodology and evidence theory have made their own contributions to various aspects of dependability and performability by adoptions of natural language expressions about reliability information [67].

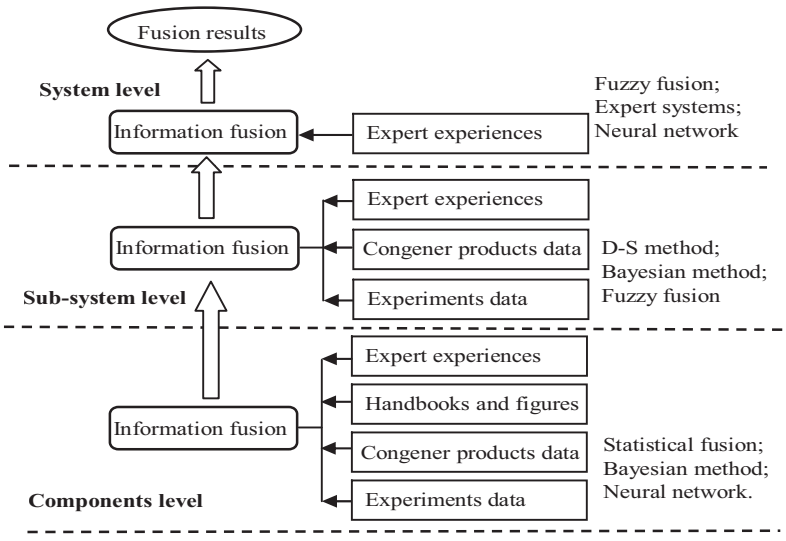


Figure 31.10. An information fusion structure for comprehensive reliability assessment [64]

31.5.1 Quality and Reliability

The characteristics of product quality consist of functionality, reliability and maintainability; reliability being the key point.

The first adoption of fuzzy methodology in reliability and failure analysis, *i.e*., the proposed notion of component possibility as a reliability index, may trace back to Kaufman's work [68], although the motivation and exact meaning of component possibility were not explained at that time. Currently more fuzzy-based approaches are appearing in reliability engineering [69] and Cai has summarized three main types of fuzzy methodology [66], respectively as,

- treating the probability as a fuzzy number;
- defining reliability in terms of a possibility measure; and
- considering failure as a fuzzy event.

31.5.1.1 Reliability Assessment and Evaluation

The reliability of a system is estimated in accordance with the probabilities of failures of its components. The information about reliability from an expert's elicitation may be imprecise and the uncertainty in parameters can be considered in a framework of *hierarchical uncertainty models*. Applications of the hierarchical models to reliability analysis using the possibility measure or imprecise probabilities have been considered by Utkin [47] as the extension of the Bayesian hierarchical model in the case of imprecise parameters of probability distributions, *e.g*., the component times to failure was characterized in a given confidence interval. Two methods (average parameters and average the system reliability) were analyzed with the result of simplicity from the computational viewpoint or minimal imprecision of results. However, further work is needed if there is no information regarding the independence of components.

Since one purpose of possibility is to represent and fuse uncertain data, and the existing fusion rules cannot deal rigorously with contradictory data, a new fusion rule merging different date sources was proposed by Delmotte and Borne [29], who used a vector expressing the reliability of the data sources and enabling a clear distinction between the data and their quality. Following the fusion rule, an algorithm assessing the indexes of reliability and moreover an index of the quality of the result

were provided. This was new in possibility theory and opened up its applications in the field of reliability.

Bai and Asgarpoor [43] presented an analytical method and Monte Carlo simulation method with fuzzy data to evaluate the substation reliability indices (such as the load point failure rate, the repair rate or repair time, and unavailability), which were represented by a possibility distribution. In the proposed models, the fuzzification rules were established by the extension principle and the techniques were tested to calculate the practical reliability indices for the substation configuration.

Besides fuzzy reliability theory in the context of possibility theory, the evidence-theory-based method is another approach to reliability analysis under incomplete information because of the simplicity of combination rules [18] and [24]. However, this approach also does not cover all possible judgments in reliability.

In attempting to implement the Dempster–Shafer and possibility theories into reliability and risk assessments, Kozine and Filimonov [20] summarized their experiences in the application of reliability areas. The criticism of the evidence theory is based on the following points:

- Failure to produce rational results in the case of inconsistent combined pieces of information according to Dempster's rule of combination.
- Inability to combine opinions of different people with overlapping experiences, especially in safety analysis applications.
- Being formally incoherent in safety assessment, just as in theory of probability.

They also encountered some difficulties that could not be solved in the frameworks of these theories [20]:

- Combination of homogeneous bodies of evidence.
- Combination of inconsistent pieces of information.
- Judgments admitted in elicitation.
- Dependence of imprecision on the amount of information, *etc*.

This indicates, in a final personal opinion, that Dempster's rule of combination can produce formally incoherent inferences.

31.5.1.2 Fault Tree Analysis (FTA)

The first implementation of fuzzy methods in the context of fault tree analysis was pioneered by Tanaka *et al.* [70], who treated imprecise probabilities of basic events as trapezoidal fuzzy numbers and employed the extension principle to describe the logical relationships leading to the top event. Furuta and Shiraishi [71] also proposed a type of importance measure but by means of max/min fuzzy operators and fuzzy integrals different than those in Tanaka's approach. With respect to to the fuzzy number, Singer [72] also regarded it as the perfectly straightforward way to overcome the deficiencies of inexact and inaccuracy knowledge. Soman and Misra [73] proposed a more general fuzzy method, also known as resolution identity to handle repeated events. Moreover, they extended this method to deal with multi-state FTA [74]. Another approach used to model imprecise relationships between physical and reliability states was proposed by Pan and Yun [75], who used fuzzy gates to describe output by triangular fuzzy numbers instead of crisp values 0 or 1. In fact, by defining fuzzy possibility of fuzzy event analogously to fuzzy probability, FTA can take into consideration subjective and expert opinions [45].

The literature on advances in FTA and fuzzy FTA is vast. Among others, we mention *fuzzy reliability theories* (see Section 31.3.1) and the *fuzzy logic* based method for linguistic (imprecise) quantification of fuzzy characteristics and construction of an approximate reasoning system.

Keller and Kara-Zaitri [76] observed the fact that interdependencies among various causes and effects may be assessed by rule-based reasoning and then introduced fuzzy logic to handle the impreciseness in fault representation.

Two possible strategies for integrating the possibilistic and the fuzzy logic-based approaches for FTA may be described as follows. One way is to construct an FTA model in the framework of possibility theory corresponding to different forms

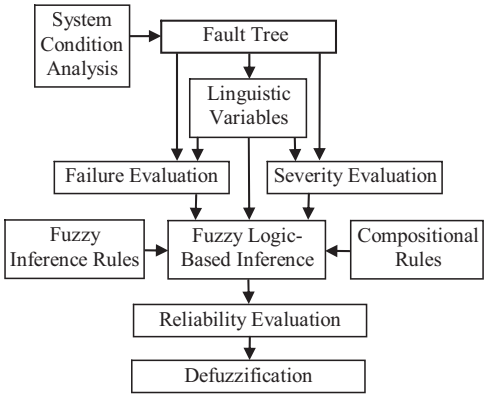


Figure 31.11. The procedure of an integrated approach of fuzzy FTA

of fuzzy reliability theory, using fuzzy logic as the fusion and reasoning strategy. The other one is to explore the FTA model in the context of fuzzy logic, applying possibility theory to meaning representation and inference. These two considerations may be integrated as in Figure 31.11.

31.5.1.3 Fault Diagnosis and Detection

Fault diagnosis partially interprets the reasons why a system fails. Some diagnosis methods are purely numerical in the sense that they exploit continuous models of the system based on automatic control methods, which are mainly regarded as fault detection. On the contrary, some diagnosis approaches focus on logical models of the system and perform consistency or inference analysis, mainly at the operational level. For example, a causal relational method for the application of a satellite fault diagnosis [77] is referred to as the latter type of method, in the framework of *fault mode effects and criticality analysis* (FMECA), where possibility calculus improved the discrimination power of the knowledge-based system, handling sequences of events consecutive to a fault.

Hence, the fuzzy approach together with the idea of fuzzy logic and the linguistic approach can be naturally used to deal with vagueness and ambiguity in system models and in human perceptions [66]. Furthermore, failure detection and identification problems can be addressed by fuzzy logic and D-S theory [67], or along with probabilistic approaches in multi-source data analysis, or the multiple-fault diagnosis problem.

Very recently, Fan and Zuo [30], [31] have proposed new decision rules based on the improved D-S evidence theory and employed the improved method in gearbox fault diagnosis, which enhance diagnostic accuracy and autonomy by means of combining expert knowledge and multi-source information.

Even now, application of D-S evidence theory in diagnosis has just begun. Issues deserving study involve how to transform expert diagnostic opinion into basic probability assignments and how to determine thresholds precisely.

31.5.2 Safety and Risk

With respect to a special kind of failure with catastrophic consequences, safety may be a part of reliability. Fuzzy methodology and fuzzy rules, together with many typical safety assessment approaches such as the *probabilistic risk assessment* (PRA) approach, have been applied in areas of safety design and risk analysis [78]–[80].

Cremona and Gao [81] developed an original possibilistic approach to evaluating the safety of structures, which was founded on the principles of possibility theory, with easy implementations compared to a probabilistic reliability approach. The development procedure contained the proof of existence of two reliability indicators (*failure possibility* and *the possibilistic reliability index*) and the application field, *i.e.*, linear and non-linear limit states involving non-interactive fuzzy intervals for welded joints damaged by fatigue. Such an example provided a full application, from uncertainty propagation (possibilistic variables transformation) and possibility distribution estimation to failure possibility determinations. Another approach to possibilistic assessment of the structures safety, where a realistic description of system behavior was obtained by applying high-quality algorithms in the structural analysis, can be found in [19].

In engineering safety analysis, in particular dealing with un-quantifiable information, several

researchers have investigated the relationships between fuzzy sets and D-S theory, and have suggested different integration approaches. Among others, we mention a belief *rule-based inference methodology using the evidential reasoning* (RIMER) approach established by Liu *et al.* [82] , for safety analysis and synthesis. The framework can be divided into two parts as follows. Safety estimation using the *fuzzy rule-based evidential reasoning* (FURBER) approach. In this part, information on various safety-related parameters can be described and transformed into an individual antecedent attribute in the rule base and in the inference process. The other is safety synthesis using the *evidential reasoning* (ER) approach to model hierarchical multi-expert analysis framework, with the final calculation of the risk level ranking index. The application of the proposed approach was illustrated by a case study of collision risk in [82].

If we must decide whether to operate or switch off a system based on available information that may be incomplete, evidence theory can be explored to meet such a demand. This is a kind of safety control problem and Dempster's rule of combination has been used for fusing a given set of information [66].

Risk concerns both failure consequences and failure occurrence uncertainty. Risk is also linked to decision-making policies. Subjects about risks are divided into two phases: risk assessments and risk management [83]. When risk management is performed in relation to PRA, the two activities are called *probabilistic risk assessment and management* (PRAM).

Quite a few research efforts have been made to establish a unified PRAM methodology where subjective assessment, value judgment, expertise and heuristics are dealt with more objectively. However, to express the uncertainty of the event occurrence in terms of a possibility measure, it is still an open and challenging problem as to how to define and assess the risk of an event.

When using possibility theory to estimate the risk of a certain act, risk is a combination of the likelihood of the occurrence and consequences of the action, which inhere in epistemic uncertainty. Two related techniques may include a numerical technique that applies classical possibility theory to crisp sets and, on the other hand, a linguistic technique that uses possibility theory on fuzzy sets. An adversary/defender model with *belief* and *plausibility* as the measure of uncertainty has been proposed as a linguistic model in an approximate reasoning rule base [84] .

31.5.3 Maintenance and Warranty

Product maintenance and warranty have received the attention of researchers from many different disciplines and are related to subareas including optimal system design, optimal reliability improvement, modeling imperfect repairs, and replacement.

A framework of possibilistic *assumption-based truth maintenance system* (ATMS), as an extension of the classical ATMS, was constructed by Bos-Plachez [85]. He combined model-based diagnosis theory and exploited possibilistic logic properties under the possibilistic principle for application in information engineering by means of the experimentation of an analog circuit diagnosis system. This approach is another solution based on approximate reasoning that can be exploited in order to detect more faults.

The contribution of the possibilistic ATMS to diagnosis problems involves the following aspects.

- Measuring non-detective faults by reducing the widths of intervals.
- Being a natural evolution towards the possibilistic ATMS by associating necessity measures in accord with certainty degrees of models and measurements.
- Remaining helpful in eliciting the values of certainty degrees from necessity measures.
- Updating the candidate set for generalization.

To the best of our knowledge, the three formal views of warranty are the exploitation theory, the signal theory, and the investment theory, respectively. On general grounds, there is a negative correlation between product quality and warranty costs. So warranty policies are structured according to the perspectives of manufacturer and buyer. Some exploration is exemplified as using

the fuzzy set approach to select maintenance strategies, working out maintenance and warranty policy with fuzzy lifetimes, or under fuzzy environment, and building up condition-based maintenance or reliability-centered maintenance with partial information. See [86] for more details.

One way to improve the reliability of a product is to eliminate infant mortality or the initial failure rate with a burn-in program. Another way is to upgrade the manufacturing process; and the third consideration may be outgoing inspection to eliminate non-conforming items [67]. In these studies, new technologies and design methods may be of benefit in providing measurable improvement in quality and investment.

31.6 Developing Trends of Possibility and Evidence-based Methods

Although significant progress has been made during the last two decades, the investigation and development of possibility theory and evidence theory is still an active domain of research. The probable and noticeable perspectives include:

1. Integrating or perfecting already-existing integration methods.
   - Integrating possibilistic and probabilistic methods that have been proven to be efficient and matured, *e.g.*, the D-S method with other related methods.
   - Reducing design iteration and shortening search intervals using combination algorithms or genetic algorithms.
   - Enhancing computational accuracy and stability and numerical efficiency.
2. Focusing on those methods that can ultimately be expressed in a common analytical framework.
   - Improving and solving the conflict problem of various uncertainties.
   - Propagating uncertainty in a global angle.
   - Constructing an error-compensation feedback loop as a software improvement or an adaptive loop as a correction mechanism.
3. Uncertainty quantification analysis and risk assessment of precise systems or difficult-to-measure systems.
4. Soft computing strategies as the cooperating framework with diverse methods.
   - Basic cooperation with fuzzy logic, probabilistic reasoning and neural networks.
   - More advanced cooperation with genetic algorithms, evidential reasoning, learning machines, and chaos theory.
5. Combining theoretical research and practical applications in real environments, from both the scientist's and the engineer's angle.

We strongly hope that reliability engineers will collaborate with statisticians in the development of models and methods to ensure applications in a field where uncertainty often plays a key role in decision making.

31.7 Conclusions

In this chapter, we have provided a detailed overview of possibility and evidence theories. Both are fundamental theories and are applicable to reliability, risk and uncertainty analysis in engineering design when there is not sufficient input data available due to specific uncertainty. From the comparison and relationship of the two measures, we conclude that possibility theory and evidence theory play a significant role in reliability analysis. Performability improvement considering various uncertainties, especially epistemic uncertainty from incomplete input data, are also important due to their given representations and theoretic fameworks. However, there is also room for further exploration of more general frameworks and performance characteristics needed for new modified design criteria. Our holistic view can provide a comprehensive understanding of existing approaches and for future work.

Acknowledgment

This research was partially supported by the National Natural Science Foundation of China under the contract number 50775026 and the Specialized Research Fund for the Doctoral Program of Higher Education of China under the contract number 20060614016.

References

[1] Klir GJ. Principles of uncertainty: What are they? Why do we need them? Fuzzy Sets and Systems 1995; 74(1): 15–31.

[2] Klir GJ, Folger TA. Fuzzy Sets, uncertainty and information. Prentice Hall, Englewood Cliffs, NJ, 1988.

[3] Kangas AS, Kangas J. Probability, possibility and evidence: Approaches to consider risk and uncertainty in forestry decision analysis. Forest Policy and Economics 2004; 6(2): 169–188.

[4] Oberkampf WL, DeLand SM, Rutherford B.M, *et al*., Estimation of total uncertainty in modeling and simulation. Sandia Report 2000-0824, Albuquerque, NM, 2000.

[5] Oberkampf WL, Helton JC, Joslyn CA, *et al*., Challenge problems: Uncertainty in system response given uncertain parameters. Reliability Engineering and System Safety 2004; 85(1–3): 11–19.

[6] Agarwal H, Renaud JE, Preston EL, *et al.,* Uncertainty quantification using evidence theory in multidisciplinary design optimization. Reliability Engineering and System Safety 2004; 85(1–3): 281–294.

[7] Sugeno M. Fuzzy measures and fuzzy intervals: A survey. In: Gupta MM, Saridis GN, Gaines BR, editors. Fuzzy automata and decision processes. North-Holland, Amsterdam, 1977.

[8] Nikolaidis E, Haftka RT. Theories of uncertainty for risk assessment when data is scarce. http://www.eng.utoledo.edu/-enikolai/

[9] Huang HZ. Fuzzy multi-objective optimization decision-making of reliability of series system. Microelectronics and Reliability 1997; 37(3): 447–449.

[10] Huang HZ. Reliability analysis method in the presence of fuzziness attached to operating time. Microelectronics and Reliability 1995; 35(12): 1483–1487.

[11] Huang HZ. Reliability evaluation of a hydraulic truck crane using field data with fuzziness. Microelectronics and Reliability 1996; 36(10): 1531–1536.

[12] Klir GJ. Fuzzy sets: An overview of fundamentals, applications and personal views. Beijing Normal University Press, 2000.

[13] Zadeh LA. Fuzzy sets as a basis for a theory of possibility. Fuzzy Sets and Systems 1978; 1: 3–28.

[14] Fioretti G. Evidence theory: A mathematical framework for unpredictable hypotheses. Metroecnomica 2004; 55(4): 345–366.

[15] Beynon M, Curry B, Morgan P. The Dempster–Shafer theory of evidence: an alternative approach to multicriteria decision modeling. Omega 2000; 28(1): 37–50.

[16] Shafer G. A mathematical theory of evidence. Princeton University Press, 1976.

[17] Dubois D, Prade H. Possibility theory and its applications: A retrospective and prospective view. The IEEE Int. Conf. on Fuzzy Systems; St.Louis, MO; May 25-28, 2003: 3–11.

[18] Bae H-R, Grandhi RV, Canfield RA. Epistemic uncertainty quantification techniques including evidence theory for large-scale structures. Computers and Structures 2004; 82(13–14): 1101–1112.

[19] Möller B, Beer M, Graf W, *et al*., Possibility theory based safety assessment. Computer-Aided Civil and Infrastructure Engineering 1999; 14(2): 81–91.

[20] Kozine IO, Filimonov YV. Imprecise reliabilities: experiences and advances. Reliability Engineering and System Safety 2000; 67(1): 75–83.

[21] Mourelatos Z, Zhou J. Reliability estimation and design with insufficient data based on possibility theory. 10th AIAA/ISSMO Multidisciplinary Analysis and Optimization International Conference 2004.

[22] Huang HZ, Zuo MJ, Sun ZQ. Bayesian reliability analysis for fuzzy lifetime data. Fuzzy Sets and Systems 2006; 157(12): 1674–1686.

[23] Huang HZ, Bo RF, Chen W. An integrated computational intelligence approach to product concept generation and evaluation. Mechanism and Machine Theory 2006; 41(5): 567–583.

[24] Bae H-R, Grandhia RV, Canfield RA. An approximation approach for uncertainty quantification using evidence theory. Reliability Engineering and System Safety 2004; 86(3): 215–225.

[25] Xu H, Smets Ph. Some strategies for explanations in evidential reasoning. IEEE Transactions on Systems, Man, and Cyberntics. (A) 1996; 26(5): 599–607.

[26] Borotschnig H, Paletta L, Prantl M, *et al*., A comparison of probabilistic, possibilistic and evidence theoretic fusion schemes for active object recognition. Computing 1999; 62(4): 293–319.

[27] Mourelatos ZP, Zhou J. A design optimization method using evidence theory. 31st Design Automation Conference. International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Long Beach, CA, USA; Sept.24-28, 2005.

[28] Limbourg P, Multi-objective optimization of problems with epistemic uncertainty. Coello Coello C.A. *et al*., Eds. EMO 2005, LNCS 3410, 2005; 413–427.

[29] Delmotte F, Borne P. Modeling of reliability with possibility theory. IEEE Transactions on Systems, Man, and Cybernetics 1998; 20(1): 78–88.

[30] Fan XF, Zuo MJ. Fault diagnosis of machines based on D-S evidence theory. Part 1: D-S evidence theory and its improvement. Pattern Recognition Letters 2006; 27(5): 366–376.

[31] Fan XF, Zuo MJ. Fault diagnosis of machines based on D-S evidence theory. Part 2: Application of the improved D-S evidence theory in gearbox fault diagnosis. Pattern Recognition Letters 2006; 27(5): 377–385.

[32] Cai KY. Wen CY, Zhang ML. Fuzzy variables as a basis for a theory of fuzzy reliability in the possibility context. Fuzzy Sets and Systems 1991; 42(2): 145–172.

[33] Cai KY, Wen CY, Zhang ML. Posbist reliability behavior of typical systems with two types of failure. Fuzzy Sets and Systems 1991; 43(1): 17–32.

[34] Cai KY, Wen CY, Zhang ML. Fuzzy states as a basis for a theory of fuzzy reliability. Microelectronics and Reliability 1993; 33(15): 2253–2263.

[35] Cappelle B, Kerre EE. On a possibilistic approach to reliability theory. Proceedings of the 2nd International Symposium on Uncertainty Analysis, Maryland MD; April 25-28, 1993: 415–418.

[36] Cappelle B, Kerre EE. A general possibilistic framework for reliability theory. IPMU 1994; 311–317.

[37] Cai KY, Wen CY, Zhang ML. Mixture models in profust reliability theory. Microelectronics and Reliability 1995; 35(6): 985–993.

[38] Cai KY, Wen CY, Zhang ML. Posbist reliability behavior of fault-tolerant systems. Micro-electronics and Reliability 1995; 35(1): 49–56.

[39] Nikolaidis E, Chen S, Cudney HH, *et al.*, Comparison of probabilistic and possibility theory-based methods for design against catastrophic failure under uncertainty. ASME, Journal of Mechanical Design 2004: 126(3): 386–394.

[40] Utkin LV, Gurov SV. A general formal approach for fuzzy reliability analysis in the possibility context. Fuzzy Sets and Systems 1996; 83(2): 203–213.

[41] Cappelle B, Kerre EE. An algorithm to compute possibilistic reliability. ISUMA-NAFIPS 1995; 350–354.

[42] Cappelle B, Kerre EE. Computer assisted reliability analysis: An application of possibilistic reliability theory to a subsystem of a nuclear power plant. Fuzzy Sets and Systems 1995; 74(1): 103–113.

[43] Bai XG. Asgarpoor S. Fuzzy-based approaches to substation reliability evaluation. Electric Power Systems Research 2004; 69(2–3): 197–204.

[44] Utkin LV. Fuzzy reliability of repairable systems in the possibility context. Microelectronics and Reliability 1994; 34(12): 1865–1876.

[45] Huang HZ, Tong X, Zuo MJ. Posbist fault tree analysis of coherent systems. Reliability Engineering and System Safety 2004; 84(2): 141–148.

[46] Dubois D, Prade H. An alternative approach to the handling of subnormal possibility distributions– A critical comment on a proposal by Yager. Fuzzy Sets and Systems 1987; 24(1): 123–126.

[47] Utkin LV, Coolen FPA. Imprecise reliability: An introductory overview. http://maths.dur.ac.uk/stats.

[48] Walley P. Statistical reasoning with imprecise probabilities. London: Chapman and Hall, 1991.

[49] Aughenbaugh JM, Paredis CJJ. The value of using imprecise probabilities in engineering design. Design Engineering Technical Conf. and Computers and Information in Engineering Conf., USA, DETC2005-85354, ASME 2005.

[50] Youn BD, Choi KK. Selecting probabilistic approaches for reliability-based design optimization. AIAA Journal 2004; 42(1): 124–131.

[51] Hall J, Lawry J. Imprecise probabilities of engineering system failure from random and fuzzy set reliability analysis. 2nd Int. Symposium on Imprecise Probabilities and Their Applications, Ithaca, NY; June 26–29, 2001: 195–204.

[52] Papalambros PY, Michelena NF. Trends and challenges in system design optimization. Proceedings of the International Workshop on Multidisciplinary Design Optimization, Pretoria, S. Africa; August 7–10, 2000: 1–15.

[53] Youn BD, Choi KK, Park YH. Hybrid analysis method for reliability-based design optimization. Journal of Mechanical Design 2003; 125(2): 221–232.

[54] Choi KK, Du L, Youn BD. A new fuzzy analysis method for possibility-based design optimization. 10th AIAA/ISSMO Symposium on Multidisciplinary Analysis and Optimization, AIAA-2004-4585, Albany, New York, 2004.

[55] Youn BD, Choi KK. Enriched performance measure approach for reliability-based design optimization. AIAA Journal 2005; 43(4): 874–884.

[56] Youn BD, Choi KK, Du L. Integration of reliability- and possibility-based design optimizations using performance measure approach. SAE World Congress, Detroit, MI; April 11-14, 2005, Keynote Paper.

[57] Tu J, Choi KK. A new study on reliability-based design optimization. Journal of Mechanical Design, Transactions of the ASME 1999; 121(4): 557–564.

[58] Bae H-R, Grandhi RV, Canfield RA. Uncertainty quantification of structural response using evidence theory. 43rd Structures, Structural Dynamics, and Materials Conference, AIAA 2002.

[59] Langley RS. Unified approach to probabilistic and possibilistic analysis of uncertain systems. Journal of Engineering Mechanics 2000; 126(11): 1163–1172.

[60] Youn BD. Integrated framework for design optimization under aleatory and/or epistemic uncertainties using adaptive-loop method. ASME 2005-85253. Design Engineering Technical and Computers and Information in Engineering Conference. Long Beach, CA 2005.

[61] Youn BD, Choi KK, Du L, *et al.,* Integration of possibility-based optimization to robust design for epistemic uncertainty. 6th World Congress of Structural and Multidisciplinary Optimization. Rio de Janeiro, Brazil, May 30– June 3, 2005.

[62] Du X, Sudjianto A, Chen W. An integrated framework for probabilistic optimization using inverse reliability strategy. Design Engineering Technical and Computers and Information in Engineering Conference, Chicago, Illinios, Sept. 2–6, 2003;1–10.

[63] Hall DL, Llinas J. An introduction to multisensor data fusion. Proceeding of the IEEE 1997; 85(1): 6–23.

[64] Zhuang ZW, Yu WX, Wang H, *et al.,* Information fusion and application in reliability assessment (in Chinese). Systems Engineering and Electronics 2000; 22(3): 75–80.

[65] Sentz K, Ferson S. Combination of Evidence in Dempster-Shafer Theory. SAND2002-0835 Report, Sandia National Laboratories 2002.

[66] Cai KY. System failure engineering and fuzzy methodology: An introductory overview. Fuzzy Sets and Systems 1996; 83(2): 113–133.

[67] Misra KB, editor. New trends in system reliability evaluation. Elsevier, New York, 1993.

[68] Kaufmann A. Advances in fuzzy sets: An overview. In: Wang Paul P, editor. Advances in fuzzy sets, possibility theory, and applications. Plenum Press, New York, 1983.

[69] Ghosh Chaudhury S, Misra KB. Evaluation of fuzzy reliability of a non-series parallel network, Microelectronics and Reliability1992; 32(1/2):1–4.

[70] Tanaka H, Fan LT, Lai FS, *et al*., Fault-tree analysis by fuzzy probability. IEEE Transactions on Reliability 1983; 32(5):453–457.

[71] Furuta H, Shiraishi N. Fuzzy importance in fault tree analysis. Fuzzy Sets and Systems 1984; 12(3): 205–214.

[72] Singer D. A fuzzy set approach to fault tree and reliability analysis. Fuzzy Sets and Systems 1990; 34(2): 145–155.

[73] Soman KP, Misra KB. Fuzzy fault tree analysis using resolution identity and extension principle, International Journal of Fuzzy Mathematics 1993; 1: 193–212.

[74] Misra KB, Soman KP. Multistate fault tree analysis using fuzzy probability vectors and resolution identity. In: Onisawa T, Kacprzyk J, editors. Reliability and safety analysis under fuzziness. Heidelberg: Physica-Verlag, 1995; 113–125.

[75] Pan HS, Yun WY. Fault tree analysis with fuzzy gates. Computers and Industrial Engineering 1997; 33(3–4): 569–572.

[76] Keller AZ, Kara-Zaitri C. Further applications of fuzzy logic to reliability assessment and safety analysis, Microelectronics and Reliability 1989; 29(3): 399–404.

[77] Cayrac D, Dubois D, Prade H. Handling uncertainty with possibility theory and fuzzy sets in a satellite fault diagnosis application. IEEE Transactions on Fuzzy Systems 1996; 4(3): 251–269.

[78] Misra KB, Weber GG. A new method for fuzzy fault tree analysis, Microelectronics and Reliability 1989; 29(2): 195–216.

[79] Huang HZ, Wang P, Zuo MJ, *et al*., A fuzzy set based solution method for multi-objective optimal design problem of mechanical and structural

systems using functional-link net. Neural Computing Applications 2006; 15(3–4): 239–244.
[80] Huang HZ, Gu YK, Du XP. An interactive fuzzy multi-objective optimization method for engineering design. Engineering Applications of Artificial Intelligence 2006; 19(5): 451–460.
[81] Cremona C, Gao Y. The possibilistic reliability theory: Theoretical aspects and applications. Structural Safety 1997; 19(2): 173–201.
[82] Liu J, Yang J.B, Wang J, *et al*., Engineering system safety analysis and synthesis using the fuzzy rule-based evidential reasoning approach. Quality and Reliability Engineering International 2005; 21:387–411.
[83] Misra KB, Weber GG. Use of fuzzy set theory for level-I studies in probabilistic risk assessment, Fuzzy Sets and Systems 1990; 37(2): 139–160.
[84] Darby JL. Evaluation of risk from acts of terrorism: the adversary/defender model using belief and fuzzy sets. SAND2006-5777, Sandia National Laboratories 2006.
[85] C Bos-Plachez. A possibilistic ATMS contribution to diagnose analog electronic circuits. International Journal of Intelligent Systems 1998; 12(11–12): 849–864.
[86] Murthy DNP, Djamaludin I. New product warranty: A literature review. International Journal of Production Economics 2002; 79(3): 231–260.

32

Optimal Reliability Design of a System

Bhupesh K. Lad[1], Makarand S. Kulkarni[1], Krishna B. Misra[2]

[1]Indian Institute of Technology, New Delhi, India
[2]RAMS Consultants, Jaipur, India

Abstract: Reliability is one of the most important attributes of performance in arriving at the optimal design of a system since it directly and significantly influences the system's performance and its life cycle costs. Poor reliability would greatly increase life-cycle costs of the system, and reliability based design must be carried out if the system is to achieve its desired performance. An optimal reliability design is one in which all possible means available to a designer have been explored to enhance the reliability of the system with minimum cost under the constraints imposed on the development of a system.

32.1 Introduction

Each system is unique, and its definition includes its intended functions, specification of its sub-systems, description of functional interrelationships between the constituent components and the environment in which these components are expected to operate. Once a hardware concept and technology of a system have been developed, a system designer is faced with the problem of designing a system that satisfies the performance requirements desired by the customer over the intended period of the system's use. These requirements generally take the form of some selected performance indices. There are a number of measures of system performance. Some of these measures that may be of interest are [64]:

1. Reliability,
2. Availability,
3. Mean time to failure (MTTF),
4. Mean Time to Repair (MTTR),
5. Operational readiness, *etc*.

An effective system design is one that satisfies these performances requirements depending upon the mission of the system.

Reliability is the probability of failure free operation and is generally chosen as the criteria of design of non-maintained systems, whereas availability is the probability that the system is working satisfactorily at any given point of time and is chosen as the design criterion for maintained systems. Alternatively, one may be interested in comparing the design alternatives based on the MTTF and MTTR. Whatever may be the index of performance assessment, one should be able to build a mathematical model for the system design problem that will fit into the present-day techniques of solution.

Modern systems are becoming more and more complex, sophisticated and automated, and a measure of effectiveness that cannot be sacrificed is their reliability. Reliability has become a mandatory requirement for customer satisfaction and is playing an increasing role in determining the

competitiveness of products. Because of these reasons, system reliability optimization is important in any system design. A survey of available literature indicates that a lot is written on system design that deals with the problem of reliability optimization (see references).

There are several alternatives available to a system designer to improve system reliability. The most known approaches are:

1. Reduction of the complexity of the system.
2. Use of highly reliable components through component improvement programs.
3. Use of structural redundancy.
4. Putting in practice a planned maintenance, repair schedule and replacement policy.
5. Decreasing the downtime by reducing delays in performing the repair. This can be achieved by optimal allocation of spares, choosing an optimal repair crew size, *etc*.

System complexity can be reduced by minimizing the number of components in a system and their interactions. However, a reduction in the system complexity may result in poor stability and transient response. It may also reduce the accuracy and eventually result in the degradation of product quality. The product improvement program requires the use of improved packaging, shielding techniques, derating, *etc.* Although these techniques result in a reduced failure rate of the component, they nevertheless require more time for design and special state-of-the-art production. Therefore, the cost of a part improvement program could be very high and may not always be an economical way of system performance improvement. Also, this way the system reliability can be improved to some degree, but the desired reliability enhancement may not be attained.

On the other hand, the employment of structural redundancy at the subsystem level, keeping system topology intact, can be a very effective means of improving system reliability to any desired level. Structural redundancy may involve the use of two or more identical components, so when one fails, the others are available and the system is able to perform the specified task in the presence of faulty components. Depending upon the type of subsystem, various forms of redundancy schemes *viz*., active, standby, partial, voting, *etc*., are available. The use of redundancy provides the quickest solution, if time is the main consideration, the easiest solution, if the component is already designed, the cheapest method, if the cost of redesigning a component is too high, and the only solution if the improvement of component reliability is not possible [64]. Thus, much of the effort in designing a system is applied to allocation of resources to incorporate structural redundancies at various subsystems which will eventually lead to a desired value of system reliability.

Maintenance, repairs and replacements, wherever possible, undoubtedly enhance system reliability [61] and can be employed in an optimal way. These facilities, when combined with structural redundancy, may provide any desired value of system reliability.

In addition to these methods, use of burn-in procedures to eliminate early failures in the field for components that have high infant mortality may also lead to an enhancement of system reliability [4].

Therefore, the basic problem in optimal reliability design of a system is to explore the extent of the use of the above mentioned means of improving the system reliability within the resources available to a designer. Such an analysis requires an appropriate formulation of the problem. The models used for such a formulation should be both practical and amenable to known mathematical techniques of solution.

Considerable amount of work has been done to systematize reliability design procedure. This chapter provides an overview of the development in the field of optimal reliability design of systems. Section 2 of this chapter provides a description of problem domain of reliability optimization. In Section 3 some of the formulations for reliability optimization are presented. Section 4 provides an overview of solution techniques. A brief review of current approaches for repairable system design is presented in Section 5 of this chapter. The last section concludes the chapter.

Notation:

R_s System reliability, $0 \le R_s \le 1$,
Q_s Unreliability of system,
R_j Component reliability of stage j, $0 \le R_s \le 1$,
Q_j Unreliability of subsystem,
$R_{j\min}$ Lower limit on R_s,
$R_{j\max}$ Upper limit on R_s,
R_0 Specified minimum R_s,
b_i Resources allocated to i^{th} type of constraint,
n Number of subsystems in the system,
m Number of resources,
$f(.)$ The system reliability function,
$g_i(.)$ The i^{th} constraint function,
x_j Number of components at subsystem j,
$x_{j\min}$ Lower limit on x_j,
$x_{j\max}$ Upper limit on x_j,
$E(X)$ Multi-state series-parallel system reliability index,
c_{jp} Cost of component of type p used in subsystem j,
x_{jp} Number of components of type p used in subsystem j,
$X = (x_{11,}x_{12,...}x_{21,}x_{22,...})$ System design vector,
k Number of components required for system surviving,
$x_{j.,v}$ Number of parallel components for $1 \le v \le V_j$,
V_j Number of versions available for component of type j $(1 \le j \le n)$,
T Operation period,
D Required demand level,
MP Maintenance policy,
$C_{j,v}$ Maintenance and acquisition cost of version v for component of type j,
$C(N)$ Average system cost per unit time with component vector N,
$C_d(N)$ Average downtime cost per unit time with component vector N,
$C_m(N)$ Average maintenance cost per unit time with component vector N,
c_d Cost of system downtime per unit time,
c_m Maintenance cost per unit time for each component in subsystem j,
$N = N_j$ Component vector for $j = 1,...n$,
$A(N), U(N)$ Availability, unavailability of system with component vector N, respectively,
$t_{\alpha,x}$ System percentile life,
C_s Total component cost of the system,
$c_j(x_j, R_j)$ Cost of x_j component having reliability R_j,
A_{ss} System inherent availability (steady-state), $0 \le A_{ss} \le 1$,
α_s Long-run cost rate of the system (cost of maintenance, cost of system unavailability),
t_M Recovery time,
μ_F Mean time to failure of component,
A_s System availability,
A_0 System availability Goal.

32.2 Problem Description

In the literature, reliability optimization problems are broadly put into three categories according to the types of their decision variables: reliability allocation, redundancy allocation, and reliability-redundancy allocation. If component reliabilities are the only variables, the problem is called reliability allocation; if the number of redundant units is the only variable, the problem becomes Redundancy Allocation Problem (RAP); if the decision variables of the problem include both the component reliabilities and redundancies; the problem is called a Reliability-Redundancy

Allocation Problem (RRAP). Misra and Ljubojevic [58] were the first to introduce this formulation in the literature. The type of reliability optimization problem determines the nature and value of decision variables such that the system objective function is optimized and all constraints are met. The criterion may be reliability, cost, weight or volume. One or more criteria may be considered in an objective function, while the others may be considered as constraints.

Reliability allocation is usually easier than redundancy allocation, but it is more expensive to improve the component reliability than to add redundant units. Redundancy allocation, on the other hand, results in increased design complexity and increased costs through additional components, weight, space, *etc*. It also increases the computational complexity of the problem, and is classified as NP-hard in the literature [14]. Classifications of published papers in the literature based on type of decision variables (component reliability, redundancy level or both) are provided in Table 32.1.

Table 32.1. Classification of published papers based on problem they addressed

Reliability allocation [2], [90], [104]
Redundancy Allocation [1],[5],[12],[15],[16],[18],[19],[33],[35],[36],[39], [40], [41], [47], [48], [52], [53], [55], [60], [61], [62], [65], [66], [67], [69], [72], [74], [75], [77], [79], [80], [81], [84], [90], [91], [96], [97], [106], [108], [110], [111], [112], [115]
Reliability and redundancy allocation [58], [13], [20], [23], [28], [31], [38], [50], [68], [79], [90], [99], [103], [105],[113],[114]

These three classifications have been researched for different system configurations like series, series-parallel, parallel-series, complex, bridge, *etc*. System configuration shows the functional relationship of components in a system. It plays a vital role in the reliability optimization problem. Series configuration or series-parallel configuration is comparatively easy to solve, but in many practical situations complex or mixed configurations have to be used. Reliability improvement is equally important for such systems. Kuo *et al.* [43], in their review classified the reliability optimization research on the basis of system configurations.

Researchers have considered issues like: types of redundancy, mixing of components, multi-state system, *etc*. Table 32.2 provides a list of references that have considered various issues in optimal reliability design problems.

Table 32.2. Classification by specific application.

Standby redundancy [28],[49],[57],[62],[87],[88], [107],[110],[111],[112]
Multi-state system [50], [76], [80], [81]
Where to allocate [10], [11], [85],[101],[102]
Mix of components [15], [16], [19], [34],[47],[68],[77],[106],[115]
Modular (multi-level) redundancy [9],[108],[109]

Misra [62] was also the first to introduce the formulation of mixed types of redundancies in the optimal reliability design of a system. Prior to [62], the formulations invariably considered only active redundancies in redundancy allocation design problems. This was made possible with the introduction of a zero-one type of formulation based on the Lawler and Bell algorithm [45], which was for the first time proposed by Misra [53] for reliability optimization problems and has been considered very useful for solving various design problems involving discrete variables. There are different ways to provide component

redundancy, *viz.,* active parallel redundancy, *k*-out-of-*n*:G type (also known as partial redundancy), voting redundancy and standby redundancy. In active parallel redundancy and *k*-out-of-*n*:G type of redundancy, all the m-redundant units are operating simultaneously but at least one or *k* must be good for the redundant subsystem to be good. Voting is similar to *k*-out-of-*n*:G redundancy. However, in standby redundancy, only one of the redundant elements operates at any given point of time, and whenever a redundant unit fails, another healthy redundant unit from standby mode takes over the operation from the failed one. The subsystem fails only when all redundant units have failed [62]. As mentioned earlier, there have been relatively very few studies that deal with the standby redundancy allocation problem.

Similarly, there has been more research on reliability optimization of systems that consist of units that can have only two states (namely, operate or fail) as compared to the multi-state system [81]. Unlike two-state systems, multi-state systems assume that a system and its components may take more than two possible states (from perfectly working to completely failed). A multi-state system reliability model provides more flexibility for modeling of system conditions than a two-state reliability model [97]. Among others, problem of where to allocate redundancy, problem of mix of component (that allows for selection of multiple component choice, with different attributes, for each subsystem) and modular or multi-level redundancy allocation are some of the important issues in reliability optimization problems.

Some studies have also considered the issue of multi-level redundancy. When redundancy is added to components, it is called single-level redundancy but if a module (group of subsystems) is chosen for redundancy, then it is called modular or multi-level redundancy. A well-known thumb-rule among design engineers is that redundancy at the component level is more effective than redundancy at the system level. However, Boland and EL Neweihi [9] have shown that it is not true in the case of redundancy in series systems with non-identical spare parts.

For a maintained (repairable) system design [61], reliability and maintainability designs are usually carried out right at the design stage, and failure and repair rates are allocated to each component of the system in order to maximize its availability and/or reliability. For such systems it becomes imperative to seek an optimal allocation for spare parts while maximizing availability/ reliability subject to some techno-economic constraints on cost, resources, *etc.*

32.3 Problem Formulation

Amongst the various design problems that have been considered in the literature, the following formulations are widely discussed.

32.3.1 Reliability Allocation Formulations

Formulation 1: From mathematical point of view, the reliability allocation problem is a nonlinear programming problem (NLP). It can be shown as follows:

Maximize

$$R_s = f(R_1, R_2, ..., R_n),$$

subject to

$$g_i(R_1, R_2, ..., R_n) \le b_i; \quad i = 1,2,...,m,$$

$$R_{j\min} \le R_j \le R_{j\max}; \quad j = 1,2,...,n.$$

For separable constraints,

$$g_i(R_1, R_2, ..., R_n) = \sum_{j=1}^{n} g_{ij}(R_j). \qquad (32.1)$$

For series configuration,

$$R_s = \prod_{j=1}^{m} R_j \ . \qquad (32.2)$$

For parallel configuration,

$$Q_s = \prod_{i=1}^{m} Q_j \ , \text{ and} \qquad (32.3)$$

$$R_s = 1 - Q_s = 1 - \prod_{j=1}^{n} Q_j = 1 - \prod_{j=1}^{n} (1 - R_j). \qquad (32.4)$$

Formulation 2: In the above formulations reliability of components takes any continuous value between zero and one. Suppose there are u_j discrete choices for component reliability at stage j for $j = 1,...,k(\leq n)$, and the choice for component reliability at stage $k+1,...,n$ is on a continuous scale. Let $R_j(1), R_j(2),..., R_j(u_j)$ denote the component reliability choices at stage j for $j = 1,...,k$. Then the problem of selecting optimal component reliabilities that maximize system reliability can be written as [43]:

Maximize

$$R_s = h[R_1(x_1),...R_k(x_k), R_{k+1},..., R_n],$$

subject to

$$g_i[R_1(x_1),..., R_k(x_k), R_{k+1},..., R_n] \leq b_i, \quad i = 1,2,...m,$$
$$x_j \in \{1,2,...,u_j\}, \quad j = 1,2,...,k,$$
$$R_{j\min} \leq R_j \leq R_{j\max}; \quad j = k+1, k+2,..., n. \qquad (32.5)$$

32.3.2 Redundancy Allocation Formulations

Formulation 3: It is generally formulated as pure integer nonlinear programming problem (INLP).

Maximize

$$R_s = f(x_1, x_2,..., x_n),$$

subject to

$$g_i(x_1, x_2,..., x_n) \leq b_i; \quad i = 1,2,...,m,$$
$$x_{j\min} \leq x_j \leq x_{j\max}; \quad j = 1,2,...,n,$$
$$x_j \text{ being an integer.}$$

For separable constraints,

$$g_i(x_1, x_2,..., x_n) = \sum_{j=1}^{n} g_{ij}(x_j). \qquad (32.6)$$

Formulation 4: Another type of formulation, where percentile life is optimized, was provided by Coit and Smith [18]. The problem is to maximize a lower percentile of the system time to failure distribution subject to resource constraints. The approach is particularly useful when no clear mission time is available. This formulation is given as follows:

Maximize

$$t_{\alpha,x}$$

subject to

$$g_i(t_{\alpha,x}; x) \leq b_i; \quad i = 1,2,...,m,$$
$$t_{\alpha,x} = \inf\{t \geq 0 : R_s \leq 1-\alpha\},$$
$$x_j \text{ being an integer.} \qquad (32.7)$$

Formulation 5: Redundancy allocation for cost minimization.

Minimize

$$C_s = \sum_{j=1}^{n} c_j(x_j),$$

subject to

$$g_i(x_1, x_2,..., x_n) \leq b_i; \quad i = 1,2,...,m,$$
$$x_{j\min} \leq x_j \leq x_{j\max}; \quad j = 1,2,...,n,$$
$$x_j \text{ being an integer.} \qquad (32.8)$$

Similarly the reliability allocation and reliability-redundancy allocation problem can also be formulated in the form of cost minimization problem.

32.3.3 Reliability and Redundancy Allocation Formulations

Formulation 6: This can be considered as mixed integer nonlinear programming problem (MINLP).

Maximize

$$R_s = f(x_1, x_2,..., x_n; R_1, R_2,..., R_n),$$

subject to

$$g_i(x_1, x_2,..., x_n; R_1, R_2,..., R_n) \leq b_i; \quad i = 1,2,...,m,$$
$$R_{j\min} \leq R_j \leq R_{j\max}; \quad j = 1,2,...,n,$$
$$x_{j\min} \leq x_j \leq x_{j\max}; \quad j = 1,2,...,n,$$
$$x_j \text{ being an integer.}$$

Here also for separable constraints,

$$g_i(x_1, x_2,..., x_n; R_1, R_2,..., R_n) = \sum_{j=1}^{n} g_{ij}(x_j, R_j), \qquad (32.9)$$

32.3.4 Multi-objective Optimization Formulations

Formulation 7: A multi-objective formulation for reliability-redundancy allocation problem can be shown as:

Maximize

$$[f_1(x_1,...,x_n;R_1,...,R_n), and - f_2(x_1,...,x_n;R_1,...,R_n)],$$

where f_2 represents a convex cost function, subject to,

$$g_i(x_1,x_2,...,x_n;R_1,R_2,...,R_n) \le b_i;\quad i=1,2,...,m,$$
$$R_{j\min} \le R_j \le R_{j\max};\quad j=1,2,...,n,$$
$$x_{j\min} \le x_j \le x_{j\max};\quad j=1,2,...,n,.$$

For separable constraints,

$$g_i(x_1,x_2,...,x_n;R_1,R_2,...,R_n) = \sum_{j=1}^{n} g_{ij}(x_j,R_j),. \tag{32.10}$$

Similarly the multi-objective formulation for redundancy allocation and reliability allocation can also be formulated.

32.3.5 Problem Formulations for Multi-state Systems

Formulation 8: The general problem formulation for minimizing the cost of a series-parallel system is shown below [81]. The objective function is the sum of the cost of the components chosen. The reliability constraint, or minimum acceptable reliability level, is E_o.

Minimize

$$\min \sum_{j=1}^{n}\sum_{p=1}^{s} c_{jp}x_{jp},$$

subject to

$$E(X) \ge E_0,$$
$$x_{jp}x_{jk} = 0,\ j, p \ne k. \tag{32.11}$$

32.3.6 Formulations for Repairable System

Formulation 9: In designing the systems for reliability and maintainability, one may be interested in determining the pair (MTBF, MTTR), for which availability reaches a maximum value subject to a cost constraint. This problem of failure and repair rates allocation can be formulated as [61]:

Maximize

$$A_{ss} = \prod_{j=1}^{n} (MTBF/MTBF + MTTR)_j,$$

subject to

$$\sum_{j=1}^{n} c_j(MTBF, MTTR) \le C_s,$$
$$(MTBF)_j \ge 0,\ (MTTR)_j \ge 0;\ \forall_j \quad \forall_j. \tag{32.12}$$

Alternatively a dual problem can also be formulated as follows.

Formulation 10: Yu *et al.* [107], have seen the reliability allocation problem of a cold-standby system from a maintenance point of view. They formulated the problem as:

$$\underset{t_M \ge 0, \mu_F > 0}{Minimize}$$
$$\alpha_S(t_M, \mu_F)$$

subject to

$$A_S(t_M, \mu_F) \ge A_0. \tag{32.13}$$

where the various symbols used above are defined as given in the notation.

Formulation 11: Nourelfath and Ait-Kadi [76] have extended the classical redundancy allocation problem to find, under reliability constraints, the minimal configuration and maintenance costs of a multi state series-parallel system with limited maintenance resources. They formulated the problem as:

Minimize

$$C_s = \sum_{j=1}^{n}\sum_{v=1}^{V_j} x_{j,v}C_{j,v},$$

subject to

$$R_s(x_1,x_2,...,x_n,D,T,MP) \ge R_0. \tag{32.14}$$

Formulation 12: For a *k*-out-of-*n* system Amari [4] modelled the problem of minimizing the average system cost per unit time. The average system cost is the sum of the average cost of downtime plus the average cost of maintenance.

$$C(N) = C_d(N) + C_m(N) \qquad (32.15)$$

The cost of down time can be calculated from percentage of downtime within a unit time duration and the loss (cost) per unit downtime. It should be noted that under steady-state conditions, the percentage of downtime is equivalent to the steady-state unavailability. Hence,

$$C(N) = c_d.U(N) = c_d.[1 - A(N)]. \qquad (32.16)$$

The cost of maintenance is proportional to the cost associated with repairs of individual components. The cost of repair of a failed component includes the miscellaneous fixed cost as well as the variable cost based on the repair time. The cost of maintenance per unit time for the whole system is:

$$C_m(N) = \sum_{j=1}^{n} N_j.c_m \ . \qquad (32.17)$$

Therefore, the average cost of the system is:

$$C(N) = \sum_{j=1}^{n} N_j.c_m + c_d.U(N) \ . \qquad (32.18)$$

The objective is to find the optimal N that minimizes $C(N)$. The problem can be further refined by considering the maximum acceptable unavailability (U_a) and the acceptable upper limit on total weight and volume. Therefore, the constraints are

volume constraint: $\sum_{j=1}^{n} v_j \le V;$

weight constraint: $\sum_{j=1}^{n} w_j \le W;$

unavailability constraint: $U(N) \le U_a$. (32.19)

32.4 Solution Techniques

From the previous sections it can be seen that reliability optimization is a nonlinear optimization problem. The solution methods for these problems can be categorized into the following classes:

1. Exact methods.
2. Approximate methods.
3. Heuristics.
4. Metaheuristics.
5. Hybrid heuristics.
6. Multi-objective optimization techniques.

Exact methods provide exact solutions to reliability optimization problems. Dynamic programming (DP) [7, 52], branch and bound [26, 51, 95], cutting plane techniques [27], implicit enumeration search technique [25] and partial enumeration search technique [45, 53] are typical approaches in this category. These methods of course provide high solution quality, but higher a computational time requirement limits their application to simple system configurations and systems with only a few constraints.

The variational method [71, 28, 55], least square formulation [56], geometric [23, 57], parametric programming [6], Lagrangian and the discrete maximum principle [22, 54] offer an approximate solution. In most of these methods, the basic assumption remains the same: the decision variables are treated as being continuous and the final integer solution is obtained by rounding off the real solution to the nearest integer. This approach produces near-optimal solutions, or solutions that are very close to the exact solution. This is generally true since reliability objective functions are well-behaved functions.

On the other hand, many heuristics have also been proposed in the literature to provide an approximate solution in relatively short computational time [37, 55, 91, 93]. A heuristic may be regarded as an intuitive procedure constructed to generate solutions in an optimization process. The theoretical basis for such a procedure in most cases is insufficient, and none of these heuristics establish the optimality of the final solution. These methods have been widely used to solve redundancy allocation problems in series systems, complex system configuration, standby redundancy, multi-state system, *etc*.

Recently, meta-heuristics have been successfully used to solve complex reliability

optimization problems. They can provide optimal or near optimal solution in reasonable time. These methods are based on artificial reasoning rather than classical mathematics-based optimization. GA (genetic algorithm) [16, 79, 108, 109], SA (simulated annealing) [38, 84], TS (tabu search) [34, 41], immune algorithm (IA) [13], and ant colony (AC) [46, 47] are some of the approaches in this category, which have been applied successfully to solve the reliability optimization problem. Meta-heuristic methods can overcome the local optimal solutions and, in most cases, they produce efficient results. However, they also cannot guarantee the global optimal solutions.

In the literature, hybrid heuristics [15, 50, 111, 112] have also been proposed to solve redundancy and reliability-redundancy allocation problems. Hybrid heuristics generally combine one or more metaheuristics or a metaheuristic with other heuristics.

In reliability optimization with a single objective function, either the system reliability is maximized subject to limits on resource constraints, or the consumption of one of the resources is minimized subject to the minimum requirement of system reliability along with other resource constraints. A design engineer is often required to consider, in addition to the maximization of system reliability, other objectives such as minimization of cost, volume, and weight. It might not be easy to define limits on each objective in order to deal with them in the form of constraints. In such situations, an engineer faces the problem of optimizing all objectives simultaneously. To deal with such situations, multi-objective optimization techniques [67, 87, 88, 100] have been applied for system reliability design.

Review on optimal system design problems has been available from time to time during the past three decades. Chronologically, the first review was published by Misra [63] in 1975. Subsequent reviews have been published by Misra [64], Tillman *et al.* [98], Kuo and Prasad [42], Kuo *et al.* [43], and more recently in 2007 by Kuo and Wan [44]. A brief survey of some of the optimization techniques is also presented in this chapter for the sake of completeness of information.

32.4.1 Exact Methods

Among these techniques, dynamic programming [7, 52] is perhaps the most well known and widely used. Dynamic Programming (DP) methodology provides an exact solution but its major disadvantage is the curse of dimensionality. The volume of computation necessary to reach an optimal solution increases exponentially with the number of decision variables [24]. Although this weakness can be compensated for by employing Lagrangian multipliers [7, 24], DP is still not applicable to non-separable objective or constraint functions as would arise in reliability optimization problems with complex structures [33]. Misra [52] and Misra and Carter [60] have described a summation form of functional equations with a view to overcome the computational hazards and memory requirements of dynamic programming formulation.

Yalaoui *et al.* [105], presented a new dynamic programming method for a reliability redundancy allocation problem for series-parallel systems, where components must be chosen among a finite set. This pseudopolynomial YCC algorithm is composed of two steps: the solution of the sub-problems, one for each of the stages of the system; and the global resolution using the results of the one-stage problems. They showed that the solutions converge quickly towards the optimum as a function of the required precision. In another study, Yalaoui *et al.* [104] have used dynamic programming to determine the reliability of the components in order to minimize the consumption of a system resource under a reliability constraint in a series-parallel system.

Ghare and Taylor [26] provided another approach to solve redundancy optimization, known as branch and bound in the literature. This technique basically involves methods for suitably partitioning the solution space into a number of subsets and determining a lower bound (for a minimization problem) of the objective function for each of these. The one with the smallest lower bound is partitioned further. The branching and bounding process continues until a feasible solution is found such that the corresponding value of the objective function does not exceed the lower

bound for any subset [65]. Most of the branch and bound algorithms are confined to linear constraints and linear/non-linear objective functions. In general, the effectiveness of a branch-and-bound procedure depends on the sharpness of the bound; the required memory increases exponentially with the size of the problem [43]. Sup and Kwon [95] have modelled redundancy allocation problem with multiple-choice constraints as a zero-one integer-programming problem. The problem is analyzed first to characterize some solution properties. An iterative Solution Space Reduction Procedure (SSRP) is then derived using those solution properties. Finally, the iterative SSRP is used to define an efficient branch-and-bound procedure algorithm. Misra and Sharma [51] have solved the reliability problem using zero-one programming and a non-binary tree search procedure. Ha and Kuo [33] proposed a branch-and-bound method to solve the INLP. The proposed method is based primarily on a search space elimination of disjoint sets in a solution space that does not require any relaxation of branched sub problems. The major merits of the proposed algorithm are its flexibility (*i.e*., it does not rely on any assumptions of linearity, separability, single constraint, or convexity) and its efficiency (in terms of computation time). Experiments were performed to demonstrate that the proposed algorithm is more efficient compared to other exact algorithms, in terms of computation time.

The implicit enumeration search technique and the partial enumeration search technique of Lawler and Bell [45], like the branch and bound techniques, involve the conversion of integer variable formulation into binary variables formulation. Both techniques yield an optimal solution in several stages of steps, excluding at each step a number of solutions that cannot possibly lead to a better value of the objective function than that obtained up to that stage. The former technique requires the assumption of separability of the objective function and constraints, whereas no such assumption is required in the latter. Lawler and Bell's technique [45] can handle non-linear constraints also, which is an added advantage over the former. Although these search techniques require an assumption of monotonicity of the objective function, it certainly is not suitable for problems in which the variables are bounded above by large integers.

The use of Lawler and Bell's [45] algorithm for reliability design was first introduced by Misra [53]. Subsequently, this algorithm came to be widely used for a variety of reliability design problems. It has been observed, however, that a major limitation of Lawler and Bell's algorithm is its computational difficulty caused by a substantial increase in the number of binary variables [62]. Misra in [62] proposed a modified L-B algorithm of Misra [53] for optimal design of a subsystem which may employ any general type of redundancy, *i.e*., standby, partial or active.

Inspired by the lexicographic search given by Lawler and Bell [45], Misra in 1991 suggested a simple and efficient algorithm for solving an integer programming problem, called MIP algorithm (Misra integer programming algorithm). It is based on a lexicographic search in an integer domain (and not in a zero-one variables domain like Lawler and Bell's algorithm). MIP requires only functional evaluations and carries out a limited search close to the boundary of resources. It can handle system-reliability design problems of any type (nonlinear functions and does not impose any convexity and concavity conditions) in which the decision variables are restricted to take integer values only. The method is applicable for both small and large problems and in [69], MIP search method was applied to integer programming problems which need not be of separable form and may have any arbitrary form of function.

Misra and Sharma [65] employed a new MIP search algorithm to attempt system reliability design problems, as it provides the advantage of exploring all the feasible design solutions near the boundary and eliminates many of the unwanted feasible points. MIP reduces the problem of extensive search effort usually involved with L-B algorithm. The MIP algorithm is conceptually simple and efficient for solving any design problem involving integer programming.

In the literature the MIP algorithm has also been used with other approaches. A bound dynamic programming partial enumeration search technique is proposed by Jianping [35], in which

the optimal solution is obtained in the bound region of the problem by using the general dynamic programming technique and the MIP bound search technique. The algorithm was later on modified by Jianping and Xishen [36] in his partial bound enumeration technique based on the bound dynamic programming and the MIP. With some examples, the author showed the efficiency and economy of the proposed algorithm in solving larger system reliability optimization problems. In 2000, Prasad and Kuo [80] proposed an implicit enumeration algorithm, which is basically similar to MIP lexicographic search, but differs in order of the search vector, to solve nonlinear integer programming redundancy allocation problems.

Another development in the field of reliability optimization took place when Misra and Ljubojevic [58] for the first time considered the fact that the globally optimum results will be achieved if the optimization of system reliability is done using both component reliability and redundancy level as decision variables in the problem. They formulated it as a mixed-integer programming problem and solved it by a simple technique. Later on, a search method to improve the solution time for the formulation of [58] was offered by Tillman *et al.* [99].

The well-known cutting plane techniques for solving linear integer programming problems are efficient tools for solving reliability optimization problems [27], but with these techniques also, the problem of dimensionality still remains difficult to tackle and the cost of achieving a solution is usually very high.

There are several other interesting methods for solving general integer programming problems. Rosenberg [86], Misra and Sharma [59], and Nakagama and Miyazaki [73] have proposed a surrogate constraints algorithm for the problem where system "costs" coefficients are integers and the formulation surrogates many constraints, thereby permitting a faster solution. The surrogate constraint method translates a multidimensional problem into a surrogate dual problem with a single dimension by using a vector of surrogate multipliers. This method then obtains an exact optimal solution to the original problem by solving this surrogate dual problem. Recently, Onishi *et al.* [77], presented an improved surrogate constraint method to solve redundancy allocation problem with a mix of components.

Apart from these, redundancy allocation problems in which the decision variables are the number of redundant units, the problem of where to allocate redundancies in a system in order to stochastically increase the system lifetime is also important in reliability theory [10]. This problem has been addressed by many researchers through stochastic ordering [10, 11, 85, 101, 102].

In general, all exact methods become computationally unwieldy, particularly in solving larger scale reliability optimization problems. It is because of this reason, the research on application of exact methods, for the complex problems like reliability-redundancy allocation problem and problems with issues like stand-by redundancy, multi-state system, component mixing and modular redundancy, *etc.*, is relatively meagre. Such problems are also classified in the literature as NP-hard problem [14]. Hence, one is quite often led to consider approximate methods, heuristics, metaheuristics, *etc.,* which can be considered economical to solve such problems.

32.4.2 Approximate Methods

Moscowitz and McLean [71] were perhaps the first to formulate mathematically the optimization of system reliability subject to a cost constraint. They derived the maximum reliability for a fixed system cost and therefore solved an unconstrained problem. Gordon [28] using a variational method also tried a problem of a single constraint employing standby redundancy. The method in [71] was extended by Misra [55] to include any number of linear constraints. This is an approximate method of solution and requires an estimate of system reliability. Misra [56] proposed a least square approach for system reliability optimization. This type of approach is found to be very simple and faster than other methods, although the solution is an approximate one.

Everett [22] attempted to solve redundancy optimization problems through the use of Lagrangian multipliers, but he considered only one constraint. Misra [54] described an approximate

method for any number of constraints yet keeping the computational effort to a minimum. Messinger and Shooman [49] have provided a good review of earlier methods and considered approximate methods of allocating spare units based on incremental reliability per pound and Lagrangian multiplier algorithm.

Federowicz and Mazumdar [23] solved the problem of optimal redundancy allocation using geometric programming formulation. It is again an approximate solution method. The numbers of redundancy are treated as continuous variables and rounded off to the nearest integer in the final solution. Geometric programming is fairly simple if one deals with a problem of single constraint, but not so attractive when a large number of constraints is involved. Misra and Sharma [57] provide a geometric programming formulation simpler than in [23] and also make possible the consideration of switching redundancy. Govil [29] also provides a geometric formulation for a series system reliability optimization problem.

32.4.3 Heuristics

The simplest method in the heuristic category was proposed by Sharma and Venkateswaran [91] and Misra [55] independently and simultaneously and so it is called the MSV (Misra, Sharma and Venkateswaran) method. It is applicable only for redundancy optimization in a series system. This method iteratively adds a component to the stage which has maximum stage unreliability. The procedure continues until either a constraint is satisfied as equality or a constraint is violated. It can be easily shown that this procedure can be used for any type of redundancy in a system.

Kalyan and Kumar [37] have proposed a heuristic based on the reliability importance of a component and showed that it provides a good and quick approximation of the implicit enumeration method. Reliability importance ($\delta h / \delta p_i$) of a component i is defined as the rate of change of the system reliability h due to a change in component reliability p_i. The heuristic allocates the redundancy with the objective of maximizing Δh.

In another study, Shi [94] proposed a heuristic based on minimal paths to yield the solution in relatively less computing time. As an improvement over previous methods, Kohda and Inoue [40] proposed a criterion of local optimality. They showed that their method generates solutions which are optimal in a 2-neighborhood, while the solutions obtained by the previous methods are optimal only in a 1-neighborhood. The Kohda and Inoue algorithm [40] performs a series of selection and exchange operations within the feasible region to obtain the improved feasible solution. While solving constrained redundancy optimization problems in complex systems, there is a risk of being trapped at a local optimum.

Kim and Yum [39] have proposed a heuristic that allows excursions over a bounded infeasible region to alleviate this risk. It is shown that in terms of solution quality, the performance of the proposed method is better than those of Shi [94] and Kohda and Inoue [40].

A heuristic algorithm for solving the optimal redundancy allocation problem for multi-state series-parallel system (MSSPS) with the objective of minimizing total system design cost has been proposed by Ramirez-Marquez and Coit [81]. The heuristic works in three steps. First, an initial feasible solution is constructed, followed by application of a methodology to improve this solution. Finally, from the best solution found, a specified number of new solutions that have both higher cost and reliability are investigated in branches to explore additional feasible regions in an attempt to lead to a better solution. These are now treated as initial solutions and the improvement methodology is reapplied.

The improvement and branching phases of this heuristic provides flexibility of choosing a number of different design alternatives, which although not optimal, are not dominated by other design solutions. Ha and Kuo [32] have presented a tree heuristic for solving the general redundancy allocation based on a divide-and-conquer algorithm which imitates the shape of a living tree. A main solution path is repeatedly divided into several sub-branches if some criterion is satisfied; otherwise, the main solution path expands without any sub-branches.

The branching criterion is the ratio of sensitivity factor gap to the maximum sensitivity factor at the current stage. The final solution is obtained by selecting the best local solution. The proposed tree heuristic outperforms some other heuristics in terms of solution quality and computation time. Xu *et al.* [103], developed a heuristic for the reliability-redundancy allocation problem, called the XKL (Xu, Kuo, Lin) method. The XKL iteratively improves the system reliability by updating redundancy allocation in the following two ways:

1. By adding redundancy to the component which has the largest value sensitivity factor;
2. By adding redundancy to the component which has the largest value of sensitivity factor and by reducing redundancy in the component which has the smallest sensitivity factor.

The solution is obtained by subsequently solving an NLP problem with the updated redundancy allocation. If there is no reliability improvement with all combination pairs of the components, the algorithm stops.

Another heuristic that uses sensitivity factors is the HKRRA (Ha Kuo Reliability-Redundancy Algorithm) heuristic. This heuristic, proposed by Ha and Kuo [31] is a multi-path iterative heuristic for reliability-redundancy allocation problems. To compute the sensitivity factors for all the variables simultaneously, a new scaling method is employed. The heuristic is compared with the XKL method through a series of experiments. The experimental results show that the HKRRA heuristic is superior to the XKL heuristic as well as other heuristics in terms of solution quality and computational time. Beraha and Misra [8] have presented a random search algorithm to solve reliability allocation problems. An initial point is chosen where all sub-stages have the same reliability and the search begins about this point. By successively improving the mean, the search ends when a desired standard deviation is obtained within the feasible region (satisfying all the constraint equations). For solving a redundancy allocation problem, Ramachandran and Sankaranarayanan [83] proposed a random search algorithm that looks at a random multisample of feasible solutions and takes the best one.

A heuristic approach based on the Hopefield model of neural networks has been used by Nourelfath and Nahas [75] to solve a redundancy allocation problem with multiple choice, budget and weight constraints incorporated. Allella *et al.* [2] have again used the well known Lagrange multipliers technique to solve the reliability allocation problem. Data uncertainty due to the scarce knowledge of component reliabilities is also taken into account by considering component reliabilities as random variables.

32.4.4 Metaheuristics

Metaheuristics such as genetic algorithms (GA), simulated annealing (SA), tabu search (TS), immune algorithms (IA), and the ant colony (AC) have been used by many researchers for reliability optimization problems. These are based on probabilistic and artificial reasoning. Genetic algorithms (GA), one of the metaheuristics techniques, seek to imitate the biological phenomenon of evolutionary production through a parent-children relationship and can be understood as the intelligent exploitation of random search. Coit and Smith [16] have solved a redundancy optimization problem by applying GA to a series-parallel system with mix of components in which each subsystem is a *k*-out-of-*n*:G system. Painton and Campbell [79] presented a GA approach to the reliability-redundancy allocation problem where the objective is to maximize the fifth percentile of the mean time-between-failures distribution. The approach is shown to be robust in spite of statistical noise and many local maxima in the space of solutions induced by statistical variations due to input failure-rate uncertainties.

Coit and Smith [18] used a GA based approach to solve the redundancy allocation problem for series-parallel systems, where the objective is to maximize a lower percentile of the system time to failure distribution. The problems for the multi-level redundancy allocation in series-parallel systems have also been solved using GA [108, 109].

Simulated annealing (SA) is an approach to seek the global optimal solution that attempts to avoid entrapment in poor local optima by allowing an occasional uphill move to inferior solutions. Ravi *et al.* [84], used this approach to solve the redundancy allocation problem subjected to multiple constraints. Recently, Kim *et al.* [38], applied it to seek the optimal solution for reliability-redundancy allocation problems with nonlinear resource constraints. Numerical experiments were conducted and compared with previous studies for the series system, series-parallel systems, and the complex systems. The results suggest that the best solution for the SA algorithm is better then most of the previous best solutions.

Hansen and Lih [34] and Kulturel-Konak *et al.* [41], have used the Tabu Search (TS) metaheuristic to solve the redundancy optimization problem. TS searches the solution in the direction of steepest ascent until a local optimum is found and then the algorithm takes a step in the direction of mildest descent, while forbidding the reverse move for a given number of iterations to avoid cycling. The procedure is then iterated until no improved solution is found in a given number of steps.

The redundancy allocation problems have also been solved by the ant system metaheuristic which is inspired by the behavior of real ants. A moving ant lays some pheromone on the ground, thus making a path by a pheromone trail. If an isolated ant moves randomly, it will detect a previously laid trail and decide where to go. The trail with more pheromone has a higher probability to be chosen by the following ants [46]. Liang and Smith [47] used this metaheuristic for solving the redundancy allocation problem with a mix of components for a series-parallel structure. A problem specific ant-system for a series-parallel redundancy allocation problem has been developed by Liang and Smith [46]. Unlike the original ant system, the author introduced an elitist strategy and mutation to the algorithm. The elitist strategy enhances the magnitude of trails of good selections of components. The mutated ants can help explore new search areas.

A penalty guided immune algorithm (IA) for solving various reliability redundancy allocation problems, which includes series system, series-parallel system, and complex (bridge) system, has been presented by Chen [13]. Unlike the traditional GA based approaches, IA based approach preserves diversity in the memory so that it is able to discover the optima over time. The author has showed that the proposed method achieves the global optimal solution or a near-global solution for each example problem tested.

Recently, Liang and Chen [48] used a Variable Neighborhood Search (VNS) type algorithm as a metaheuristic to solve the series-parallel redundancy allocation problem with a mix of components. This metaheuristic employs a set of neighborhood search methods to find the local optimum in each neighborhood iteratively and hopefully reaches the global optimum at the end. The author is reported to have tested 33 test problems ranging from less to severely constrained conditions and showed that the variable neighborhood search method provides a competitive solution quality in comparison with the best-known metaheuristics like ant colony optimization [47] , genetic algorithm [17], *etc*.

32.4.4 Hybrid Heuristics

In another development in the field of reliability optimization, different heuristics and/or metaheuristics have been combined to give hybrid heuristics. One such approach is the hybrid intelligent algorithm that combines GA and artificial neural networks for solving reliability optimization problems. Zhao and Song [111] and Zhao and Liu [112] have used this approach to solve the fuzzy chance-constrained programming model for standby redundancy. The algorithm uses fuzzy simulation to generate a training data set for a back-propagation neural network to approximate the uncertainty function and GA to optimize the system performance. In a study that utilizes stochastic simulation, neural networks and GA, a stochastic programming model for general redundancy-optimization problem for both parallel and standby redundancy has been proposed by Zhao and Liu [110]. The model is constructed to maximize the mean system-lifetime, α-system lifetime, or system reliability and solve through a

hybrid intelligent algorithm. Stochastic simulation, neural networks and GA are integrated to produce a hybrid intelligent algorithm for solving these models. Stochastic simulation is used to generate training data, and then a back-propagation algorithm is used to train a neural network to approximate the system performance. Finally, the trained neural network is embedded into a genetic algorithm to form a hybrid intelligent algorithm.

In a similar work, Coit and Smith [15] present a combined neural network and genetic algorithm (GA) approach for the redundancy allocation problem for series-parallel systems. You and Chen [106] used GA with greedy method for solving a series-parallel redundancy allocation problem with separable constraints.

For highly constrained problems, infeasible solutions may make a relatively big portion of the population of solutions, and in such cases feasible solutions may be difficult to find. Dynamic adaptive penalty functions have been used with genetic searches to solve such problems, and the effectiveness of the dynamic adaptive penalty approach is demonstrated on complex system structures with linear as well nonlinear constraints [1].

Meziane *et al.* [50], used a universal moment generating function and an ant colony algorithm for finding the optimal series-parallel multi-state power system configurations. The ant colony algorithm is combined with a degraded ceiling local search technique to give a hybrid algorithm to solve the redundancy allocation problem for series-parallel systems [72].

32.4.5 Multi-objective Optimization Techniques

Toshiyuki *et al.* [100], have considered a multi-objective reliability allocation problem for a series system with time dependant reliability allocation and preventive maintenance schedule. Sakawa [87, 88] formulated the multi-objective reliability optimization problem not only for parallel redundant systems, but also for standby redundant systems, which is solved by using the surrogate worth trade-off (SWT) and sequential proxy optimization Technique (SPOT). In one more article on the multi-objective optimization method, Sakawa [89] dealt with the problem of determining optimal levels of component reliabilities and redundancies in a large-scale system with respect to multiple objectives. The author considered following objectives:

1. Maximization of system reliability,
2. Minimization of cost, weight, and volume.

This approach derives Pareto optimal solutions by optimizing composite objective functions, which are obtained by combining these objective functions. The Lagrangian function for each composite problem is decomposed into parts and optimized by applying both the dual decomposition method and the surrogate worth trade-off method.

Misra and Sharma [67] have used the MIP algorithm and a multicriteria optimization method based on the min-max concept for obtaining Pareto optimal solutions of redundancy allocation problems in reliability systems. Another similar approach used to solve multi-objective reliability-redundancy allocation problems with mixed redundancies has been proposed by Misra and Sharma [68].

Dingra [20] and Rao and Dingra [82] used goal programming formulation and the goal attainment method to generate Pareto optimal solutions. A heuristic method based on steepest ascent is used to solve goal programming and the goal attainment model. A generalization of the problem in the presence of vague and imprecise information is also addressed using the techniques of fuzzy multiobjective optimization. The multiobjective ant colony system (ACS) meta-heuristic has been developed to provide solutions for the reliability optimization problem of series-parallel systems with multiple component choices [115]. Tian and Zuo [97] and Salazar *et al.* [90], have used a genetic algorithm to solve the nonlinear multi-objective reliability optimization problems.

32.5 Optimal Design for Repairable Systems

As already mentioned in [61], availability could be the better performance measure for repairable systems than reliability. Since in most of the

practical situations, the systems are repairable, the availability and/or reliability may be optimized for such systems to achieve their performance goal. Numbers of approaches have been proposed for the optimal design of a repairable system. Mohamed [70] presented a brief review of optimization models for systems that consist of repairable components. Besides [61], Sharma and Misra [92] have proposed a formulation for an optimization problem involving three sets of decision variables, *viz*. redundancy, spares and number of repair facilities, simultaneously. Here again, MIP was shown to be most effective method to solve the problem. In the following section a brief discussion of some of the current approaches for repairable systems is presented.

Gurov *et al.* [30] solved the reliability optimization problem for repairable systems using the dynamic programming method and found the allocation of redundant units and repairmen. The computational experiments showed that this approach is accurate in results.

Dinesh and Knezevic [21] presented three models for spares optimization. The objective is to maximize the availability (or minimize the space) subject to space constraint (or availability constraint). The main advantage of the models presented in this paper is that these models can be solved efficiently by using general purpose algorithms such as SOLVER of EXCEL. The paper in fact presents an efficient branch and bound procedure to solve the optimization problem.

For a repairable system, the cost associated with downtime can be lowered by reducing the unavailability of the system. System unavailability can be reduced by adding additional spares for each subsystem, but the cost of the system increases due to the added operational and maintenance costs. Thus, it is desirable to derive a cost-effective solution that strikes a balance between the system downtime costs and the maintenance costs of providing spares for the system. Amari *et al.* [3], have formulated the problem of finding the optimal number of spares in each subsystem that minimizes the overall cost associated with the system as shown in formulation 12, and the authors proposed a simple search algorithm to solve the problem. The main contribution of their work is in reducing the search space by providing the bounds for optimal spares for each subsystem.

Yu *et al.* [107], used probability analysis, and formulated the system design problem as minimizing the system cost rate subject to an availability constraint to find mean time to failure of the components and the policy time of good-as-new maintenances. Then, a resolution procedure is developed to solve this problem.

Nourelfath and Ait-Kadi [76] extended the classical redundancy allocation problem for a repairable system to find, under reliability constraints, the optimal configuration and maintenance costs of a series-parallel system for which the number of maintenance teams is less than the number of repairable components. The problem is presented in formulation 11 in this chapter, and the authors suggest a heuristic method based on a combination of the universal generating function method and the Markov model to solve this optimization problem.

Ouzineb *et al.* [78], proposed a Tabu Search (TS) metaheuristic approach to solve the redundancy allocation problem for multi-state series-parallel repairable systems. The proposed method determines the minimal cost system configuration under specified availability constraints.

32.6 Conclusion

Reliability Design of a system is one of the most studied topics in the literature. The present chapter presents the developments that have taken place in this field since 1960. During these past four decades, researchers have presented various reliability design problems depending on the kind of system structure, objective functions and constraints and have provided various problem formulations and solution techniques.

The kinds of the problems studied in the literature are mainly based on: type of decision variables (reliability allocation and/or redundancy allocation), kind of redundancy (active, stand-by, *etc*.), type of the system (binary or multi-state

system), levels of the redundancy (multi-level system) and choice of the components (multiple component choice). While the redundancy allocation problem is the most studied reliability optimization problem, the reliability-redundancy allocation problem is gaining greater attention from researchers. Standby redundancy, multi-state systems, and multi-level redundancy are some of the areas having practical applications and provide good scope for further research in this area. Further, the problems of repairable system design have also been studied in literature. Availability is generally used as a measure of performance of such systems. Spare parts allocation, failure and repair rate allocation problem are very common availability/ reliability optimization problems for such systems.

Optimal reliability design problems are usually formulated to maximize system reliability under resource constraints like cost, weight, volume, *etc*. Multi-objective programming approaches have been used where multiple criteria are considered simultaneously. Other performance measures like percentile life have been proposed as a measure of system performance in the absence of specified mission time. More investigation in this direction is needed, as this would provide a new dimension to system reliability design problems.

While exact solution techniques are available to solve reliability optimization problems, heuristic and metaheuristics techniques are gaining popularity due to the ease of computational effort. Especially, metaheuristics techniques like Genetic Algorithm (GA), Simulated Annealing (SA), Tabu Search (TS) and Ant Colony (AC) provide reasonably good quality solutions in comparatively less computational times. The effectiveness and efficiency offered by these methods provide good motivation for researchers. The future trend appears to be in the direction of application of hybrid optimization techniques that would combine either two metaheuristics or a heuristic with any of the metaheuristics for reliability optimization.

Further, the reliability design problem is generally seen as an independent exercise from quality, maintainability, safety and sustainability considerations. In case of repairable systems with a long life cycle, maintenance costs may be a critical component of its life cycle costs, so all the maintenance and maintainability issues like reliability, maintainability design, maintenance policies, *etc*., must be fully explored at the design stage only. Also, every stage of product life-cycle, be it extraction of material, manufacturing, use or disposal, energy and materials are required as inputs, and emissions (gaseous, solid effluents or residues) are always associated which influence the environmental health of our planet. Therefore, these environmental factors must also be considered while designing a system. Unless we consider all these factors in an integrated way, we cannot call the design of products, systems and services truly optimal from an engineering point of view.

Thus the system design process must be considered from a whole life-cycle point of view by extending the reliability design by integrating it with the other constituent criteria of performability to give a true optimal design process which may eventually be called design for performability.

References

[1] Agarwal M, Gupta R. Genetic search for redundancy optimization in complex systems. Journal of Quality in Maintenance Engineering 2006; 12(4):338–353.

[2] Allella F, Chiodo E, Lauria D. Optimal reliability allocation under uncertain conditions, with application to hybrid electric vehicle design. International Journal of Quality and Reliability Management 2005; 22(6):626–641.

[3] Amari SV, Pham H, Gidda K, Priya SK. A novel approach for spares optimization of complex repairable systems. Proceedings IEEE RAMS 2005: 355–360.

[4] Amari SV. Optimal system design. In: Pham H, editor. Springer Handbook of Statistics. Springer, Berlin, 2006 (pt. F/54); 1–26.

[5] Balagurusamy E, Misra KB. A stochastic approach to reliability design of redundant energy systems. IEEE-PES Summer Meeting, Portland; July 18-23, 1976.

[6] Banergee SK, Rajamani K. Optimization of system reliability using a parametric approach. IEEE Transactions on Reliability 1973; R-22:35–39.

[7] Bellman R, Dreyfus SE. Dynamic programming and reliability of multicomponent devices. Operations Research 1958; 6:200–206.
[8] Beraha D, Misra KB. Reliability optimization through random search algorithm. Microelectronics and Reliability 1974; 13:295–297.
[9] Boland PJ, EL-Neweihi E. Component redundancy vs. system redundancy in the hazard rate ordering. IEEE Transactions on Reliability 1995; 44(4):614–619.
[10] Bueno VC, Carmo IM. Active redundancy allocation for a *k*-out-of-*n*:F system of dependent components. European Journal of Operational Research 2007; 176:1041–1051.
[11] Bueno VC. Minimal standby redundancy allocation in a *k*-out-of-*n*:F system of dependent components. European Journal of Operational Research 2005; 165:786–793.
[12] Bulfin RL, Liu CY. Optimal allocation of redundant components for large systems. IEEE Transactions on Reliability 1985; 34(4):241–247.
[13] Chen T. IAs based approach for reliability redundancy allocation problems. Applied Mathematics and Computation 2006; 182:1556–1567.
[14] Chern M. On the computational complexity of reliability redundancy allocation in a series system. Operational Research Letters 1992; 11:309–315.
[15] Coit DW, Smith AE. Solving the redundancy allocation problem using combined neural network/genetic algorithm approach. Computers and Operations Research 1996; 23(6):515–526.
[16] Coit DW, Smith AE. Reliability optimization of series-parallel systems using a genetic algorithm. IEEE Transactions on Reliability 1996; 45: 254–260.
[17] Coit DW, Smith AE. Penalty guided genetic search for reliability design optimization. Computers and Industrial Engineering 1996; 30(4): 895–904.
[18] Coit DW, Smith AE. Redundancy allocation to maximize a lower percentile of the system time to failure distribution. IEEE Transactions on Reliability 1998; 47(1):79–87.
[19] Coit DW, Konak A. Multiple weighted objectives heuristic for the redundancy allocation problem. IEEE Transactions on Reliability 2006; 55(3):551–558.
[20] Dhingra AK. Optimal apportionment of reliability and redundancy in series systems under multiple objectives. IEEE Transactions on Reliability 1992; 41(4):576–582.
[21] Dinesh KU, Knezevic J. Spare optimization models for series and parallel structures. Journal of Quality in Maintenance Engineering 1997; 3(3):177–188.
[22] Everett H III. Generalized Lagrangian multiplier method of solving problems of optimal allocation of resources. Operations Research 1963; 11:399–417.
[23] Federowicz AJ, Mazumdar M. Use of geometric programming to maximize reliability achieved by redundancy. Operations Research 1968; 19: 948–954.
[24] Fyffee DE. Hines WW, Less NK. System reliability allocation and a computational algorithm. IEEE Transactions on Reliability1968; 17:64–69.
[25] Geoffrion AM. An improved implicit enumeration approach for integer programming. Operation research 1969; 17:437–454.
[26] Ghare PM, Taylor RE. Optimal redundancy for reliability in a series system. Oper. Res. 1969; 17(5):838–847.
[27] Gomory R. An algorithm for integer solutions to linear programs. Princeton: IBM Mathematical Research Report 1958.
[28] Gordon K. Optimum component redundancy for maximum system reliability. Operations Research. 1957; 5:229–243.
[29] Govil KK. Geometric programming method for optimal reliability allocation for a series system subject to cost constraints. Microelectronics & Reliability 1983; 23(5):783–784.
[30] Gurov SV, Utkin LV, Shubinsky IB. Optimal reliability allocation of redundant units and repair facilities by arbitrary failure and repair distributions. Microelectronics and Reliability 1995; 35(12):1451–1460.
[31] Ha C, Kuo W. Multi-path approach for reliability-redundancy allocation using a scaling method. Journal of Heuristics 2005; 11:201–217.
[32] Ha C, Kuo W. Multi path heuristic for redundancy allocation: the tree heuristic. IEEE Transactions on Reliability 2006; 55(1):37–43.
[33] Ha C, Kuo W. Reliability redundancy allocation: an improved realization for non-convex nonlinear programming problems. European Journal of Operational Research 2006; 171:24–38.
[34] Hansen P, Lih K. Heuristic reliability optimization by Tabu search. Annals of Operations Research 1996; 63:321–336.
[35] Jianping L. A bound dynamic programming for solving reliability redundancy optimization. Microelectronics and Reliability 1996; 36(10):1515–1520.
[36] Jianping L, Xishen J. A new partial bound enumeration technique for solving reliability

redundancy optimization. Microelectronics and Reliability 1997; 37(2):237–242.

[37] Kalyan R, Kumar S. A study of protean systems-redundancy optimization in consecutive-*k*-out-of *n*:f systems. Microelectronics and Reliability 1990; 30(4):635–638.

[38] Kim H, Bae C, Park D. Reliability-redundancy optimization using simulated annealing algorithms. Journal of Quality in Maintenance Engineering 2006; 12(4):354–363.

[39] Kim J, Yum B. A heuristic method for solving redundancy optimization problems in complex systems. IEEE Transactions on Reliability 1993; 42(4):572–578.

[40] Kohda T, Inoue K. A reliability optimization method for complex systems with the criterion of local optimality. IEEE Transactions on Reliability 1982; 31:109–111.

[41] Kulturel-Konak S, Smith AE, Coit DW. Efficiently solving the redundancy allocation problem using tabu search. IIE Transactions 2003; 35:515–526.

[42] Kuo W, Prasad VR. An annotated overview of system-reliability optimization. IEEE Transactions on Reliability 2000; 49(2):176–187.

[43] Kuo W, Prasad VR, Tillman FA, Hwang C. Optimal reliability design: fundamentals and applications. Cambridge University Press, 2001; 1–65.

[44] Kuo W, Wan R. Recent advances in optimal reliability allocation. IEEE Transactions on System, Man, and Cybernetics–Part A: System and Humans 2007; 37(2):143–156.

[45] Lawler EL, Bell MD. A method of solving discrete optimization problems. Operations Research. 1966; 14:1098–1112.

[46] Liang Y, Smith AE. An ant system approach to redundancy allocation. Proceedings of the Congress on Evolutionary Computation (CEC) 1999; 2:1478–1484.

[47] Liang Y, Smith E. An ant colony optimization algorithm for the redundancy allocation problem. IEEE Transactions on Reliability 2004; 53(3):417–423.

[48] Liang Y, Chen Y. Redundancy allocation of series-parallel systems using a variable neighborhood search algorithm. Reliability Engineering and System Safety 2007; 92:323–331.

[49] Messinger M, Shooman ML. Techniques for spare allocation: a tutorial review. IEEE Transactions on Reliability 1970; 19:156–166.

[50] Meziane R, Massim Y, Zeblah A, Ghoraf A, Rahil R. Reliability optimization using ant colony algorithm under performance and cost constraints. Electric Power System Research 2005; 76:1–8.

[51] Misra KB, Sharma J. Reliability optimization of a system by zero-one programming. Microelectronics and Reliability 1969; 12:229–233.

[52] Misra KB. Dynamic programming formulation of redundancy allocation problem. International Journal of Mathematical Education in Science Tech. (UK) 1971; 2(3):207–215.

[53] Misra KB. A method of solving redundancy optimization problems. IEEE Transactions on Reliability 1971; 20(3):117–120.

[54] Misra KB. Reliability optimization of a series-parallel system, part I: Lagrangian multiplier approach, part II: maximum principle approach. IEEE Transactions on Reliability 1972; 21:230–238.

[55] Misra KB. A simple approach for constrained redundancy optimization problems. IEEE Trans. on Reliability 1972; 21:30–34.

[56] Misra KB. Least square approach for system reliability optimization. International Journal of Control 1973; 17(1):199–207.

[57] Misra KB, Sharma J. A new geometric programming formulation for a reliability problem. International Journal of Control 1973; 18(3):497–503.

[58] Misra KB, Ljubojevic M. Optimal reliability design of a system: a new look. IEEE Transactions on Reliability 1973; R-22:255–258.

[59] Misra KB, Sharma J. Reliability optimization with integer constraints coefficients. Microelectronics and Reliability 1973;12: 431–433.

[60] Misra KB, Carter CE. Redundancy allocation in a system with many stages. Microelectronics and Reliability 1973; 12:223–228.

[61] Misra KB. Reliability design of a maintained system. Microelectronics and Reliability 1974; 13: 493–500.

[62] Misra KB. Optimal reliability design of a system containing mixed redundancies. IEEE Transactions on Power Apparatus Systems, PAS 1975; 94(3):983–993.

[63] Misra KB. On optimal reliability design: a review. IFAC, 6th World Conference, Boston, MA 1975; 4:1–10.

[64] Misra KB. On optimal reliability design: A review. System Science 1986; 12(4):5–30.

[65] Misra KB, Sharma U. An efficient algorithm to solve integer-programming problems arising in a system-reliability design. IEEE Transactions on Reliability 1991; 40(1):.81–91.

[66] Misra KB. Search procedure to solve integer programming problems arising in reliability design

of a system. International Journal of. Systems Science 1991; 22(11):2153–2169.

[67] Misra KB, Sharma U. An efficient approach for multi criteria redundancy optimization problems. Microelectronics and Reliability 1991; 40(1): 81–91.

[68] Misra KB, Sharma U. Multicriteria optimization for combined reliability and redundancy allocation in system employing mixed redundancies. Microelectronics and Reliability 1991; 31(2/3):323–335.

[69] Misra K, Misra V. Search Method for Solving General Integer Programming Problems. International Journal of Systems Science 1993; 24(12): 2321–2334.

[70] Mohamed A, Leemis LM, Ravindran A. Optimization techniques for system reliability: A review. Reliability. Engineering. and System Safety 1992; 35: 137–146.

[71] Moscowitz F, McLean JB. Some reliability aspects of system design. IRE Transactions on Reliability and Quality Control 1956; 8:7–35.

[72] Nahas N, Nourelfath M, Ait-Kadi D. Coupling ant colony and the degraded ceiling algorithm for the redundancy allocation problem of series parallel system. Reliability Engineering and System Safety 2007; 92:211–222.

[73] Nakagama Y, Miyazaki S. Surrogate constraints algorithm for reliability optimization problems with two constraints. IEEE Transactions on Reliability 1981; R-30(2):175–180.

[74] Nakashima K, Yamato Y. Optimal design of a series-parallel system with time-dependent reliability. IEEE Transactions on Reliability 1977; 26(3): 199–120.

[75] Nourelfath M, Nahas N. Artificial neural networks for reliability maximization under budget and weight constraints. Journal of Quality in Maintenance Engineering 2005; 11(2):139–151.

[76] Nourelfath M, Ait-Kadi D. Optimization of series-parallel multi–state systems under maintenance policies. Reliability Engineering and System Safety. Dec. 2007;92(12):1620-1626.

[77] Onishi J, Kimura S, James RJW, Nakagawa T. Solving the redundancy allocation problem with a mix of components using the improved surrogate constraint method. IEEE Transactions on Reliability, March 2007; 56(1): 94-101.

[78] Ouzineb M, Nourelfath M, Gendreau M. Availability optimization of series-parallel multi-state systems using a tabu search metaheuristic. International Conference on Service systems and Service Management. Troyes, France; Oct. 25-27, 2006:953–958.

[79] Painton L, Campbell J. Genetic algorithms in optimization of system reliability. IEEE Transactions on Reliability 1995; 44(2):172–178.

[80] Prasad VR, Kuo W. Reliability optimization of coherent systems. IEEE Transactions on Reliability 2000; 49(3):323–330.

[81] Ramirez-Marquez JE, Coit DW. A heuristic for solving the redundancy allocation problem for multi-state series-parallel systems. Reliability Engineering and System Safety 2004; 83:341–349.

[82] Rao SS, Dhingra AK. Reliability and redundancy apportionment using crisp and fuzzy multiobjective optimization approaches. Reliability Engineering and System Safety 1992; 37: 253–261.

[83] Ramachandran V, Sankaranarayanan V. Dynamic redundancy allocation using Monte-Carlo optimization. Microelectronics and Reliability 1990; 30(6):1131–1136.

[84] Ravi V, Muty B, Reddy P. Non equilibrium simulated-annealing algorithm applied reliability optimization of complex systems. IEEE Transactions on Reliability 1997; 46(2):233–239.

[85] Romera R, Valdes JE, Zequeira RI. Active redundancy allocation in systems. IEEE Transactions on Reliability 2004; 53(3):313–318.

[86] Rosenberg IG. Aggregation of equation in integer programming. Discrete Mathematics 1974; 10:325–341.

[87] Sakawa M. Multi-objective reliability and redundancy optimization of a series parallel system by the surrogate worth trade off method. Microelectronics and Reliability 1978; 17:465–467.

[88] Sakawa M. An interactive computer program for multi-objective decision making by the sequential proxy optimization technique. International Journal of Man-Machine Studies 1981; 14:193–213.

[89] Sakawa M. Optimal reliability-design of a series-parallel system by a large scale multiobjective optimization method. IEEE Transactions on Reliability 1981; 30:173–174.

[90] Salazar D, Rocco CM, Galvan BJ. Optimization of constrained multiple-objective reliability problems using evolutionary algorithms. Reliability Engineering and System Safety 2006;91:1057–1070,

[91] Sharma J, Venkateswaran KV. A direct method for maximizing the system reliability. IEEE Transactions on Reliability 1971; 20:256–259.

[92] Sharma U, Misra KB. Optimal availability design of a maintained system. Reliability Engineering and System Safety 1988; 20:147–159.

[93] Sharma U, Misra KB, Bhattacharya AK. Optimazation of CCNs: Exact and heuristic

approaches. Microelectronics and Reliability 1990; 30(1):43–50.
[94] Shi DH. A new heuristic algorithm for constrained redundancy optimization in complex systems. IEEE Transactions on Reliability 1978; 27: 621–623.
[95] Sup SC, Kwon CY. Branch-and-bound redundancy optimization for a series system with multiple-choice constraints. IEEE Transactions on Reliability 1999; 48(2):108–117.
[96] Taboada HA, Baheranwala F, Coit DW, Wattanapongsakorn N. Practical solution for multi-objective optimization: an application to system reliability design problems. Reliability Engineering and System Safety 2007; 92: 314–322.
[97] Tian Z, Zuo M.J. Redundancy allocation for multi-state systems using physical programming and genetic algorithms. Reliability Engineering and System Safety 2006; 91:1049–1056.
[98] Tillman FA, Hwang CL, Kuo W. Optimization of system reliability with redundancy–A review. IEEE Transactions on Reliability 1977; R-26(3):148–155.
[99] Tillman FA, Hwang CL, Kuo W. Determining component reliability and redundancy for optimal system reliability. IEEE Transactions on Reliability 1977; R-26:162–165.
[100] Toshiyuki I, Inoue K, Akashi H. Interactive optimization for system reliability under multiple objectives. IEEE Transactions on Reliability 1978; 27:264–267.
[101] Valdes JE, Zequeira RI. On the optimal allocation of an active redundancy in a two-component series system. Statistics and Probability Letters 2003; 63:325–332.
[102] Valdes JE, Zequeira RI. On the optimal allocation of two active redundancies in a two-component series system. Operations Research Letters 2006; 34:49–52.
[103] Xu Z, Kuo W, Lin H. Optimization limits in improving system reliability. IEEE Transactions on Reliability 1990; 39(1):51–60.
[104] Yalaoui A, Chatelet E, Chu C. Reliability allocation problem in a series-parallel system. Reliability Engineering and System Safety 2005; 90:55–61.
[105] Yalaoui A, Chatelet E, Chu C. A new dynamic programming method for reliability and redundancy allocation in a parallel-series system. IEEE Transactions on Reliability 2005; 54(2):254–261.
[106] You P, Chen T. An efficient heuristic for series parallel redundant reliability problems. Computers and Operations Research 2005; 32:2117–2127.
[107] Yu H, Yalaoui F, Chatelet E, Chu C. Optimal design of a maintainable cold-standby system. Reliability Engineering and System Safety 2007; 92: 85–91.
[108] Yun WY, Kim JW. Multi-level redundancy optimization in series systems. Computers and Industrial Engineering 2004; 46:337–346.
[109] Yun WY. Song YM, Kim H. Multiple multi-level redundancy allocation in series systems. Reliability Engineering and System Safety 2007; 92: 308–313.
[110] Zhao R, Liu B. Stochastic programming models for general redundancy-optimization problems. IEEE Transactions on Reliability 2003; 52(2):181–191.
[111] Zhao R, Song K. A hybrid intelligent algorithm for reliability optimization problems. IEEE International Conference on Fuzzy Systems 2003; 2:1476–1481.
[112] Zhao R, Liu B. Standby redundancy optimization problems with fuzzy lifetimes. Computers and Industrial Engineering 2005; 49:318–338.
[113] Nakagawa Y. Studies on optimal design of high reliable system: Single and multiple objective nonlinear integer programming. Ph.D. Thesis, Kyoto University, Japan, Dec. 1978.
[114] Nakashima Kyoichi. Studies on reliability analysis and design of complex systems. Ph.D. Thesis , Kyoto University, Japan, March 1980.
[115] Zhao J, Liu Z, Dao M. Reliability optimization using multiobjective ant colony system approaches. Reliability Engineering and System Safety 2007; 92:109–120.

33

MIP: A Versatile Tool for Reliability Design of a System

S.K. Chaturvedi[1] and K.B. Misra[2]

[1]Reliability Engineering Centre, IIT Kharagpur, Kharagpur (WB) India
[2] RAMS Consultants, Jaipur

Abstract: In many reliability design problems, the decision variables can only take integer values. There are many examples such as redundancy allocation, spare parts allocation, repairman allocation that necessitate integer programming formulations and solutions thereof. In other words, the integer programming plays an important role in system reliability optimization. In this chapter, a simple yet powerful algorithm is described, which provides an exact solution to any general class of integer programming formulations and thereby offers reliability designers an efficient tool for system design. The algorithm is presented with an illustration to make the readers understand various steps. Besides, the applications of the algorithm to various reliability design problems are also provided.

33.1 Introduction

Advances in technology have always led system engineers, manufacturers and designers to design and manufacture systems with ever increasing sophistication, complexity, and capacity. Unreliable performance of some of the constituent sub-systems in these systems may lead to disastrous consequences for the system and its environment and loss of lives including economic, legal and sociological implications. Therefore it necessarily requires designers to design systems with the highest possible reliability within the constraints of cost, time, space, volume, technological limits *etc*. As a result, reliability is one of the system attributes that cannot be compromised in system planning, design, development and operation. It is of paramount concern to practicing engineers, manufacturers, economists and administrators. However, it is an established fact that the occurrence of failure can not be completely eliminated even for well-designed, well-engineered, thoroughly tested and properly maintained equipment. As a consequence, a present day user is not prepared to compromise on reliability, yet would like to have its best value for resources consumed in designing a system. Reliability and maintainability design is one of the areas in reliability engineering which makes possible more effective use of resources and helps decrease the wastage of scarce finances, material, and manpower.

An optimal design is one in which all the possible means available to a designer have been explored to enhance the reliability of the system under certain objective(s), operational requirements and allocated resources. Some of the

means through which a designer might attempt to enhance system reliability are:

- Reducing the system complexity.
- Increasing the reliability of constituent components through some product improvement program.
- Use of structural redundancy.
- Putting in practice a planned maintenance and repair/replacement policy.

Although each of the aforementioned alternatives has its relative advantages and disadvantages, one may have to strike a balance between them to achieve a system's objectives.

The employment of structural redundancy at subsystem/component level, without disturbing the system topology, can provide a very effective means of improving system reliability to any desired level [1]. In fact, structural redundancy in combination with an appropriate maintenance strategy may lead to provide almost unity reliability. The structural redundancy involves the use of two or more identical components, to ensure that if one fails, the system operation does not get affected and continues to carry on the specified task even in presence of a faulty component. Depending on the type of system, various forms of redundancy schemes, *viz.,* active, standby, partial, voting, *etc*., are available, and this may provide the quickest, easiest, cheapest and sometimes the only solution. However, the only factors, which may influence such a decision, could be the time constraints, existence of an already designed component, a costly and prohibitive redesign, and of course the technological limits.

There are several kinds of reliability design problems a designer may face. For example, it may include reliability allocation, repairman allocation, failure/repair rate allocation, spare parts allocation problem, *etc.*, or a combination of these problems. Depending on the situation, appropriate techniques can be adopted.

The present chapter describes an exact and efficient search technique, known as *Misra Integer Programming* (MIP) in the literature to address many system design problems. Although the algorithm was originally conceived to deal with the redundancy allocation problem, it can solve not only several other problems in system reliability design but many other general integer programming problems with equal ease [12].

Before providing the details of the search algorithm and its applications, the next section presents a brief overview of the redundancy allocation problem and the necessity and importance of developing a useful yet very simple algorithm to solve many design problems.

33.2 Redundancy Allocation Problem

33.2.1 An Overview

The problem of redundancy allocation is concerned with the determination of the number of redundant units to be allocated to each subsystem to achieve an optimized objective function (usually the reliability or some other related attribute of the system, *e.g.*, average life, MTTF), subject to one or more constraints reflecting the availability of various resources. Mathematically, the problem can be stated as:

$$Max.\ R_s = f[R_1(x_1), R_2(x_2)...R_n(x_n)], \quad (33.1)$$

$$Sub.\ \text{to}\ g_i(x) = g(x_1, x_2...x_n) \le b_i, i = 1, 2...m, \quad (33.2)$$

where reliability R_s (of n sub-systems with x_j redundant units at the j^{th} subsystem, each with a component reliability of r_j) will be a function of its subcomponents' reliabilities, $R_j(x_j)$. The functional form of $f(\cdot)$ depends on the system configuration and the type of redundancy being used. The form of m number of constraints, $g_i(x)$ (linear/nonlinear, separable/non-separable) can usually be determined from physical system considerations. However, if the constraints are separable functions, we can write (33.2) as:

$$g_i(x) = \sum_{j=n}^{n} g_{ij}(x_j) \le b_i, i = 1, 2...m. \quad (33.3)$$

The decision variables x_j, in the above formulations can take only non-negative integer values; therefore, the problem belongs to the class of non-linear integer programming problems, and

expression R_s, in general, may not be separable in x_j. Also, the nonlinear constraints may not necessarily be separable. However, an active-parallel redundant system in a series model consisting of n subsystems with linear constraints can be written in a closed form [10, 13].

In general, a redundancy allocation problem involving integer programming formulation can be stated as:

$$Optimize\ f(x), \tag{33.4}$$

$$Sub.\ to\ \ g_i(x) \le b_i; i = 1,2...m. \tag{33.5}$$

The function *f(x)* in (33.4) can be minimized or maximized and could be set to $f(x^*) = \pm\infty$, in general, ("+" for minimization and "–" for maximization) to start the search process. The variable $x = (x_1, x_2, ...x_n)$ is a vector of decision variables in E^n (the n-dimensional Euclidian plane), which is allowed to take positive integer values belonging to the feasible region $\mathcal{R}$ only and bounded by (33.5). Further, some x_i can also assume a value equal to zero. However, most often all x_i, being non-negative integers, are defined between the limits: $x_j^l \le x_j \le x_j^u$. In a redundancy optimization problem, x_i would have positive integer values between $1 \le x_j \le x_j^u$.

The value of x_k^u for the kth subsystem can easily be determined through the consideration of the ith constraint and accepting a minimum of the upper limits computed over all i=1,2...m, while maintaining $x_j^l = 1, \forall j = 1,2...n, j \ne k$ for other subsystems, *i.e.,*

$$x_k^u = \min_i \{x_j^{\max}\}, \forall k = 1,2...n, i = 1,2...m, k \ne j. \tag{33.6}$$

Therefore, the search to optimize, $f(x^*)$ could begin at one of the corners of feasible region, *i.e.*, $\left(x_1^u, x_2^l ... x_n^l\right)$ of $\mathcal{R}$ and finish at another point $\left(x_1^l, x_2^l ... x_n^u\right)$. Both of these points are certainly in the feasible region.

Therefore, the MIP basically relies on a systematic search near the boundary of constraints and involves functional evaluations on feasible points satisfying a specified criterion that a feasible point x would lie within the constraints and the current test point is close to the boundary from within the feasible region. However, the stopping criteria can be chosen depending upon the problem and objective of analysis. One of the ways of choosing the stopping criterion could be a test for maximum permissible slacks defined as:

$$mps_i = \min_j \{c_{ij}\} - \varepsilon.$$

To initiate the search, we frequently require the computation of $x_1^{\max}$, and in case of linear constraints $x_1^{\max}$ could be computed as:

$$x_1^{\max} = \min \left\{ x_1 : x_1 = \frac{b_i - \sum_j g_i(x_j; j = 2,3...n)}{\cos t\ coefficients\ of\ i^{th}\ type\ constra\text{int}s\ corrresponding\ to\ x_1} \right\}, \tag{33.7}$$

where $g_i(\cdot)$ and b_i are the constraint functions of variables and resources available for an ith type of constraint, respectively.

In case of non-linear constraints, $x_1^{\max}$ can be obtained by incrementing x_1, successively, by one unit at a time until at least one of the constraints gets violated, while keeping x_j at a minimum level at all other stages. It would be computationally advantageous if we compute and store the nonlinear incremental costs for the whole range of x_1 in memory rather than evaluate it every time $x_1^{\max}$ is desired.

33.2.2 Redundancy Allocation Techniques: A Comparative Study

Among the well known methods to provide an exact solution are: (i) Dynamic Programming approach, and (ii) Search Technique, *e.g.,* Cutting plane, Branch and Bound, Implicit search, and

partial enumerations using functional evaluations and certain rules for detecting an optimal solution from as few feasible solutions as possible.

Besides the exact techniques, several approximate and earlier methods such as Lagrange Multiplier [1, 8], Geometrical programming and the maximum principle approach [8], Differential dynamic programming sequential simplex search, penalty function approaches, *etc*., have also been employed by treating the integer decision variables as real variables and the final solution is obtained by rounding off the optimal variables to the nearest integers. In view of the fact that a decision problem involving integer variables is NP-complete, a number of heuristic procedures for solving design problems have also been proposed. Some evolutionary techniques inspired by some natural phenomenon such as biological (GA) or functioning of brain (ANN) have also been applied to deal with reliability design problems. Such techniques are known as meta-heuristic algorithms in the literature. The interested reader may refer to [6] for a comprehensive survey and a good account of various reliability design problems, their types and classifications, solution approaches along with the applications of some meta-heuristic techniques (such as GA and ANN).

Summarily, most of the exact integer programming techniques mentioned above, except those which are strictly based on some heuristic criteria, are computationally tedious, time-consuming and sometimes unwieldy, and have limitations of one kind or the other. The other simple techniques are mostly heuristic and thus approximate.

However, the approach described later in this chapter can solve a variety of general integer programming problems also, is simple to comprehend, is amenable to computerization, and easy to formulate. The advantages of the approach over the existing techniques are briefly given as under:

1. It does not require the conversion of variables into binary variables as in [5, 7].
2. It is applicable to a very wide variety of problems, with arbitrary nature of objective and constraint functions and without any assumption on the separability of objective functions. However, the functions involved must be non-decreasing functions of decisions variables.
3. It can solve both integer programming as well as zero-one programming problems with ease and effectiveness.
4. As stated earlier, the present approach to solve redundancy allocation problem is a systematic search near the boundary of feasible reason, so it drastically reduces the number of search points.

33.3 Algorithmic Steps to Solve Redundancy Allocation Problem

The entire algorithm can be summarized in following eight steps [9]:

1. Compute the upper and lower bounds of the decision variables to determine the entire feasible region. Lower bounds are generally known from the system description whereas upper bounds are determined from constraints (see (33.6)). Set $t = 2$ and $\nu = 0$, $x \equiv \left(x_1^u, x_2^l \ldots x_n^l\right)$ and $x^* = x$. If this point is within the slack band $\langle b_i - mps_i, b_i \rangle, \forall i = 1, 2 \ldots m$, go to step 8.
2. Set $x_2 = x_2 + 1$. If $x_2 \le x_2^u$, go to next step. Otherwise go to step 4.
3. Keeping all other variables, x_j, $j = 2, 3 \ldots n$ at the current level, determine the value of $x_1^{\max}$ which does not violate any of the constraints (refer to (1.8) and subsequent paragraph). If $x_1^{\max} = 0$, go to next step. Otherwise go to step 7.
4. $\nu = \nu + 1$. if $\nu > (n\text{-}2)$, STOP and print the optimal result. Otherwise proceed to step 5.
5. Set $k = t + \nu$ and $x_k = x_k + 1$. If $x_k > x_k^u$, return to step 4. Otherwise proceed to step 6.

6. Set $x_j = x_j^l$ for $j = 2,3...k-1$. Also, set v=0. Return to step 3.
7. Calculate slacks for constraints, $s_i, \forall i = 1,2...m$. If the current point lies within the allowable slacks for all *i*, go to next step. Otherwise return to step 2.
8. Evaluate the objective function *f(x)* at the current point *x*. If it is better than $f(x^*)$, then replace $x^* = x$ and $f(x^*) = f(x)$. Return and continue from step 2.

The algorithmic steps are simple and self explanatory. However, for the reader's benefit some of the steps of algorithm are explained in the following illustration.

Illustration:
Consider a SP system with four subsystems, two linear constraints and with subsystem reliabilities as, $r = [0.85\ 0.80\ 0.70\ 0.75]$, respectively.
Mathematically, we can formulate it as:

$$\textit{Maximize} \qquad R_s = \prod_{j=1}^{4} (1-(1-r_j)^{x_j}),$$

Sub. to

$$6.2x_1 + 3.8x_2 + 6.5x_3 + 5.3x_4 \le 51.8$$
$$9.5x_1 + 5.5x_2 + 3.8x_3 + 4x_4 \le 67.8.$$

Let us determine the upper and lower bounds (step 1) of the variables involved using (33.6) and the search area bounded by its constraints.

By keeping $x_k = 1, \forall j = 1,2,3,4, k \ne j$, the upper bound of a variable, say x_1, can be determined from constraints as:

$$6.2x_1 + 3.8 + 6.5 + 5.3 \le 51.8 \Rightarrow x_1 \le 5.8387$$
$$9.5x_1 + 5.5 + 3.8 + 4 \le 67.8 \Rightarrow x_1 \le 5.7368,$$

i.e., $x_1^u = \min(5.8387, 5.7368) \cong 5$.

Similarly, $x_2^u = 8, x_3^u = 5, x_4^u = 6$, respectively. Therefore, the starting point in the search would be $x = [5111]$, and will finish once we reach $x = [1116]$.

After following the steps of the algorithm with minimum cost difference of 3.7 units, the optimum system reliability, $R^* = 0.8559967$ is obtained for $x^* = [2232]$. Although the total number of search points in the region is 1200, the functional evaluations performed by the algorithm were only done at 43 points, whereas the number of functional value comparisons to obtain maximum reliability was only 5.

The above steps are the essence of the algorithm, and other variables shown in the algorithmic steps are just to make the translation of the algorithm in a suitable programming language easy.

33.4 Applications of MIP to Various System Design Problems

Here we provide an exhaustive list of applications areas and problem formulations, where the MIP has been successfully applied. The areas are as follows:

33.4.1 Reliability Maximization Through Active Redundancy

33.4.1.1 SP System with Linear and/or Nonlinear Constraints

The series parallel (SP) model is one of the simplest and most widely used models in reliability studies. Mathematically, the problem for such systems could be formulated as:

$$\textit{Maximize } R_s = \prod_{j=1}^{n} (1-(1-r_j)^{x_j}), \tag{33.8}$$

$$\textit{Sub. to: } g_i(x_j) = \sum_{j=1}^{n} c_{ij} x_j \le b_i, i = 1,2...m, \tag{33.9}$$

where the constraints could either be linear, nonlinear or a combination of both (linear and nonlinear).

Example 1: The illustration taken belongs to this category, where the constraints are linear. The optimal solution point provided by the algorithm is $x^* = [2232]$, with optimal system reliability $R_s^* = 0.85599$, with resource consumptions as 50.1 and 49.9, respectively.

Example 2: Consider a SP System with five subsystems, three nonlinear constraints with subsystem reliabilities $r = [0.80\ 0.85\ 0.90\ 0.65\ 0.75]$, respectively. The problem is to

$$\text{Maximize } R_s = \prod_{j=1}^{5} (1-(1-r_j)^{x_j}),$$

Subject to:

$$x_1^2 + 2x_2^2 + 3x_3^2 + 4x_4^2 + 5x_5^2 \le 60,$$
$$7(x_1 + e^{-x_1/4}) + 7(x_2 + e^{-x_2/4}) + 5(x_3 + e^{-x_3/4}) + 9(x_4 + e^{-x_4/4}) + 4(x_5 + e^{-x_5/4}) \le 225,$$

and

$$7x_1 e^{x_1/4} + 8x_1 e^{x_1/4} + 8x_1 e^{x_1/4} + 6x_1 e^{x_1/4} + 9x_1 e^{x_1/4} \le 340.$$

The optimal solution point provided by the algorithm is $x^* = [22223]$ with an optimal value of system reliability of $R_s^* = 0.80247$, and resources consumed of 58, 122.63 and 152.78, units, respectively.

33.4.1.2 NSP System with Linear and/or Nonlinear Constraints

The general formulation of the problem for such systems is:

$$\text{Maximize } R_s = f(x, r) \quad (33.10)$$
$$\text{Sub. to } g_i(x) \le b_i,\ i = 1, 2...m, \quad (33.11)$$

where $f(x, r)$ is the reliability function of the NSP system.

Example 3: Consider a NSP system with five nodes and seven links as shown in Figure 33.1.

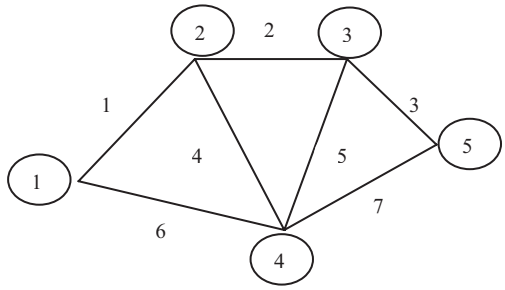


Figure 33.1. A five-node, seven-link NSP system

The objective is to maximize the reliability of the network with the following linear cost constraint:

$$4x_1 + 5x_3 + 2x_4 + 3x_5 + 3x_6 + 5x_7 \le 45,$$

given the component reliabilities as $r = [0.7, 0.9, 0.8, 0.65, 0.7, 0.85, 0.85]$. The optimal reliability of the network computed by the algorithm is $R_s^* = 0.99951$ at $x^* = [1121143]$ with no slacks. Also, out of a total of 11,61,600 search points, it carries out functional evaluations only at 815 points.

Example 4: Consider the bridge network shown in Figure 33.2 with the following three nonlinear constraints:

$$x_1^2 + 2x_2^2 + 3x_3^2 + 4x_4^2 + 5x_5^2 \le 110,$$
$$7(x_1 + e^{-\frac{x_1}{4}}) + 7(x_2 + e^{-\frac{x_2}{4}}) + 5(x_3 + e^{-\frac{x_3}{4}}) + 9(x_4 + e^{-\frac{x_4}{4}}) + 5(x_5 + e^{-\frac{x_5}{4}}) \le 175,$$

and

$$7x_1 e\frac{x_1}{4} + 8x_2 e\frac{x_2}{4} + 8x_3 e\frac{x_3}{4} + 6x_4 e\frac{x_4}{4} + 9x_5 e\frac{x_5}{4} \le 200.$$

The optimal allocation for maximizing the reliability of the bridge network is computed to be $x^* = [32343]$, with $R_s^* = 0.99951$, with resource consumption $g_1 = 110, g_2 = 156.55, g_3 = 198.44$,

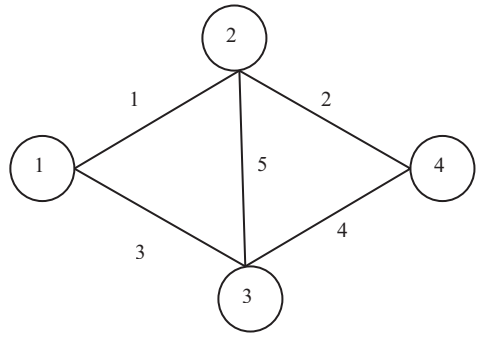


Figure 33.2. A bridge network

respectively. The total number of points visited by the algorithm was 3125, whereas the functional evaluations were at 173 points only.

33.4.2 System with Multiple Choices and Mixed Redundancies

In many engineering applications, it may be possible that the system might need the support of a mixture of available redundancy types (active-parallel, *k*-out-of-*m*, standby, partial, *etc*.) at various subsystems levels. The following example illustrates a typical problem type and its formulation.

Example 5: Consider a three stage series system. The system reliability can be increased by choosing a more reliable component out of four available candidates at stage one. The second stage needs active parallel redundancy whereas the third stage requires a 2-out-of-3:G configuration. The objective is to maximize system reliability with three nonlinear constraints. The formulation of the above problem is as follows.

The objective of the problem can be formulated as:

$$\textit{Maximize } R_s = \prod_{j=1}^{n} R_j(x_j), \tag{33.12}$$

where $R_j(x_j)$ is the *j*th subsystem reliability whose form would vary from subsystem to subsystem and therefore no closed form expression for R_s can be obtained. The constraints can either be linear or nonlinear of the type given by (33.11). For this case, we have four choices available for the components of reliability at the first stage, *i.e.*,

$$R_1 = \begin{bmatrix} 0.88 \\ 0.92 \\ 0.98 \\ 0.99 \end{bmatrix} \text{ (also called ultiple choice).}$$

At the second stage, there is an active redundant system with single component reliability equal to 0.81. Clearly, the subsystem reliability expression for this stage would be $R_2(x_2) = 1-(1-0.81)^{x_2}$, and third stage has a 2-out-of-*x*:G subsystem, with unit component reliability = 0.77, *i.e.,* the reliability expression for this stage is given by

$$R_3 = \sum_{2}^{x_3} \binom{x_3}{k} (0.77)(1-0.77)^{x_3-k}.$$

The constraints are:

$$4e^{\left\{\frac{0.02}{1-R_1(x_1)}\right\}} + 5x_2 + 2x_3 \le 45,$$

$$e^{\frac{x_1}{8}} + 3\left(x_2 + e^{\frac{x_2}{4}}\right) + 5(x_3 + e^{\left(\frac{x_3-1}{4}\right)}) \le 65,$$

and

$$8x_2 e^{\frac{x_2}{4}} + 6\left(x_3 - 1\right) e^{\frac{x_3-1}{4}} \le 230.$$

Clearly, the upper and lower bounds of stage one are 1 and 4, respectively, whereas for the others, the bounds would be decided by the constraints and can be computed by using (33.6) (see illustration for how to use the equation).

By following the algorithmic steps, the optimal solution is obtained at $x^* = [3,3,6]$ with $R^* = 0.9702399$. The resources consumed were $g = [37.87, 64.26, 155.52]$. The total search points were 144 with functional evaluations performed at 23 points only.

33.4.3 Parametric Optimization

In many cases, a decision maker would like to know the effects on the solution, if a certain change in constraints values are made. Besides, some constraints values may not be known with certainty (usually they are guessed at). In general, the problems of these types can be transformed into parametric nonlinear programming problems. Several formulations to such problems can be found in [2]. A general parametric programming formulation to reliability design for *n*-stage SP systems is:

$$\textit{Maximize } R_s = \prod \left(1-\left(1-r_j\right)^{x_j}\right), \tag{33.13}$$

$$\textit{subject to } \sum_{j=1}^{n} g\left(x_j\right) \le b \pm \theta u_i, i = 1,2...m, \tag{33.14}$$

where $0 = \theta_0 < \theta_1 ... < \theta_l = 1, \theta = \theta_0, \theta_1 ... \theta_l$, $x_j \ge 1$ and are integers, and θ, u_i are non-negative constants. The assumptions made in such formulations are:

1. Each stage is essential for overall operational success of the mission.
2. All components are mutually *s*-independent and in the same stage the probability of failure of components is the same.
3. All the components at each stage work simultaneously, and for the stage to fail, all components in that stage must fail.

We provide an illustration for the above formulation.

Example 6: Consider a series system having four stages and two constraints such that we wish to

$$\textit{Maximize } \begin{matrix} R_s = \left(1-\left(1-0.6\right)^{x_1}\right)\left(1-\left(1-0.9\right)^{x_2}\right) \\ \left(1-\left(1-0.55\right)^{x_3}\right)\left(1-\left(1-0.75\right)^{x_4}\right) \end{matrix},$$

subject to

$$\begin{matrix} 6.2x_1 + 3.8x_2 + 6.5x_3 + 5.3x_4 \le 51.8 + 10\theta \\ 9.5x_1 + 5.5x_2 + 3.8x_3 + 4.0x_4 \le 67.8 - 15\theta, \\ 0 \le \theta \le 1 \end{matrix}.$$

The optimal result was obtained at $\theta = \mathbf{0.37}$, by varying θ between zero to one inclusive, which were the same as obtained by [8]. The optimal allocation was $x^* = [2,2,3,3]$, with $R^* = 0.74401$, and consumed resources were $g = (55.4, 53.4)$.

The summary of optimal results of the numerical examples considered in above sections is shown in Table 33.1.

33.4.4 Optimal Design of Maintained Systems

33.4.4.1 Availability Maximization with Redundancy, Spares and Repair Facility

The availability is a more appropriate measure than reliability or maintainability for maintained systems. So the objective for such systems becomes to maximize availability subjected to multiple constraints (linear and/or nonlinear) taking into account the cost of redundancy, spares and repair facility. Therefore, the formulations to such problems are mostly concerned, directly or

Table 33.1. Summary of the optimal results

Ex. #	Results	Remark
1.	$x^* = [2232]$ $R_s^* = 0.80247$	SP system with two linear constraints
2.	$x^* = [22223]$ $R_s^* = 0.80247$	SP system with three nonlinear constraint
3.	$x^* = [1121143]$ $R_s^* = 0.99951$	NSP with a linear constraint.
4.	$x^* = [32343]$ $R_s^* = 0.99951$	NSP with three nonlinear constraints
5.	$x^* = [3,3,6]$ $R^* = 0.9702399$	Mixed redundant series system with three nonlinear constraints
6.	$x^* = [2,2,3,3]$ $R^* = 0.74401$	Parametric optimization, Series system, two linear constraints

indirectly, with either redundancy or spare parts or repairman allocations. Besides, since these three variables can only assume integer values, availability (a nonlinear function of these variables) optimization would necessitate a nonlinear integer programming formulation but increasing the actual number of variables to three times the number of subsystems as compared to the redundancy allocation problems discussed earlier.

The foregoing section has provided the versatility of the algorithm to deal with redundancy optimization problems related to non-maintained systems. However, it can be applied with equal ease to problems such as spares allocation, repairmen allocation, *etc.*, for maintained system and to multi-criteria optimization.

Let us consider a SP-system of n stages, and each stage not only has redundancy but also has a separate maintenance facility like spares and repair in terms of repair. The jth stage of such a system is shown in Figure. 33.3, where k_j, σ_j and ρ_j, are the minimum number of components (functional requirement), spares, and used repairmen provided for the jth subsystem, respectively. The problem statement of the system is as follows:

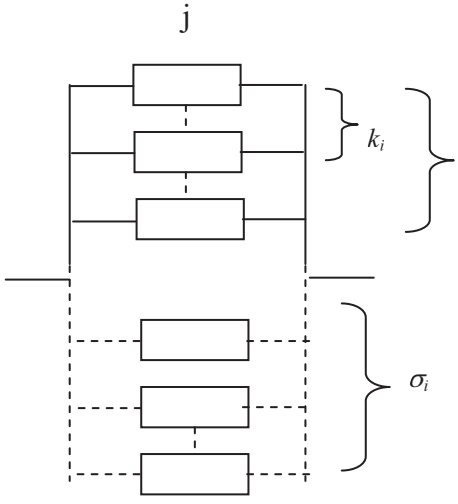


Figure 33.3. A General Subsystem Structure of a j^{th} Stage of a Maintained System

Maximize the availability of a series-parallel maintained system with redundancy, spares, and repair as decision variables, subject to linear constraints. Mathematically, the problem can be expressed as:

$$Maximize\ A_s^s = \prod_{j=1}^{n} A_j^s ,$$

where the steady-state subsystem availability is expressed as $A_i^s \equiv f(x_j, \sigma_j, \rho_j)$, assuming that all subsystems can be repaired independently. The formulation is subject to the constraints,

$$g_i \equiv \sum_{j=1}^{n} g_{ij}\left\{(x_j - k_j), \sigma_j, \rho_j\right\} \le b_i, i = 1, 2...m .$$

The details of various symbols, assumptions, mathematical formulation and solution of the above problem using the present algorithm have been provided in [15, 17].

33.4.5 Computer Communication Network Design with Linear/Nonlinear Constraints and Optimal Global Reliability/Availability

A CCN is defined as a collection of nodes, N, at which the computing resources reside, which communicate with each other via a set of data communicating channels (set of links), L. The main objective of such a CCN is to provide efficient communication among various computer centers in order to increase their utility and to make their services available to more users. One of the fundamental desiderata in designing such a system is that of global availability, *i.e.*, the probability that the network is at least simply connected (connectedness), which depends on the topological layout and the availability of individual computer systems and communication facilities.

Assuming link duplexity, a two state model (working or failed), and the presence/absence of a link in a network can be represented by a binary variable, taking a value either zero or one. The problem for such networks can be stated as [16]: determine an optimal CCN topology that gives maximum overall availability within the given

permissible cost. In other words, the objective is to find a set of links from a given set of links, which together constitute an optimal CCN topology within the budgetary constraints of C_s. Mathematically, the problem can be expressed as:

Maximize $A_s \equiv f(A_1, A_2 \ldots A_n) = f(x_1, x_2 \ldots x_n)$,

subject to:

$$\sum_{j=1}^{n} x_j (y_{j1} y_{j2} \ldots y_{jn}) = \{11 \ldots 1\}, \quad \text{with } \delta(x) \geq N-1 \tag{33.15}$$

$$\sum_{j=1}^{n} c_j x_j \leq c_s \,. \tag{33.16}$$

The form of A_s entirely depends on the network topology and is a minimized expression of global reliability/availability of the network, which can be obtained if the spanning trees of the network are known. In the above formulation, (33.15) signifies the continuity constraint, which ensures that the allocation of the decision variables provides a globally available network. The summation and product sign in the constraint represents binary sum and product, respectively. Note that here $x_j (y_{j1} y_{j2} \ldots y_{jn}) = (x_j y_{j1})(x_j y_{j2}) \ldots (x_j y_{jn})$, and $(y_{j1} y_{j2} \ldots y_{jn})$ is a string of binary variables corresponding to the *j*th link, *e.g.,* if L_j connects the *p*th and *q*th nodes, then $y_{jp}, y_{jq} = 1$, and $y_{jk} = 0 \forall k \neq p \neq q$, *e.g.,* if L_4 connects the second and fourth nodes in a five node network then $(y_{41} y_{42} y_{43} y_{44} y_{45}) = \{01010\}$. Variable x_j can be either one or zero and represents the presence/absence of the link in the network. The cost constraint (33.16) is self explanatory. The details of the above problem and application of the algorithm can be found in [17, 18].

33.4.6 Multicriteria Redundancy Optimization

In many situations, the reliability design problems of complex engineering systems may necessitate consideration of several non-commensurable criteria, which may be equally important. In order to offer alternatives to a system designer, it may be better to achieve some kind of balance among the several conflicting properties rather than to optimize just one property. This situation can be mathematically formulated as multicriteria optimization problem in which the designer's goal is to minimize or maximize not a single objective function but several functions simultaneously.

A multi-objective optimization problem, in general, can be stated as follows:

Find a vector $x^* = [x_1^*, x_2^* \ldots x_n^*]$, which satisfies m inequality constraints

$$g_i(x) \geq 0, i = 1, 2 \ldots m$$

and p equality constraints

$$h_u(x) = 0, u = 1, 2 \ldots p < n,$$

such that the vector function

$$f(x) = [f_1(x), f_2(x) \ldots f_k(x)]$$

gets optimized, where $x^* = [x_1^*, x_2^* \ldots x_n^*]$ is a vector of decision variables defined in the n-dimensional Euclidean space of variables E^n $f(x) = [f_1(x), f_2(x) \ldots f_k(x)]$ is a vector function defined in k-dimensional Euclidean space of objectives E^k, and $g_i(x)$, $h_u(x)$, and $f_l(x)$ are linear and/or nonlinear functions of variables $x_1^*, x_2^* \ldots x_n^*$. The constraints (equality and inequality) define the feasible region X and any point x in X defines a feasible solution.

In fact, the task involved in multi-criteria decision making is to find a vector of the decision variables which satisfies constraints and optimizes a vector function whose elements represent several objective functions. These functions form a mathematical description of the performance criteria, which are usually in conflict with each other. Therefore, the term "optimize" here would mean finding a solution which provides acceptable values for all the objective functions simultaneously.

The extension to MIP to such problems provides an efficient approach for solving multicriteria reliability design problems. This is accomplished in combination with the min-max approach for generating Pareto optimal solutions for multicriteria optimization. For detailed

discussions, examples and their solutions thereof, the interested reader can refer to [11].

33.5 Conclusions

The search approach presented in this chapter is quite versatile in dealing with problems involving integer programming formulations arising in reliability design. The approach can be easily programmed using any suitable language a user is familiar with. It does not require proving any conditions of convexity, concavity or differentiability of involved functions (objective and constraints) in the optimization process. It is simple, requiring only objective function evaluations for testing the feasibility of very few solution vectors in the search space bounded by the constraints and a comparison with the previous value of the evaluated function.

The major benefit that one can draw from such a search pattern is that for a given set of constraints, the search pattern is independent of the objective function involved. This allows a designer to change the objective function without changing the search pattern and one only need evaluate the objective function to arrive at a different optimal solution. This may be found useful in studying various configurations of constituent subsystems/ components for optimal reliability or any other measures of system performance.

The technique is not only an effective and efficient tool for problems involving single objective functions but is also suitable for problems involving multiple objective functions.

References

[1] Becker PW. The highest and lowest reliability achievable with redundancy. IEEE Transactions on Reliability 1977; R-26:209–213.

[2] Chern MS, Jan RH. Parametric programming applied to reliability optimization problems. IEEE Transactions on Reliability 1985; R-34(2):165–170.

[3] Everett III H. Generalized Lagrangian multiplier method for solving problems of optimum allocation of resources. Operations Research 1963; 11:339–417.

[4] Federowicz AJ, Mazumdar M. Use of geometrical programming to maximize reliability achieved by redundancy. Operations Research 1968; 16:948–954.

[5] Geoffrion AM. Integer programming by implicit enumeration and Bala's method. Society of Industrial and Applied Mathematics Review 1967; 9:178–190.

[6] Kuo W, Prasad VR, Tillman FA, Hwang C. Optimal reliability design: fundamentals and applications. Cambridge University Press, 2001.

[7] Lawler E, Bell MD. A method for solving discrete optimization problems. Operations Research 1966; 14:1098–1112.

[8] Misra KB. Reliability optimization of series-parallel system Part-I: Lagrangian multiplier approach Part:II maximum principle approach. IEEE Transaction on Reliability 1972; R-21(4):230–238.

[9] Misra KB. Search procedure to solve integer programming problems arising in reliability design of a system. International Journal of Systems Science 1991; 22(11):2153–2169.

[10] Misra KB. Reliability analysis and prediction: A methodology oriented treatment. Elsevier, Amsterdam, 1992.

[11] Misra KB. Multicriteria redundancy optimization using an efficient search procedure. International Journal of System Science.1991; 22(11):2171–2183.

[12] Misra K, Misra V. Search method for solving general integer programming problems. International Journal of System Science 1993; 24(12): 2321–2334.

[13] Misra KB (Editor). New trends in system reliability evaluation. Elsevier, Amsterdam, 1993.

[14] Ohno K. Differential dynamic programming for solving nonlinear programming problems. Journal of Operations Research Society of Japan 1978; 21:371–398.

[15] Sharma U, Misra KB. Optimal availability design of a maintained system. Reliability Engineering and System Safety 1988; 20:146–159.

[16] Sharma U, Misra KB, Bhattacharji A.K. Optimization of computer communication networks: Exact and heuristic approaches, Microelectronics and Reliability 1990; 30: 43–50.

[17] Sharma U. On some aspects of reliability design of complex systems. Ph. D. Thesis, Guide: Misra KB, Reliability Engineering Centre, IIT Kharagpur, 1990.

[18] Sharma U, Misra KB, Bhattacharji AK. Applications of an efficient search technique for optimal design of a computer communication network. Microelectronics and Reliability 1991; 31:337–341.

34

Reliability Demonstration in Product Validation Testing

Andre Kleyner

Delphi Corporation, USA

Abstract: This chapter presents an overview of reliability demonstration methods applied in the industry for product validation programs. Main emphasis is made on success run testing and test to failure approaches. It also presents a discussion on the underlying assumptions, complexities, and limitations of the reliability demonstration methods.

34.1 Introduction

Reliability testing is the cornerstone of a reliability engineering program. A properly designed series of tests, particularly during the product's earlier design stages, can generate data that would be useful in determining if the product meets the requirements to operate without failure during its mission life. Most of the product development programs require a series of environmental tests to be completed to demonstrate that the reliability requirements are met by the manufacturer and consequently demonstrated to the customer.

Reliability demonstration testing is usually performed at the stage where hardware (and software when applicable) is available for tests and is either fully functional or can perform most of the intended product functions. Designing adequate reliability demonstration tests also referred as product validation tests is an integral part of any reliability program. While it is desirable to be able to test a large population of units to failure in order to obtain information on a product's or design's reliability, time and resource constraints sometimes make this impossible. In cases such as these, a test can be run on a specified number of units, or for a specified amount of time, that will demonstrate that the product has met or exceeded a given reliability at a given confidence level. In the final analysis, the actual reliability of the units will of course remain unknown, but the reliability engineer will be able to state that certain specifications have been met. This chapter will discuss those requirements and different ways of meeting and exceeding them in the industrial setting. The examples and case studies in this chapter are taken from the automotive and consumer electronics industries, where most of the discussed methods are utilized on an every day basis.

34.2 Engineering Specifications Associated with Product Reliability Demonstration

The majority of the products designed to be utilized by consumers in the real world are

validated using a series of environmental tests. Product development usually begins with technical specifications covering various aspects of product requirements including the expected reliability. A model example of reliability specifications is the General Motors standard for validation of electrical and electronic products [1], one of the few such documents available in the open literature. This standard covers a wide variety of environmental tests including temperature, humidity, vibration, mechanical shock, dust, electrical overloads, and many others. Analysis of product specifications and the resulting development of the test plan is a critical stage of product validation, since it is where most of its engineering and business decisions are made. Due to a large variety of required test procedures it would take a long time to do all the required tests sequentially on the same set of units.

The test flow may have several test legs ran in parallel in order to reduce the total test time and also to accommodate the destructive tests, such as flammability, assembly crush, immersion, and others. Parallel testing saves time but increases the size of the sample population, since each leg would require its own set of test units. A truncated example of a GMW3172 [1] test flow is presented in Figure 34.1.

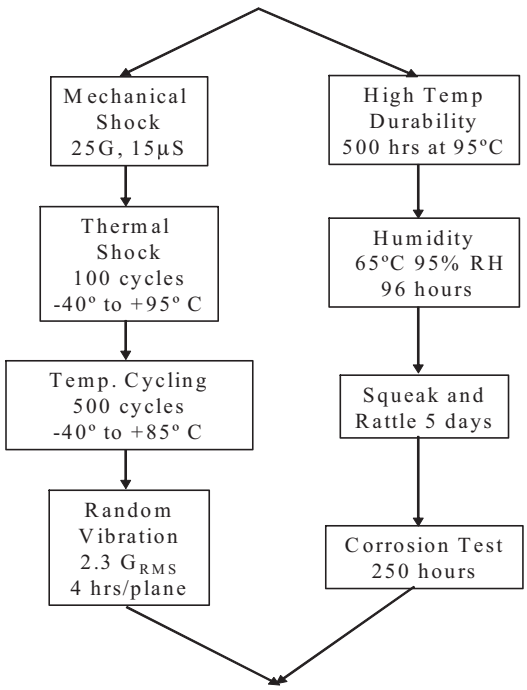


Figure 34.1. Example of a product validation test flow per GMW3172

Most environmental tests for a functional hardware can be divided into two categories: *durability* tests and *reliability* [2] (often referred as *capability* [1] *or robustness*) tests. The durability tests are intended to simulate a full mission life and may trigger some fatigue failure mechanisms. For example, the most common automotive durability tests are vibration, high temperature endurance, low temperature endurance, PTC (power temperature cycling), and others. These types of tests require costly test equipment and are often lengthy and expensive to perform. For example, an automotive electronics PTC tests may take several weeks and are often sequenced with other environmental tests. The capability /reliability / robustness tests do not simulate the mission life, but instead are used to verify that the product is capable of functioning under certain environmental conditions. Failures in capability tests can result in a permanent damage or a temporary loss of function that can be "reset" after the environmental stressing condition is withdrawn. The examples of these tests can include dust exposure, over-voltage, transportation packaging, altitude, moisture susceptibility, and some others.

With increasing demands for development cost reduction and shortening of the product development cycle time, there is often a pressure to reduce the test sample size, test duration, or both. Even with the accelerated test levels there are certain limits on achieving that objective, therefore the modern validation program should accommodate all the available knowledge about the product, its features, functionality, environments, expected failure modes, *etc*. The durability testing is where the potential cost savings can be substantial due to the longer tests intended to represent the total mission life as opposed to capability tests that are targeted at discovering more easily detectable design flaws. Considering that a product is normally designed to survive a predetermined mission life (*e.g*., 10 years

and/or 150,000 miles for automotive products) reliability demonstration concepts most often applied to demonstrate that the particular reliability would reveal the adequacy of the design to the engineering specifications as well the consistency of the product parameters across the production lot.

Most engineering product specifications have reliability demonstration requirements, which are usually expressed in terms of B_X life, MTBF, MTTF, failure rates, and reliability-confidence terms. B_X life is the time at which X% of the units in a population will have failed and can be expressed by the equation below.

$$R(B_X) = (100 - X)\% . \qquad (34.1)$$

For example the B_{10} life of 10 years would be equivalent to 90% reliability for 10 year mission life. MTBF (mean time between failures), MTTF (mean time to failure), and failure rates are all reliability terms derived under assumption of exponential distribution (34.2), where MTBF applies to repairable systems and MTTF to non-repairable,

$$R(t) = e^{-\lambda t} , \qquad (34.2)$$

where:
$R(t)$ = reliability as a function of time,
λ = failure rate, and
t = time.

Under exponential distribution assumption of (34.2) MTTF is a time period where 62.3% of the population fail, and failure rate can be calculated as λ = 1/MTTF for non-repairable systems and λ = 1/MTTF for repairable.

One form of reliability requirement can usually be converted to the other and used interchangeably. For example, the B_{10} life of 10 years can be converted into MTTF by merging (34.1) and (34.2) in the following way:

$$R(10yr) = 0.9 = e^{-\frac{10yrs}{MTTF}} . \qquad (34.3)$$

Therefore by solving (34.3) we would find that MTTF = 94.9 years is required to meet the B_{10} life requirement of 10 years. The application of technical specifications containing system reliability and confidence level will be discussed in detail in the next section.

In addition to reliability demonstration, product technical specifications may also contain requirements on reliability prediction, which is simply the analysis of parts and components in an effort to predict and calculate the rate at which the system will fail. A reliability prediction is usually based on an established model. Common models are MIL-HDBK-217, RDF2000, Telcordia for electronic components and NSWC-98/LE1 for mechanical components. Reliability predictions usually reflect the inherent reliability of the product and due to their analytical nature are often higher than those required for the reliability demonstration. This alone can be a cause of confusion and misunderstanding between design engineers, system engineers, and reliability specialists. More detailed information on reliability prediction methods can be found in [3].

34.3 Reliability Demonstration Techniques

34.3.1 Success Run Testing

One of the most common techniques utilized in the industry, where survival of the product at the end of the test is expected, is called *success run testing*. Industry dependent, it is also referred to as an attribute test, a zero failure substantiation test, a mission life test, or a non-parametric binomial. Under those conditions a product is subject to a test, which is often accelerated, representing an equivalent to one mission life (*test to a bogey*), which is expected to be completed without failure by all the units in the test sample.

Success run testing is most often based on the binomial distribution, requiring a particular test sample size in order to demonstrate the desired reliability number with the required confidence level [4]. For example, a common requirement in automotive industry is to demonstrate a reliability of 97% with a 50% confidence level.

Mathematically it can be presented as follows: let us consider p as a probability of a product to fail. According to binomial distribution the probability of obtaining k bad items and $(n-k)$ good items $f(k)$ is:

$$f(k) = \frac{n!}{k!(n-k)!} p^k (1-p)^{n-k}. \quad (34.4)$$

If applied to reliability, where $R=1-p$, and based on (34.4)

$$C = 1 - \sum_{i=0}^{k} \frac{N!}{i!(N-i)!} R^{N-i} (1-R)^i, \quad (34.5)$$

where R = unknown reliability,
C = confidence level required, and
N = total number of test samples.

If k = 0 (no units failed), (34.2) turns into the equation for success run testing:

$$C = 1 - R^N. \quad (34.6)$$

Equation (34.6) can be solved for the test sample size N as:

$$N = \frac{\ln(1-C)}{\ln R}. \quad (34.7)$$

From (34.7) it is easy to notice that if the demonstrated reliability R is approaching 1.0 the required sample size N is approaching infinity. Table 34.1 illustrates (34.7) for the confidence levels of 50% and 90%.

Table 34.1. Examples of reliability sample sizes at confidence levels of 50% and 90%

Reliability, R	Sample size N at $C=50\%$	Sample size N at $C=90\%$
90%	7	22
95%	14	45
97%	23	76
99%	69	230
99.9%	693	2,301
99.99	6,932	23,025

Cost considerations are always an important part of the test planning process. The test sample size carries the cost of producing each test sample (which can be quite high in some industries), equipping each sample with monitoring equipment, and adequate test capacity equipment to accommodate all the required samples (for the cost details see the section on cost reduction). The last contribution to the test sample size can present a significant cost problem, since a large sample may require additional capacities of expensive test equipment, such as temperature/humidity chambers or vibration shakers costing tens or hundreds of thousands of dollars. More details on product validation costs will be presented later in this chapter

Example 1

To simplify the calculations, let us consider 500 cycles of PTC (Figure 34.1) as a test equivalent of one mission life of 10 years in the fields. In order to meet the automotive electronics requirement of R = 97%, C = 50% [1] it would be required according to (34.7) to run $N = \ln(0.5)/\ln(0.97) = 23$ samples without failure for the duration of 500 cycles. It is important to note that by testing the product to pass we would in practice demonstrate the lower boundaries of the obtained values. In this example, a 97% demonstrated reliability establishes the lower boundary value ($R \geq 97\%$), and would not automatically doom the remaining 3% of the population to failure.

Among the advantages of success run testing is its shorter time and the ease of monitoring. Indeed, the test duration would be limited to only one equivalent of the mission life and it would be necessary to check the hardware functionality only after the test is complete. On the downside, a success run does not provide enough information about the design margins, since the entire test results are only relevant to the completed tests. For example, after successful completion of the 8-hour bogey vibration testing we would not be able to tell if the product would have failed soon after the 8-hour mark or would have enough design margin to survive another mission life.

34.3.2 Test to Failure

Due to increasing computing power and a desire to better understand the product design margins test to failure is often requested by the customer as a part of reliability demonstration program. The Weibull distribution is one of the most widely used lifetime distributions in reliability engineering. It is a versatile distribution that can take on the

characteristics of other types of distributions, based on the value of its shape parameter.

Under two-parameter Weibull distribution the product reliability function *R(t)* can be presented in form of:

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^{\beta}}, \qquad (34.8)$$

where:
β = Weibull shape parameter,
η = Weibull scale parameter, and
t = time.

For analysis purposes (34.8) can be rewritten as:

$$\frac{1}{1-F(t)} = e^{\left(\frac{t}{\eta}\right)^{\beta}}, \qquad (34.9)$$

where $F(t) = 1 - R(t)$ is a cumulative failure function often calculated using median ranks for the 50% confidence level [5].

If we take two natural logarithms of (34.9) it will take the form of:

$$\ln\ln\frac{1}{1-F(t)} = \beta(\ln t) - (\beta \ln \eta). \qquad (34.10)$$

This equation has a linear form $Y = \beta X + C$,
where :
$Y = \ln(\ln[1/(1-F(t))])$,
$X = \ln t$, and
$C = -\beta \ln \eta$.

Equation (34.10) represents a straight line with a slope β and intercept C on the Cartesian X, Y coordinates. Hence the plot of $\ln(\ln[1/(1-F(t))])$ against $\ln t$ will be a straight line with the slope of β. According to (34.8) parameter η can be determined as an X-coordinate corresponding to the unreliability of 63.2% on the Y-axis. The obtained Weibull parameters β and η can be substituted into (34.8) in order to define the reliability as a function of time $R(t)$. With the use of the available on the market software packages the Weibull function can be easily calculated within any confidence bounds required by the product's technical specifications. For more details on test to failure and Weibull distribution see [5] or [6].

Example 2

Let us consider reliability requirements [1], where test-to-failure can be an alternative to success run testing with the expected test duration not exceeding two mission lives. 23 samples were placed on test for 1000 temperature cycles (2× mission life). During that time 5 units have failed at 550, 600, 700, 750, and 1000 cycles. The remaining 18 functional units were considered suspended at the end of the test. The Weibull plot in Figure 34.2 demonstrates 97% reliability at 500 cycles with 50% confidence. Please note that the suspended units are not shown in the Weibull plot, but accounted for in the process of calculating median ranks and therefore $F(t)$.

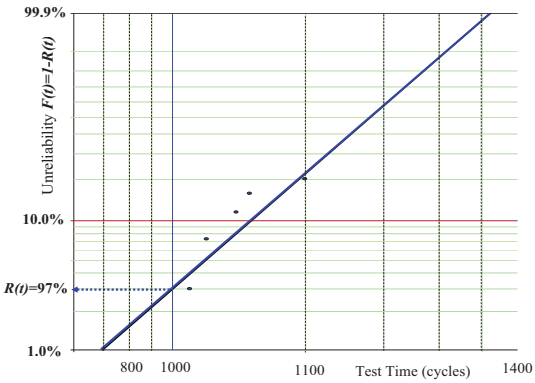


Figure 34.2. Weibull plot of the life data in the example (generated with ReliaSoft®, Weibull++)

The test to failure approach and consequently Weibull analysis has many advantages, since it provides more comprehensive information about the product reliability. It includes the analytical description of the reliability as a function of time $R(t)$, a better understanding of the product's design margins, and a better determination of the product's life phase on the bathtub curve (infant mortality, useful life, or wear-out mode) [4]. That is partly the reason why an increasing number of customers wants to see Weibull analysis as a part of their validation programs. On the downside, it is typically a longer test, which also requires some form of monitoring equipment to record failure times with a reasonable degree of accuracy. The PTC test in Example 2 took 1000 cycles, which is

twice as long as was required for the success run testing. Therefore, due to the ever-increasing pressure for the development of cycle reduction, project managers, when given the choice, often opt for success run testing.

It is also important to remember that two-parameter Weibull distribution does not hold the monopoly on reliability data analysis. Other statistical distributions such as three-parameter Weibull, lognormal, gamma, exponential, and others are also commonly utilized in the life data analysis.

34.3.3 Chi-Squared Test Design – An Alternative Solution for Success Run Tests with Failures

A method for designing tests for products that have an assumed constant failure rate, or exponential life distribution (34.2), draws on the chi-squared distribution. This method only returns the necessary accumulated test time for a demonstrated reliability or MTTF. The accumulated test time is equal to the total amount of time experienced by all of the units on test combined. The chi-squared method can be useful in the case of failures during a bogey test. This method is often utilized when the failures are unanticipated and/or their exact times are not known. Assuming that the failures follow an exponential distribution pattern (34.2), a one-sided estimate for MTTF based on the total test time T [7] will be:

$$MTTF \geq \frac{2T}{\chi^2_{\alpha,2(k+1)}}, \qquad (34.11)$$

where:
$\chi^2_{\alpha,\,2(k+1)}$ = chi-square distribution,
$\alpha = 1 - C$ = risk factor,
N = number of test units, and
k = number of failures,

Since the failure rate λ = 1/MTTF such that:

$$\lambda \leq \frac{\chi^2_{\alpha,2(k+1)}}{2T}. \qquad (34.12)$$

Therefore, based on (34.12)

$$R \geq \exp\left(-\frac{\chi^2_{\alpha,2(k+1)}}{2N}\right). \qquad (34.13)$$

Example 3

Let us consider the case where one of the 23 test samples required by [1] failed during the expected mission life test. In this case k = 1 with 50% confidence and, therefore $\chi^2_{0.5,\,2(1+1)} = 3.357$. Thus according to (34.13) the demonstrated reliability will be reduced from the 97% obtained earlier to a lower value of

$$R = \exp\left(-\frac{3.357}{2\times 23}\right) = 92.7\%. \qquad (34.14)$$

When failures occur during a success run test, several different outcomes are possible. If a root cause analysis determines that the problem can be attributed to a non-design related problem, such as a test sample quality, test equipment problem, workmanship, or some other assignable cause, the customer may accept the results of the test and continue with the development program. When the failure is attributed to a product design flaw, the customer may request some form of a hardware redesign, material change, or other corrective actions.

34.4 Reducing the Cost of Reliability Demonstration

34.4.1 Validation Cost Model

Naturally one of the goals of test planning is to lower the overall cost of the testing, and one of the ways to achieve that is to reduce a test sample. The expenses linked to the test sample size may be qualified as variable costs. Needless to say, the larger the test sample size the greater the cost of validation. Despite this, the cost effect of the number of samples required to be tested is rarely given enough attention. Meanwhile, each test sample carries the following costs associated with the sample population:

1. The cost of producing a test sample.
2. The cost of equipping each test sample. Applied to electronics it would include harnesses, cables, test fixtures, connectors, *etc*.
3. The cost of monitoring each sample during the test. In the electronics industry this would include the labor costs of:
    - designing and building the load boards simulating the inputs to the electronic units,
    - connecting and running the load boards,
    - recording the data, and
    - visual and other types of inspection.

Considering that some tests may run for weeks or even months, these expenses can be quite substantial. Calculation of product validation cost includes both the cost of ownership of test equipment and the expenses associated with each test sample size [8]. The key cost contributors are: capital and depreciation cost D, which includes acquisition, installation, and cost of scraping, spread over the useful life of the equipment; maintenance cost M, which includes both scheduled and unscheduled maintenance plus indirect maintenance cost; indirect maintenance including technician training, lost revenue due to the equipment idle time, *etc*.;and miscellaneous costs Y including energy cost, floor space, upgrades, insurance, *etc*. Therefore, assuming the 24-hour operation of the test facilities, the total cost of product validation per test can be represented by

$$VAL_Cost = t_T\left(\varphi_T + \frac{(M+D+Y)}{365\times 24}\right)\left\lceil \frac{N}{K} \right\rceil + N(\alpha_p + \alpha_e + \alpha_m) \tag{34.15}$$

where:

φ_T = hourly labor rate of performing the test,
t_T = test duration,
N = test sample size,
K = equipment capacity, and
$\lceil\ \rceil$ = ceiling function, indicating rounding up to the next highest integer,
α_p = cost of producing one test sample,
α_e = cost of equipping one test sample, and
α_m = cost of monitoring one test sample.

It is also important to note that the increase in sample size may cause the growth of the equipment-related cost as a step-function due to a discrete nature of the equipment capacity. For example, if a temperature chamber can accommodate 25 units of a particular geometric size, then a test sample of 26 units would require two chambers instead of the one needed for 25 samples, *i.e.*, $\left\lceil \frac{N}{K} \right\rceil = \left\lceil \frac{26}{25} \right\rceil = 2$.

As can be seen from (34.15) the test sample size N is a critical factor in defining the cost of validation program. Depending on the geometry along with the complexity of the product test samples and what is involved in validating them, test sample sizes above certain level become impractical due to the rapidly growing "variable" cost of validation. With ever-increasing reliability requirements, the sample population to be tested would require more and more of human resources and capital equipment.

34.4.2 Extended Life Testing

Test duration can be used as a factor to affect the cost of product validation. There is a relationship between the test sample size and the test duration referred to as the *parametric binomial*, which allows the substitution of test samples for an extended test time and *vice versa*. This relationship is based on Lipson equality [9] tying one test combination (N_1, t_1) with another (N_2, t_2) needed to demonstrate the same reliability and confidence level,

$$\frac{N_2}{N_1} = \left(\frac{t_1}{t_2}\right)^{\beta}, \tag{34.16}$$

where:

β = the Weibull slope for primary failure mode (known or assumed),
N_1, N_2 = test sample sizes, and
t_1, t_2 = test durations.

Therefore it is possible to extend the test duration in order to reduce the test sample size. The new test duration $t_2 = Lt_1$, where t_1 is a product mission life or its test equivalent and L is

the life test ratio. Thus combining (34.15) and (34.16) will produce

$$N_1 = L^{\beta} N_2 . \quad (34.17)$$

With the use of (34.17) the classical success run formula (34.6) will transform into:

$$C = 1 - R^{NL^{\beta}} \ or \ R = (1-C)^{\frac{1}{NL^{\beta}}} . \quad (34.18)$$

Besides the understandable cost saving objective, (34.18) is often used to match the test equipment capacity in the cases, where N is slightly higher than K, see (34.15). The required number of test samples can be reduced L^{β} times in the cases of extended life testing ($L > 1$). Therefore, this approach allows an additional flexibility in minimizing the cost of testing by adjusting the test sample size up or down according to the equipment capacity. The detailed derivation of (34.18) and its applications can be found in [9] and is also reproduced in [10]

Example 4

The relationship (34.18) is widely utilized in the automotive electronics industry and beyond and it has been included in various engineering specifications. In Example 3 let us assume that the temperature chamber along with the test monitoring rack has a capacity of only 12 units. Applying (34.18) as recommended by [1], we propose the alternative test sample size of 12 units instead of the previously discussed 23. The value of Weibull slope β, suggested by [1] is 2.0. Thus substituting $R = 97\%$, $C = 90\%$, $n = 12$, and $\beta = 2.0$ into (34.18) produces:

$$L = \left(\frac{\ln(1-C)}{N \ln R} \right)^{\frac{1}{\beta}} = \left(\frac{\ln(1-0.9)}{12 \ln 0.97} \right)^{\frac{1}{2}} = 1.38 . \quad (34.19)$$

Therefore the original test duration of 500 cycles (see Example 1) would be transformed into Lt = 1.38×500=690 cycles without failures in order to demonstrate our initial reliability goals with only 12 samples instead of 23.

It is important to note that (34.18) is derived under the assumption of success run testing, *i.e.*, no failures are experienced during the test. However as L increases, the probability of a failure occurrence also increases. Therefore, the value of L should be limited to provide a reasonable duration within the framework of success run testing. The β-value in (34.18) is corresponding to the end-of life conditions and, therefore, the higher β the sooner the product would be expected to fail, and the higher the probability that the *zero-failure* assumption will be violated.

34.4.3 Other Validation Cost Reduction Techniques

As demonstrated before, the test sample size grows exponentially with the increasing reliability targets. For example, Table 34.1 shows that the demonstration of $R = 99.9\%$ with 90% confidence would require the impractical number of 2,301 samples. However in some cases customer requirements do contain very high reliability targets, which cannot be supported by conventional reliability demonstration testing. In those instances, alternative methods and techniques should be considered. The approaches to reduce the test sample size to a manageable level include knowledge-based techniques, such as Bayesian analysis. Most of the designed products are created through a development cycle of evolutional rather than revolutionary changes. Thus a certain amount of existing product information can be incorporated into a validation program by utilizing the Bayesian approach of analyzing priors and obtaining posteriors. In the cases where priors are favorable, *i.e.*, high reliability of the existing product or its prototypes, a significant reduction in sample size can be achieved. More detailed information about these methods can be found in [11, 12, 13].

Another cost reduction alternative is HALT (highly accelerated life test) where the specially designed test equipment creates environmental conditions well exceeding those in the field and even exceeding the conditions applied during conventional accelerated tests. More details about HALT can be found in [14]. Even though HALT is often utilized in reliability testing due to significant cost savings, its appropriateness as a reliability demonstration tool has often been debated due to the inconsistency of HALT-induced failure modes with those observed in the field. The HALT test is

considered as an excellent qualitative learning method that quickly identifies product weaknesses or operating limits from vibration and temperature, rather than as a conventional reliability demonstration tool.

Analytical methods such as finite element analysis, stress-strength calculations, stochastic simulation, design for six sigma, and field return analysis can also be applied in estimating expected product reliability. However they are not generally considered as reliability demonstration methods and are not covered in this chapter.

34.5 Assumptions and Complexities of Reliability Demonstration

In the industrial setting involving suppliers and customers, validation programs often require approvals of OEMs or a lower-tier supplier, which sometimes becomes a source of contention. As mentioned before, in some instances customers set the reliability targets to a level not easily achievable by the conventional methods listed in this chapter, which might require the interference of the deep-skilled reliability professionals on both sides.

It is important to remember that the upward potential of the demonstrated reliability is severely limited by the test sample size no matter which method you choose and therefore by the amount of money a company can afford to spend on validation activities. Moreover, the issue of reliability demonstration becomes even more confusing when the customer directly links it with the expected product performance in the field [15]. More than once we have heard the argument that reliability of 99.9% would be equivalent to 5,000 babies going home from the hospital with the wrong parents, 2000 wrong prescriptions per year, 1000 lost articles of mail per week, or some other scary statistics. Naturally, nobody wants all those bad things to happen, but that is the point where the issue of reliability demonstration by test gets confused. In order to clarify some of these issues, the following are the arguments against equating the number of units subject to test with the outcome of product's quality and reliability.

Firstly, the reliability of R=99.9% implies 0.1% accuracy, which cannot possibly be obtained with the methodologies applied. Most of the tests performed by reliability engineers (the automotive industry is no exception) are accelerated tests with all the uncertainties associated with testing under conditions different from those in the field, the greatest contributor to which would be the field to test correlation. In other words, based on a test lasting from several hours to several weeks, we are trying to draw conclusions about the behavior of the product in the field for the next 10–15 years. There are humidity failure modes, thermal cycling failure modes, vibration failure modes, high temperature dwell failure modes, *etc*. With so many unknown factors the overall uncertainty well exceeds 0.1% accuracy.

Secondly, system interaction problems contribute heavily to warranty claims. The analysis of automotive warranties shows that reliability related failures comprise only a fraction of the field returns. Thus even if such a high reliability is demonstrated, it would not nearly guarantee that kind of performance in the field, since many other failure factors would be present. Quality defects (items not produced to design specifications) also contribute heavily to the amount of warranty returns. The purpose of reliability testing is to validate the product design and the process design; it is not a tool to capture or control quality defects, design variations, process variations, system non-conformances, customer abuse, *etc*.

As mentioned before, reliability analysis has a considerable element of uncertainty. The business of predicting the life of a product has also much in common with biological and medical sciences. At present no amount of tests can accurately predict the life expectancy of a particular individual. It can be done on a statistical level and only on a large population, while the accuracy of that prediction will be low for a small group of individuals. The same is true of hardware life. There are many models that can provide data on product life under given conditions, but there is no model that can exactly predict a product life for all failure modes. It often takes some paradigm adjustment to accept a certain level of fuzziness in reliability science, and therefore reliability engineers should not

become fixated on one model or method and should instead try to find the right tool(s) for the job. Stepped overstress testing, finite element analysis, stress-strength calculations, stochastic simulation, design for six sigma, HALT programs, and field return analysis are often more appropriate than hopelessly trying to meet quadruple or quintuple reliability *nines* by stuffing chambers with ever-increasing numbers of test units. The practicality of testing should be a strong consideration of what reliability and confidence level to select, taking into account the feasibility and cost aspects of a particular testing. Reliability demonstration testing is just one tool among many in the large toolbox available to reliability engineers and test development professionals.

34.6 Conclusions

Now, with all that said, let us summarize what indeed the practical value of reliability demonstration testing is. It offers a consistent approach to testing and to addressing the issue of product and process design performance. It provides a consistent approach to sample size selection based on the testing goals. Indeed, it always helps to plan a test when there are mathematical criteria as to why 20 samples are better than 10 and how much better. In addition, it provides a clear trigger for when corrective actions need to be taken by meeting or not meeting the initial reliability requirements linked to the test sample size. It can also be a good figure of merit for comparing product design A versus design B in terms of expected reliability. Based on that, reliability testing and demonstration will most likely remain a valuable engineering tool for many years to come.

References

[1] GMW3172, General specification for electrical/electronic component analytical/development/ validation (A/D/V) Procedures for Conformance to Vehicle Environmental, Reliability, and Performance Requirements, General Motors Worldwide Engineering Standard, 2005. http://www.standardsstore.ca

[2] Lewis M. Designing reliability-durability testing for automotive electronics – A commonsense approach. TEST Engineering and Management 2000; August/September: 14–16.

[3] ReliaSoft Corporation. Lambda predict users guide. ReliaSoft Corporation, Tucson, AZ, 2004, http://www.reliasoft.com

[4] O'Connor P. Practical reliability engineering. 4th edition, Wiley, New York, 2003.

[5] Abernethy R. The new Weibull handbook. 4th edition by Dr. Robert Abernethy, ISBN 0-9653062-1–6, 2000.

[6] ReliaSoft Corporation. Weibull++ user guide. ReliaSoft Corporation, Tucson, AZ, 2002. http://www.reliasoft.com

[7] Kececioglu D, Reliability engineering handbook. Prentice Hall, Englewood Cliffs, NJ, 2002.

[8] Kleyner A, Sandborn P, Boyle J. Minimization of life cycle costs through optimization of the validation program – A test sample size and warranty cost approach. Proceedings of Annual Reliability and Maintainability Symposium, Los Angeles., CA, 2004; 553–557.

[9] Lipson C, Sheth N. Statistical design and analysis of engineering experiments. McGraw-Hill, New York, 1973.

[10] Kleyner A, Boyle J. Demonstrating product reliability: Theory and application. Tutorial Notes of Annual Reliability and Maintainability Symposium, Alexandria, VA, Jan. 2005; (Section 12).

[11] Martz H, Waller R. Bayesian reliability analysis. Wiley, New York, 1982.

[12] Kleyner A, Bhagath S, Gasparini M, Robinson J, Bender M. Bayesian techniques to reduce the sample size in automotive electronics attribute testing. Microelectronics and Reliability 1997; 37(6):879–883.

[13] Krolo A, Bertsche B. An approach for the advanced planning of a reliability demonstration test based on a Bayes procedure. Proc. RAMS -Conference, Tampa, FL; Jan. 2003:288–294.

[14] Hobbs G. Accelerated reliability engineering: HALT and HASS. Wiley, New York, 2000.

[15] Kleyner A, Boyle J. The myths of reliability demonstration testing. TEST Engineering and Management 2004; August/ September: 16–17.

35

Quantitative Accelerated Life-testing and Data Analysis

Pantelis Vassiliou[1], Adamantios Mettas[2] and Tarik El-Azzouzi[3]

[1]President and CEO, ReliaSoft Corporation, USA
[2]VP Product Development, ReliaSoft Corporation, USA
[3] Research Scientist, ReliaSoft Corporation, USA

Abstract: Quantitative accelerated testing can reduce the test time requirements for products. This chapter explains the fundamentals of quantitative accelerated life testing data analysis aimed at quantifying the life characteristics of the product at normal use conditions and the currently available models and procedures for analyzing data obtained from accelerated tests involving time-independent single stress factor, time-independent multiple stress factors and time varying stress factors.

35.1 Introduction

Accelerated tests are becoming increasingly popular in today's industry due to the need for obtaining life data quickly. Life testing of products under higher stress levels, without introducing additional failure modes, can provide significant savings of both time and money. Correct analysis of data gathered *via* such accelerated life testing will yield parameters and other information for the product's life under use stress conditions.

Traditional "life data analysis" involves analyzing times-to-failure data (of a product, system or component) obtained under "normal" operating conditions in order to quantify the life characteristics of the product, system or component. In many situations, and for many reasons, such life data (or times-to-failure data) is very difficult, if not impossible, to obtain. The reasons for this difficulty can include the long life times of today's products, the small time period between design and release, and the challenge of testing products that are used continuously under normal conditions. Given this difficulty, and the need to observe failures of products to better understand their failure modes and their life characteristics, reliability practitioners have attempted to devise methods to force these products to fail more quickly than they would under normal use conditions. In other words, they have attempted to accelerate their failures. Over the years, the term *accelerated life testing* has been used to describe all such practices.

35.2 Types of Accelerated Tests

Different types of tests, that have been called accelerated tests, provide different information about the product and its failure mechanisms. Generally, accelerated tests can be divided into three types:

35.2.1 Qualitative Tests

In general, qualitative tests *are not designed to yield life data that can be used in subsequent analysis or for "accelerated life Test analysis.* Qualitative tests do not quantify the life (or reliability) characteristics of the product under normal use conditions. They are designed to reveal probable failure modes. However, if not designed properly, they may cause the product to fail due to modes that would not be encountered in real life.

Qualitative tests have been referred to by many names including elephant tests, torture tests, HALT (highly accelerated life testing) and shake and bake tests. HALT and HASS (highly accelerated stress screening) are covered in more detail in [5] and [6].

35.2.2 ESS and Burn-in

ESS (environmental stress screening) is a process involving the application of environmental stimuli to products (usually electronic or electromechanical products) on an accelerated basis. The goal of ESS is to expose, identify and eliminate latent defects that cannot be detected by visual inspection or electrical testing but which will cause failures in the field.

Burn-in can be regarded as a special case of ESS. According to MIL-STD-883C, burn-in is a test performed for the purpose of screening or eliminating marginal devices before customers receive them. Marginal devices are those devices with inherent defects or defects resulting from manufacturing aberrations that cause time-dependent and stress-dependent failures.

ESS and burn-in are performed on the entire population and do not involve sampling. Readers interested in the subject of ESS and burn-in are encouraged to refer to Kececioglu and Sun [1] for ESS and for burn-in to [2] by the same authors.

35.2.3 Quantitative Accelerated Life Tests

Quantitative accelerated life testing, unlike the qualitative testing methods, consists of quantitative tests designed to quantify the life characteristics of the product, component or system under normal use conditions, and thereby provide "reliability information." Reliability information can include the determination of the probability of failure of the product under use conditions, mean life under use conditions, and projected returns and warranty costs. It can also be used to assist in the performance of risk assessments, design comparisons, *etc*.

Accelerated life testing can take the form of "usage rate acceleration" or "overstress acceleration". Both accelerated life test methods are described next. Because usage rate acceleration test data can be analyzed with typical life data analysis methods, the overstress acceleration method is the testing method relevant to this chapter.

For all life tests, some time-to-failure information for the product is required, since the failure of the product is the event we want to understand. In other words, if we wish to understand, measure, and predict any event, we must observe the event!

35.2.3.1 Usage Rate Acceleration

For products that do not operate continuously under normal conditions, if the test units are operated continuously, failures are encountered earlier than if the units were tested at normal usage. For example, if we assume an average washer use of 6 hours a week, the testing time could conceivably be reduced 28-fold by testing these washers continuously. Data obtained through usage acceleration can be analyzed with the same methods used to analyze regular times-to-failure data.

35.2.3.2 Overstress Acceleration

For products with very high or continuous usage, the accelerated life-testing practitioner must stimulate the product to fail in a life test. This is accomplished by applying stress level(s) that exceed the level(s) that a product will encounter under normal use conditions. The times-to-failure data obtained under these conditions are then used to extrapolate to use conditions. Accelerated life tests can be performed at high or low temperatures, humidity, voltage, pressure, vibration, *etc.*, and/or

combinations of stresses to accelerate or stimulate the failure mechanisms.

Accelerated life test stresses and stress levels should be chosen so that they accelerate the failure modes under consideration but do not introduce failure modes that would never occur under use conditions. Normally, these stress levels should fall outside the product specification limits but inside the design limits (Figure 35.1)

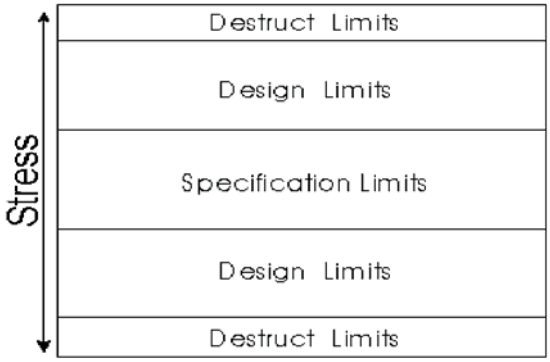


Figure 35.1. Typical stress range for a component, product or system

This choice of stresses as well as stress levels and the process of setting up the experiment are of the utmost importance. Consult your design engineer(s) and material scientist(s) to determine what stimuli (stress) is appropriate as well as to identify the appropriate limits (or stress levels). If these stresses or limits are unknown, multiple tests with small sample sizes can be performed in order to ascertain the appropriate stress(es) and stress levels. Information from the qualitative testing phase of a normal product development process can also be utilized in ascertaining the appropriate stress(es). Proper use of design of experiments (DOE) methodology is also crucial at this step. In addition to proper stress selection, the application of the stresses must be accomplished in some logical, controlled and quantifiable fashion. Accurate data on the stresses applied as well as the observed behavior of the test specimens must be maintained.

It is clear that as the stress used in an accelerated test becomes higher, the required test duration decreases. However, as the stress level moves away from the use conditions, the uncertainty in the extrapolation increases. This is what we jokingly refer to as the "there is no free lunch" principle. Confidence intervals provide a measure of this uncertainty in extrapolation.

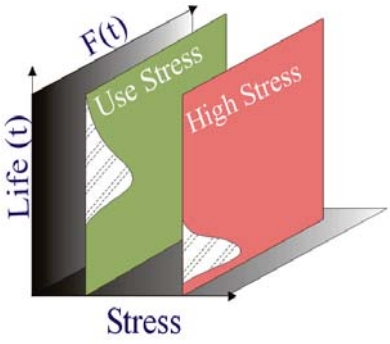
35.3 Understanding Accelerated Life Test Analysis

In accelerated life testing analysis, we face the challenge of determining the use level pdf from accelerated life test data rather than from times-to-failure data obtained under use conditions. To accomplish this, we must develop a method that allows us to extrapolate from data collected at accelerated conditions to arrive at an estimation of use level characteristics. To understand this process, let us look closely at a simple accelerated life test. For simplicity we will assume that the product was tested under a single stress and at a single constant stress level. The pdf of the stressed times-to-failure can be easily obtained using traditional life data analysis methods and an underlying life distribution. The objective in an accelerated life test, however, is not to obtain predictions and estimates at the particular elevated stress level at which the units were tested, but to obtain these measures at another stress level, the use stress level. To accomplish this objective, we must devise a method to traverse the path from the overstress pdf to extrapolate a use level pdf.

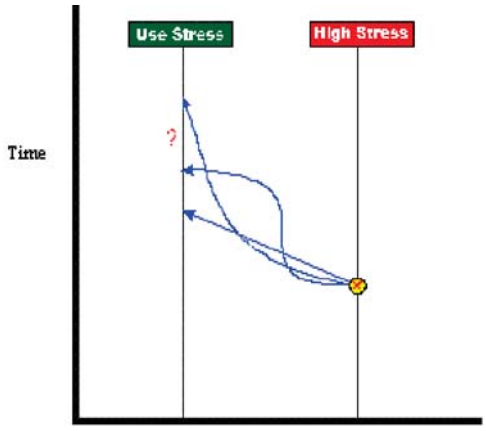
Figure 35.2(a) illustrates a typical behavior of the pdf at the high stress (or overstress level) and the pdf at the use stress level. Figure 35.2(b) illustrates the need to determine a way to project (or map) a certain failure time, obtained at the high stress, to the use stress.

Obviously there are infinite ways to map a particular point from the high stress level to the use stress level. We will assume that there is some road map (model or a function) that maps our point from the high stress level to the use stress level. This model or function can be described mathematically and can be as simple as the equation for a line. Figure 35.3 demonstrates some simple models or relationships. Even when a model is assumed (*i.e.*, linear, exponential, *etc*.),

the mapping possibilities are still infinite since they depend on the parameters of the chosen model or relationship. For example, we can fit infinite number of lines through a point.



(a)



(b)

Figure 35.2. Traversing from a high stress to the use stress

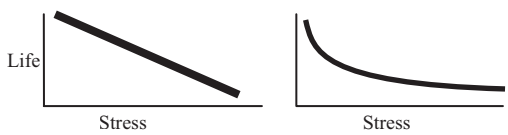


Figure 35.3. A simple linear and a simple exponential relationship

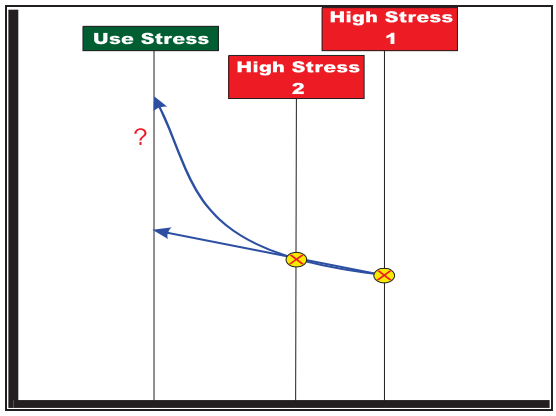


Figure 35.4. Testing at two (or more) higher stress levels allows us to better fit the model

However, if we tested specimens of our product at two different stress levels, we could begin to fit the model to the data. Obviously, the more points we have, the better off we are in correctly mapping a particular point, or fitting the model to our data. Figure 35.4 illustrates the need for a minimum of two stress levels to properly map the function to a use stress level.

35.4 Life Distribution and Life-stress Models

Analysis of accelerated life test data, then, consists of an underlying life distribution that describes the product at different stress levels and a life-stress relationship (or model) that quantifies the manner in which the life distribution (or the life distribution characteristic under consideration) changes across different stress levels. These elements of analysis are shown graphically in Figure 35.5.

The combination of both an underlying life distribution and a life-stress model can be best seen in Figure 35.6 where a pdf is plotted against both time and stress.

The assumed underlying life distribution can be any life distribution. The most commonly used life distributions include, Weibull, the exponential and the lognormal distributions.

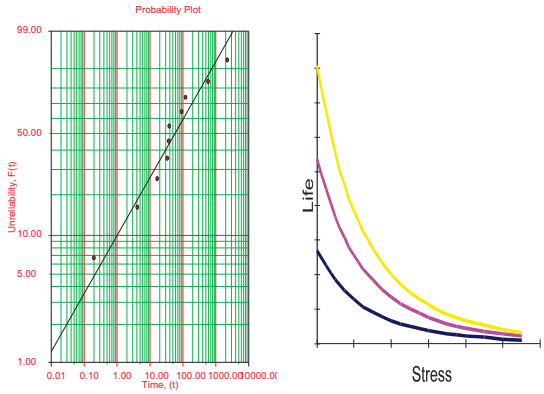


Figure 35.5. A life distribution and a life-stress relationship

The practitioner should be cautioned against using the exponential distribution, unless the underlying assumption of a constant failure rate can be justified. Along with the life distribution, a life-stress relationship is also used. A life-stress relationship can be one of the empirically derived relationships or a new one formulated for the particular stress and application. The data obtained from the experiment is then fitted to both the underlying life distribution and life-stress relationship.

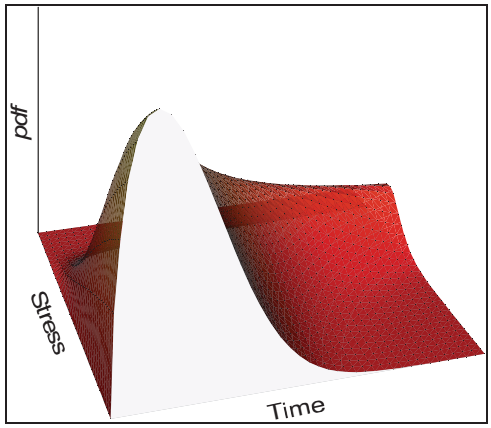


Figure 35.6. A three-dimensional representation of the pdf *vs.* time and stress created using ReliaSoft's ALTA 6.0 software [7]

35.4.1 Overview of the Analysis Steps

35.4.1.1 Life Distribution

The first step in performing an accelerated life test analysis is to choose an appropriate life distribution for your data. The commonly used distributions are the Weibull, lognormal, exponential (usually not appropriate because it assumes a constant failure rate) distributions.

35.4.1.2 Life-Stress Relationship

The second step is to select (or create) a model that describes a characteristic point or a life characteristic of the distribution from one stress level to another (*i.e.,* the life characteristic is expressed as a function of stress). The life characteristic can be any life measure such as the mean, median, *etc*. Depending on the assumed underlying life distribution, different life characteristic are considered. Typical life characteristics for some distributions are shown in Table 35.1

For example, when considering the Weibull distribution, the scale parameter, η, is chosen to be the "life characteristic" that is stress-dependent, while β is assumed to remain constant across different stress levels. A life-stress relationship is then assigned to η. The assumption that β remains constant across different stress levels implies that the same failure mechanism is observed at different stresses. The objective of accelerated testing is to make the studied failure mode occur faster so as not to introduce new failure modes that do not normally occur in normal condition. For thisreason, β is assumed to remain constant across different stress levels. The same reasoning is applied on the assumption that σ is constant when the lognormal distribution is used.

Table 35.1. Typical life characteristics

Distribution	Parameters	Life characteristic
Weibull	β*, η	H
Exponential	Λ	Mean life = 1/ λ
Lognormal	$\overline{T}$, σ*	Median: $\breve{T}$

**Usually assumed independent of the stress level*

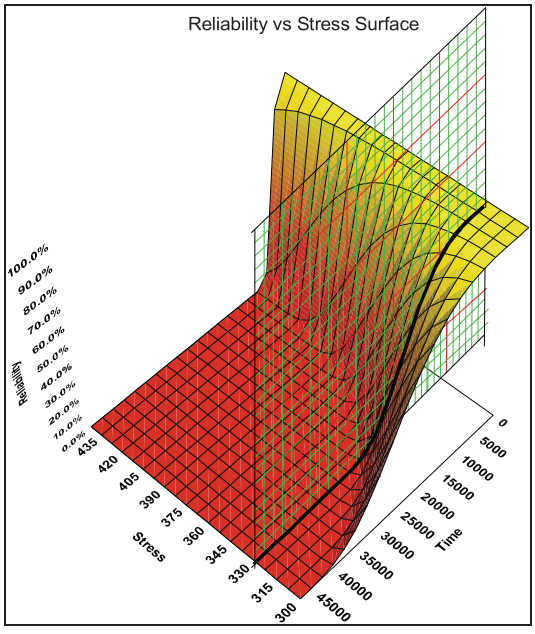


Figure 35.7. A graphical representation of a Weibull reliability function plotted as both a function of time and stress

There are many life-stress models, including:

- The Arrhenius relationship.
- The Eyring relationship.
- The inverse power law relationship.
- The temperature–humidity relationship.
- The temperature–non-thermal relationship.

These models will be discussed in more detail later in this chapter.

The data obtained from the experiment is then fitted to both the underlying life distribution and the life-stress relationship. The combination of both an underlying life distribution and a life-stress model can be best seen in Figure 35.6 where a pdf is plotted against both time and stress. Reliability is also dependent on time and stress as shown in Figure 35.7.

35.5 Parameter Estimation

The next step is to estimate the parameters of the combined model based on the selected life distribution and life-stress relationship that best fit the accelerated test data. The task of parameter estimation can vary from trivial (with ample data, a single constant stress, a simple distribution, and a simple model) to impossible. Available methods for estimating the parameters of a model include the graphical method, the least squares method, and the maximum likelihood estimation (MLE) method. MLE is typically the more appropriate method because its properties are desired in accelerated life test analysis. Computer software can be used to accomplish this task [1, 5, 7].

35.6 Stress Loading

Different types of loads can be considered when an accelerated test is performed. Accelerated life tests can be classified as constant stress, step stress, cycling stress, or random stress. These types of loads are classified according to the dependency of the stress with respect to time.

There are two possible stress loading schemes: loadings in which the stress is time-independent and loadings in which the stress is time-dependent. The mathematical treatment varies depending on the relationship of stress to time.

35.6.1 Time-independent (Constant) Stress

When the stress is time-independent, the stress applied to a sample of units does not vary. In other words, if temperature is the thermal stress, each unit is tested under the same accelerated temperature, *e.g.*, 100°C, and data are recorded (Figure 35.8).

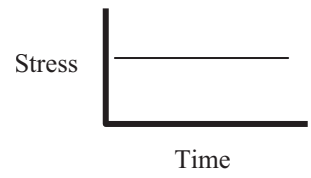


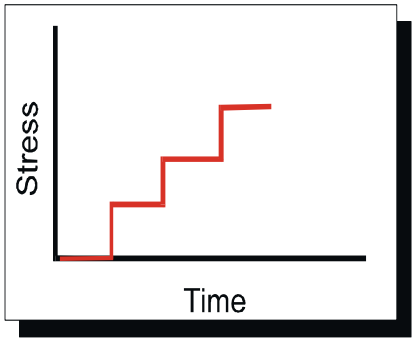
Figure 35.8. Time-independent stress loading

Constant stress loading has many advantages over time-dependent stress loadings. Specifically:

- Most products are assumed to operate at a constant stress under normal use.
- It is far easier to run a constant stress test (*e.g.*, one in which the chamber is maintained at a single temperature).
- It is far easier to quantify a constant stress test.
- Models for data analysis exist, are widely publicized, and are empirically verified.
- Extrapolation from a well executed constant stress test is more accurate than extrapolation from a time-dependent stress test.
- Smaller test sample sizes are required (compared to time-dependent tests).

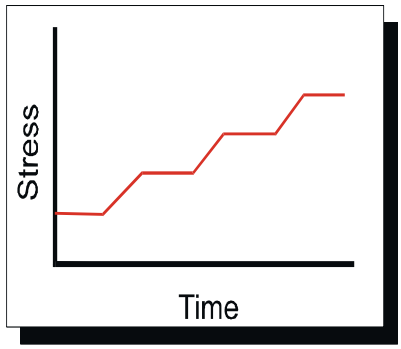
35.6.2 Time-dependent Stress

When the stress is time-dependent, the product is subjected to a stress level that varies with time (Figures 35.9, 35.10 and 35.11). Products subjected to time-dependent stress loadings will yield failures more quickly and models that fit them are thought by many to be the "holy grail" of accelerated life testing. For more details about analysis of time-dependent accelerated testing, the reader is referred to [6]. Analyses of time-dependent stress models are more complex models and require advanced software packages [1].



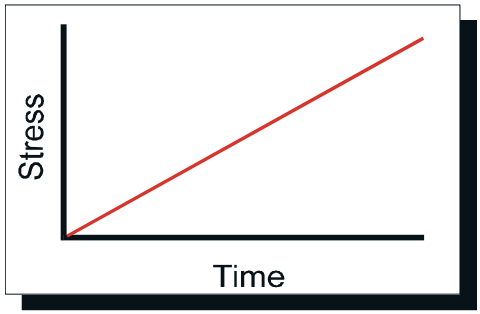
A- Step-stress model

Figure 35.9. Quasi time-dependent models

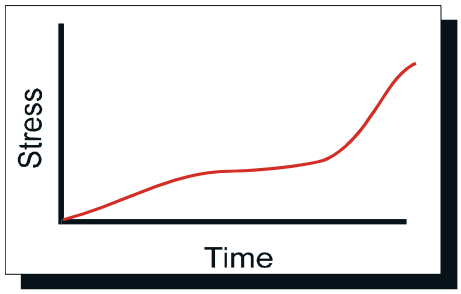


B- Ramp-stress model

Figure 35.10. Quasi time-dependent models



A- Constantly increasing stress model.



B- Completely time-dependent stress model.

Figure 35.11. Continuously time-dependent stress models

35.7 An Introduction to the Arrhenius Relationship

One of the most commonly used life-stress relationships is the Arrhenius model. It is an

exponential relationship and was formulated by assuming that life η is proportional to the inverse reaction rate of the process. Thus the Arrhenius life-stress relationship is given by (35.1).

$$L(V) = C \cdot e^{\frac{B}{V}}, \qquad (35.1)$$

where:

- L represents a quantifiable life measure, such as mean life, characteristic life, median life, or BX life, *etc*.
- V represents the stress level (formulated for temperature and temperature values in absolute units *i.e.*, degrees Kelvin or degrees Rankine. This is a requirement because the model is exponential, thus negative stress values are not possible).
- C and B are model parameters to be determined ($C > 0$).

Since the Arrhenius relationship is a physics-based model derived for temperature dependence, it is strongly recommended that the model be used for temperature-accelerated tests. For the same reason, temperature values must be in absolute units (Kelvin or Rankine), even though (35.1) is unitless.

The Arrhenius relationship can be linearized and plotted on a life *vs.* stress plot by taking the natural logarithm of both sides in (35.1), which leads to (35.2),

$$\ln\left(L(V)\right) = \ln(C) + \frac{B}{V}. \qquad (35.2)$$

Note that the inverse of the stress, and not the stress, is the variable. In Figure 35.12, life is plotted versus stress and not versus the inverse stress. The shaded areas shown in Figure 35.12 are the imposed pdf's at each test stress level. From such imposed pdf's one can see the range of the life at each test stress level, as well as the scatter in life.

The points shown in these plots represent the life characteristics at the test stress levels (the data were fitted to a Weibull distribution, thus the points represent the scale parameter, η).

Depending on the application (and when the stress is exclusively thermal), the parameter B can be replaced by (35.3),

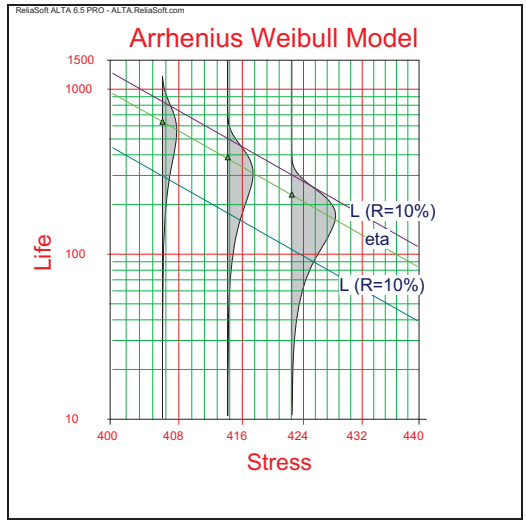


Figure 35.12. The Arrhenius relationship linearized on log-reciprocal paper

$$B = \frac{E_A}{K} = \frac{\text{activation energy}}{\text{Boltzman's constant}} = \frac{\text{activation energy}}{8.623\times10^{-5}\,\text{eV}\cdot\text{K}^{-1}} \qquad (35.3)$$

Note that in this formulation, the activation energy must be known *a priori*. If the activation energy is known then there is only one model parameter remaining, C. Because in most real life situations this is rarely the case, all subsequent formulations will assume that this activation energy is unknown

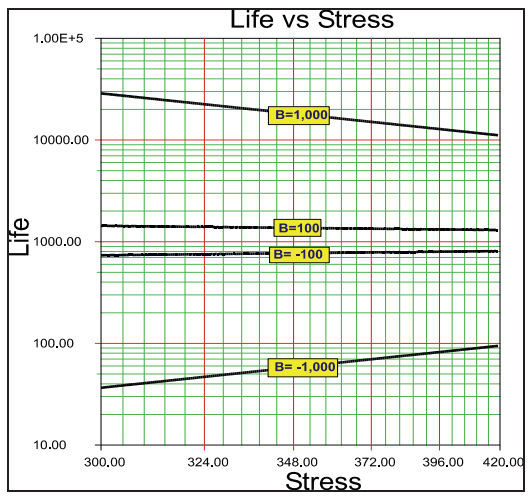


Figure 35.13. Behavior of the parameter B

and treat B as one of the model parameters. B is a measure of the effect that the stress has on the life. The larger the value of B, the higher the dependency of the life on the specific stress. B may also take negative values (*i.e.*, life is increasing with increasing stress), see Figure 35.12. An example of this would be plasma filled bulbs that last longer at higher temperatures.

35.7.1 Acceleration Factor

Most practitioners use the term acceleration factor to refer to the ratio of the life (or acceleration characteristic) between the use level and a higher test stress level or as shown in (35.4).

$$A_F = \frac{L_{Use}}{L_{Accelerated}}. \qquad (35.4)$$

For the Arrhenius model this factor is shown in (35.5),

$$A_F = \frac{L_{USE}}{L_{Accelerated}} = \frac{C \cdot e^{\frac{B}{V_u}}}{C \cdot e^{\frac{B}{V_A}}} = \frac{e^{\frac{B}{V_u}}}{e^{\frac{B}{V_A}}} = e^{\left(\frac{B}{V_u} - \frac{B}{V_A}\right)}. \qquad (35.5)$$

If B is assumed to be known *a priori* (using an activation energy), the assumed activation energy alone dictates this acceleration factor!

35.7.2 Arrhenius Relationship Combined with a Life Distribution

All relationships presented must be combined with an underlying life distribution for analysis.

We illustrate the procedure for combining the Arrhenius relationship with an underlying life distribution, using the Weibull distribution. The two-parameter Weibull distribution equation is shown in (35.6),

$$f(t) = \frac{\beta}{\eta} \cdot \left(\frac{t}{\eta}\right)^{\beta - 1} e^{-\left(\frac{t}{\eta}\right)^{\beta}} \qquad (35.6)$$

The Arrhenius–Weibull model pdf can be obtained by setting $\eta = L(V)$ in (35.7) to (35.8),

$$\eta = L(V) = C \cdot e^{\frac{B}{V}}. \qquad (35.7)$$

Substituting for η in (35.7), we get the Arrhenius–Weibull model in (35.8),

$$f(t,V) = \frac{\beta}{C \cdot e^{\frac{B}{V}}} \cdot \left(\frac{t}{C \cdot e^{\frac{B}{V}}}\right)^{\beta - 1} e^{-\left\{\frac{t}{C \cdot e^{\frac{B}{V}}}\right\}^{\beta}} \qquad (35.8)$$

An illustration of the pdf for different stresses is shown in Figure 35.14. Figure 35.15 illustrates the behavior of the reliability function at different stress levels.

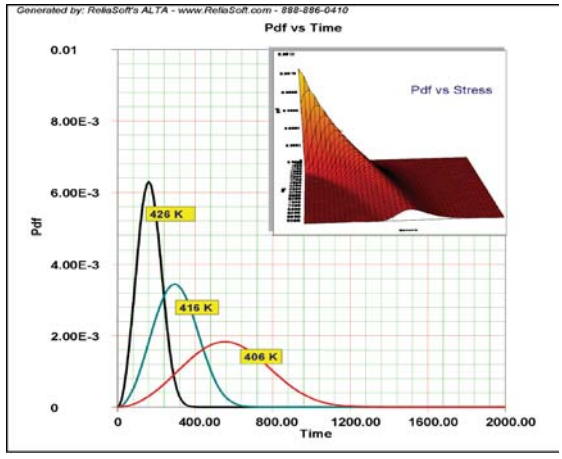


Figure 35.14. Probability density function at different stresses and with the parameters held constant

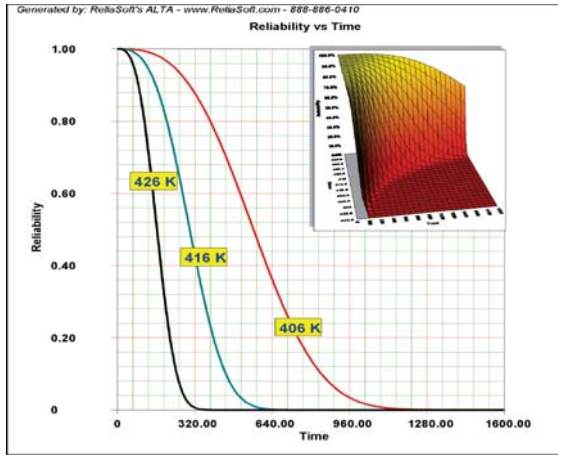


Figure 35.15. Reliability function at different stresses and with the parameters held constant

The following equations ((35.9)–(35.11)) are a summary of the Arrhenius model combined with some common distributions.

Arrhenius–Weibull

$$f(t,V) = \frac{\beta}{C \cdot e^{\frac{B}{V}}} \cdot \left(\frac{t}{C \cdot e^{\frac{B}{V}}} \right)^{\beta-1} e^{-\left(\frac{t}{C \cdot e^{\frac{B}{V}}} \right)^{\beta}} \tag{35.9}$$

Arrhenius–lognormal

$$f(t,V) = \frac{1}{T' \cdot \sigma_{T'} \sqrt{2\pi}} \cdot e^{-\frac{1}{2}\left(\frac{T' - \bar{T}'}{\sigma_{T'}} \right)^2} \tag{35.10}$$

Arrhenius–exponential

$$f(t,V) = \frac{1}{C \cdot e^{\frac{B}{V}}} \cdot e^{-\frac{1}{C \cdot e^{\frac{B}{V}}} \cdot t} \tag{35.11}$$

Once the pdf has been obtained, all other metrics of interest *(i.e.*, reliability, MTTF, *etc.*) can be easily formulated. For more information, see [1 , 5].

35.7.2.1 Example

Consider the following times-to-failure data at three different stress levels.

Table 35.2. Times-to-failure data at three different stress levels

Stress	393 K	408 K	423 K
Time Failed (hrs)	3850	3300	2750
	4340	3720	3100
	4760	4080	3400
	5320	4560	3800
	5740	4920	4100
	6160	5280	4400
	6580	5640	4700
	7140	6120	5100
	7980	6840	5700
	8960	7680	6400

The data were analyzed jointly and with a complete MLE solution over the entire data set, using [7]. The analysis yields.

$$\hat{\beta} = 4.291,\ \hat{B} = 1861.618,\ \hat{C} = 58.984 \cdot$$

Once the parameters of the model are estimated, extrapolation and other life measures can be directly obtained using the appropriate equations. Using the MLE method, confidence bounds for all estimates can be obtained.

35.7.3 Other Single Constant Stress Models

Similarly to the approach described in Section 35.6.2, combining the distribution and the life-stress relation in one model is done by substituting the appropriate life characteristic (as indicated in Table 35.1) of the distribution with the life-stress relationship. Equations (35.12)–(35.17) summarize some of the most common life-stress/life distribution models.

Eyring–Weibull

$$f(t,V) = \beta V^{n} \cdot e^{\left(A - \frac{B}{V}\right)} \cdot \left(t V^{n} \cdot e^{\left(A - \frac{B}{V}\right)} \right)^{\beta-1} e^{-\left(t V^{n} \cdot e^{\left(A - \frac{B}{V}\right)} \right)^{\beta}} \tag{35.12}$$

Eyring–lognormal

$$f(t,V) = \frac{1}{T' \cdot \sigma_{T'} \sqrt{2\pi}} \cdot e^{-\frac{1}{2}\left(\frac{T' + \ln(V^{n}) + A - \frac{B}{V}}{\sigma_{T'}} \right)^2} \tag{35.13}$$

Eyring–exponential

$$f(t,V) = V^{n} \cdot e^{\left(A - \frac{B}{V}\right)} \cdot e^{-V^{n} \cdot e^{\left(A - \frac{B}{V}\right)} \cdot t} \tag{35.14}$$

IPL–Weibull

$$f(t,V) = \beta K V^{n} \left(K V^{n} t \right)^{\beta-1} \cdot e^{-\left(K V^{n} t \right)^{\beta}} \tag{35.15}$$

IPL–lognormal

$$f(t,V) = \frac{1}{T \cdot \sigma_{T'} \sqrt{2\pi}} \cdot e^{-\frac{1}{2}\left(\frac{T' + \ln(K) + n\ln(V)}{\sigma_{T'}}\right)^2} \tag{35.16}$$

IPL–exponential

$$f(t,V) = K V^n e^{-K V^n t} \tag{35.17}$$

One must be cautious in selecting a model. The physical characteristics of the failure mode under consideration must be understood and the selected model must be appropriate. As an example, in cases where the failure mode is fatigue, the use of an exponential relationship would be inappropriate since the physical mechanism are based on a power relation (*i.e.*, the inverse power law model is more appropriate).

35.8 An Introduction to Two-stress Models

35.8.1 Temperature–Humidity Relationship-Introduction

The temperature–humidity (T–H) relationship has been proposed for predicting the life at use conditions when temperature and humidity are the accelerated stresses in a test. This combination model is given by (35.18),

$$L(U,V) = A \cdot e^{\left\{\frac{\phi}{V} + \frac{b}{U}\right\}}, \tag{35.18}$$

where,

- Φ, b and A are three parameters to be determined. b is also known as the activation energy for humidity;
- U is the relative humidity (decimal or percentage); and
- V is temperature (in absolute units)

Since life is now a function of two stresses, a life vs. stress plot can only be obtained by keeping one of the two stresses constant and varying the other one.

When using the T–H relationship, the effect of both temperature and humidity on life is sought. Therefore, the test must be performed in a combination manner between the different stress levels of the two stress types. For example, assume that an accelerated test is to be performed at two temperature and two humidity levels, then the test should be performed at three out of the four possible combinations in order to be able to determine the effect of each stress type.

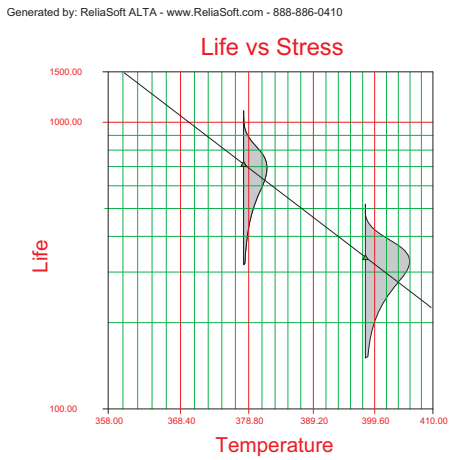


Figure 35.16(a). Life *vs*. stress plots for the temperature-humidity model, holding humidity constant

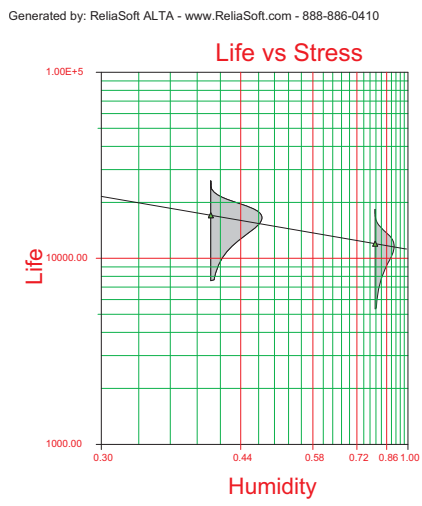


Figure 35.16(b). Life *vs.* stress plots for the temperature-humidity model, holding temperature constant

35.8.1.1 An Example Using the T–H Model

The data in Table 35.3 were collected after testing twelve electronic devices at different temperature and humidity conditions.

Table 35.3. T–H data

Time, hr	Temperature, K	Humidity
310	378	0.4
316	378	0.4
329	378	0.4
411	378	0.4
190	378	0.8
208	378	0.8
230	378	0.8
298	378	0.8
108	398	0.4
123	398	0.4
166	398	0.4
200	398	0.4

Using [7], the following results were obtained assuming a Weibull distribution and using the T–H life stress model:

$$\hat{\beta}=5.874,\ \hat{A}=0.0000597,\ \hat{b}=0.281,\ \hat{\phi}=5630.330.$$

Figure 35.16 shows the effect of temperature and humidity on the life of the electronic devices.

35.8.2 Temperature–Non-thermal Relationship Introduction

When temperature and a second non-thermal stress (*e.g.*, voltage) are the accelerated stresses of a test, then the Arrhenius and the inverse power law models can be combined to yield the temperature–non-thermal (T–NT) model. This model is given by (35.19),

$$L(U,V)=\frac{C}{U^{n}e^{-\frac{B}{V}}}, \qquad (35.19)$$

Where:

- U is the non-thermal stress (*i.e.*, voltage, vibration, *etc.*);
- V is the temperature (in absolute units); and
- B, C and n are parameters to be determined.

In Figure 35.17, data obtained from a temperature and voltage test were analyzed and plotted on a log-reciprocal scale.

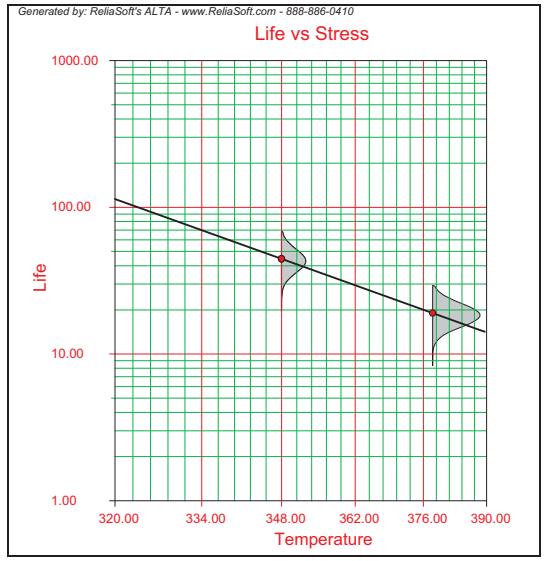


Figure 35.17(a). Life *vs.* stress plots for the temperature–non-thermal model, holding voltage constant

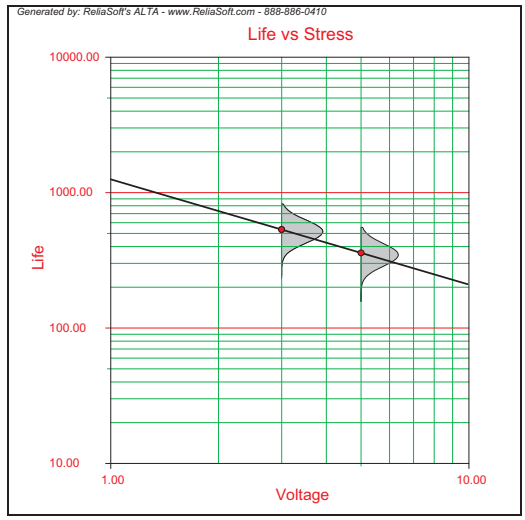


Figure 35.17(b). Life *vs.* stress plots for the temperature–non-thermal model, holding temperature constant

35.9 Advanced Concepts

35.9.1 Confidence Bounds

The confidence bounds on the parameters and a number of other quantities such as the reliability and the percentile can be obtained based on the asymptotic theory for maximum likelihood estimates, for complete and censored data. This type of confidence bounds is most commonly referred to as the Fisher matrix bounds. For more details about analysis in time-dependent accelerated testing analysis, the reader is referred to [6].

35.9.2 Multivariable Relationships and the General Log-linear Model

So far in this chapter the life-stress relationships presented have been either single stress relationships or two stress relationships. In most practical applications however, life is a function of more than one or two variables (stress types).

In addition, there are many applications where the life of a product as a function of stress and of some engineering variable other than stress is sought. A multivariable relationship called the general log-linear relationship, which describes a life characteristic as a function of a vector of n stresses is used. Mathematically the general log-linear (GLL) model is given by (35.20),

$$L\left(\underline{X}\right) = e^{\left(a_0 + \sum_{i=1}^{n} a_i X_i\right)}, \qquad (35.20)$$

Where:

- a_0 and a_j are model parameters,
- $\underline{X}$ is a vector of n stresses, And
- X_n are the levels of the n stresses.

This relationship can be further modified through the use of transformations. As an example, a reciprocal transformation on X, or $X=1/V$ will result in an exponential life stress relationship (for example, thermal factors), while a logarithmic transformation, $X=\ln(V)$, results in a power life stress relationship (for example, non-thermal factors.) Note that the Arrhenius, the inverse power law, the temperature–humidity and temperature–non-thermal relationships are all special cases of the GLL model.

Like the previous models, the general log-linear model can be combined with any of the available life distributions by expressing a life characteristic from that distribution with the GLL relationship.

35.9.2.1 Example

Consider the data summarized in Table 35.4 and Table 35.5.

Table 35.4. Stress profile summary

Profile	Temp (K)	Voltage (V)	Operation Type
A	358	12	On/Off
B	358	12	Continuous
C	378	12	On/Off
D	378	12	Continuous
E	378	16	On/Off
F	378	16	Continuous
G	398	12	On/Off
H	398	12	Continuous

Table 35.5. Failure data

Profile	Failure Time / Suspensions
A	498, 750
B	445, 586, 691 20 units suspended at 750
C	176, 252, 309, 398
D	211, 266, 298, 343, 364, 387 14 units suspended at 445
E	118, 163, 210, 249
F	145, 192, 208, 231, 254, 293 10 units suspended at 300
G	87, 112, 134, 163
H	116, 149, 155, 173, 193, 214 7 units suspended at 228

The data of Table 35.5 is analyzed assuming a Weibull distribution, an Arrhenius life-stress relationship for temperature, and an inverse power life-stress relationship for voltage. No transformation is performed on the operation type. The operation type variable is treated as an indicator variable, using the discrete values of 0 and 1, for on/off and continuous operation, respectively.

The best fit values for the parameters are:

$\hat{\beta} = 3.7483,\ \hat{\alpha}_0 = -6.0220;\ \hat{\alpha}_1 = 5776.9341;$

$\hat{\alpha}_2 = -1.4340;\ \hat{\alpha}_3 = 0.6242$

In this case, since the life is a function of three stresses, three different plots can be created. Such plots are created by holding two of the stresses constant at the desired use level, and varying the remaining one. The use stress levels for this example are 328 K for temperature and 10 V for voltage. For the operation type, a decision has to be made by the engineers as to whether they implement on/off or continuous operation. From Figure 35.18, it can be concluded that the continuous operation has a better effect on the life of the product than the on/off cycling.

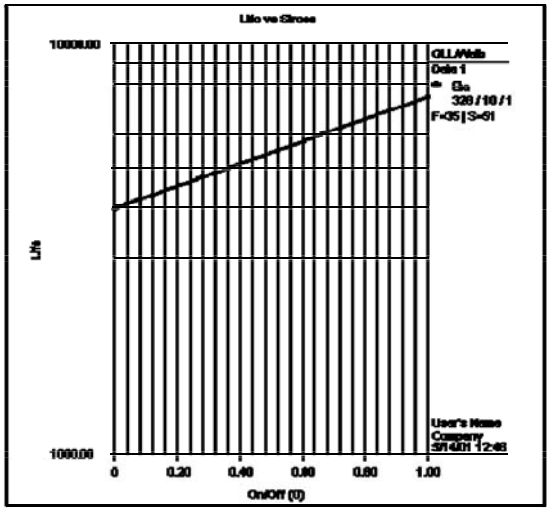


Figure 35.18. Effect of operation type on life

35.9.3 Time-varying Stress Models

When dealing with data from accelerated tests with time-varying stresses, the life-stress model must take into account the cumulative effect of the applied stresses. Such a model is commonly referred to as a "cumulative damage" or "cumulative exposure" model. Nelson [3] defines and presents the derivation and assumptions of such a model.

Time-varying stress models apply for any of the following situations:

- The test stress is time-dependent and the use stress is time-independent.
- The test stress is time-independent and the use stress is time-dependent.
- Both the test stress and the use stress are time-dependent.

We illustrate the derivation of the cumulative damage mode using the Weibull distribution as the life distribution model and the inverse power relationship as the life-stress model. Given a time-varying stress $x(t)$, the reliability function of the unit under a single stress is given by (35.21),

$$R\left(t, x\left(t\right)\right) = e^{-\left[\int_0^t \frac{1}{\eta(u)} du\right]^{\beta}}. \quad (35.21)$$

The inverse power law relationship is expressed by (35.22):

$$\eta(t) = \left(\frac{a}{x\left(t\right)}\right)^{n}. \quad (35.22)$$

Therefore, the pdf is as given in (35.23),

$$f\left(t, x\left(t\right)\right) = \beta\left(\frac{x\left(t\right)}{a}\right)^{n} \cdot \left(\int_0^t \left(\frac{x\left(t\right)}{a}\right)^{n} du\right)^{\beta-1} \cdot e^{-\left[\int_0^t \left(\frac{x\left(t\right)}{a}\right)^{n} du\right]^{\beta}} \quad (35.23)$$

The above procedure can be used with other distribution types or life-stress relationships and can be extended to analysis involving multiple stress types using the general-log linear model concept. Parameter estimation can be accomplished via maximum likelihood estimation methods and confidence intervals can be approximated using the Fisher matrix approach.

35.9.3.1 Example

12 units were tested using the time-dependent voltage profile shown in Figure 35.19.

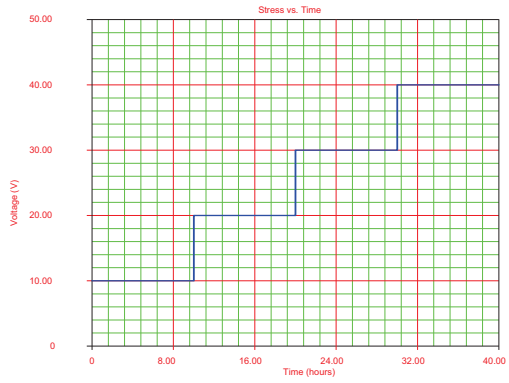


Figure 35.19. Stress profile

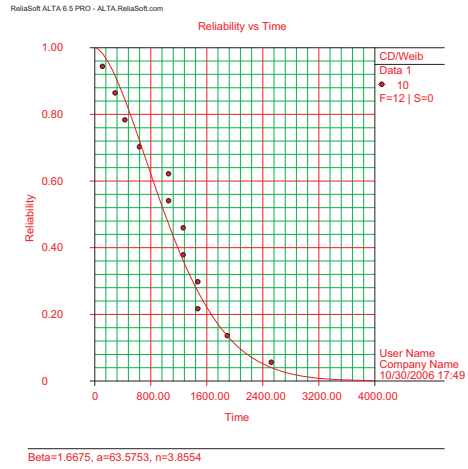


Figure 35.20. Reliability plot at use condition

The failure times (in hours) were, 17, 22, 24, 27, 31, 31, 32, 32, 33, 33, 35 and 38.

Assuming the Weibull distribution and using the power life-stress model and MLE as the analysis method, we use [7] to obtain the reliability plot in Figure 35.20 at the normal use condition of 10 V.

References

[1] Dimitri Kececioglu, Feng-Bin Sun. Environmental stress screening – Its quantification, optimization and management. Prentice Hall, Englewood Cliffs, NJ, 1995.

[2] Dimitri Kececioglu, Feng-Bin Sun. Burn-in testing – Its quantification and optimization. Prentice Hall, Englewood Cliffs, NJ, 1997.

[3] Wayne Nelson. Accelerated testing: Statistical models, test plans, and data analyses. Wiley, New York, 1990.

[4] ReliaSoft Corporation. Life data analysis reference, ReliaSoft Publishing, Tucson, AZ, 2000. Parts are also published on-line at www.Weibull.com.

[5] ReliaSoft Corporation. Accelerated life testing reference, ReliaSoft Publishing, Tucson, AZ, 1998. Also published on-line at www.Weibull.com.

[6] ReliaSoft Corporation, ALTA 6 accelerated life testing reference, ReliaSoft Publishing, Tucson, AZ, 2001.

[7] ReliaSoft Corporation, ALTA 6.0 software package, Tucson, AZ, www.ReliaSoft.com.

36

HALT and HASS Overview: The New Quality and Reliability Paradigm

Gregg K. Hobbs

Hobbs Engineering, 4300 W 100th Ave., Westminster, CO 80031, USA

The following quote reminds me of my struggles to introduce the new paradigms in the mid-1960s through enthusiastic acceptance in the late 1990s.

"Every truth passes through three stages before it is recognized.
In the first, it is ridiculed,
In the second, it is opposed,
In the third, it is recognized as self-evident." - 19th century German philosopher, Aurther Schopenhauer.

Abstract: Highly accelerated life tests (HALT) and highly accelerated stress screens (HASS) are introduced and discussed in this chapter. A few successes from each technique are described. These techniques have been successfully used by the author, and some of the author's consulting clients and seminar attendees for more than 38 years. Most of the accomplished users do not publish their results because of the pronounced financial and technical advantages of the techniques over the classical methods, which are not even in the same league in terms of speed and cost. It is important to note that the methods are still evolving as is the equipment required in order to implement the techniques. This chapter is an overview of the methods and also gives a partial chronology of their development. Full details are available in [1] and [2].

36.1 Introduction

The HALT and HASS methods are designed to improve the reliability of products, not to determine what the reliability is. The approach is therefore proactive as compared to a rel-demo (reliability demonstration) or MTBF tests that do not improve the product at all but simply (attempt to) measure what the reliability of the current design and fabrication is. This is a major difference between the classical and the HALT approaches. HALT is discovery testing whereas MIL-SPEC testing is compliance testing. These are two totally different paradigms and the differences should be completely clear to anyone attempting to perform either one. In HALT, every attempt is made to find the weak links and then fix them so that the problems will never occur again. In compliance testing, one simply attempts to satisfy all design testing requirements in order to obtain customer acceptance of the design, usually resulting in a very marginal if not completely inadequate design.

In compliance testing, overstress testing is definitely not used as it would expose weak links, which are not desired to be exposed; that is, the goal is to pass regardless of any design flaws, fabrication flaws or any other things that would prevent successful operation in the field. If failures occur, every attempt is made to discount the failure by whatever means that seem plausible so that customer acceptance will be obtained. The author started his technical life in the MIL-SPEC arena and so knows it all too well, although I must admit to having some guilty thoughts about the methods at that time. But, in the compliance arena, one must comply with the contract or payment is not forthcoming. Doing too much may actually reduce the payments, as faults could be discovered and delay certification and or payment.

HALT is performed during the design stages to eliminate design weaknesses and HASS is performed during the production stages to eliminate process problems. Therefore, HALT is basically a design tool and HASS is basically a process control tool. No matter where we find problems, it is always beneficial to take corrective action.

36.2 The Two Forms of HALT Currently in Use

It is appropriate to briefly discuss the two forms of HALT currently in use. Classical HALT uses one stress at a time with the product fully monitored with high coverage and also with good resolution. The stresses to be used are all of the field stresses plus any that could contribute to relevant flaw discovery by the Cross Over Effect™. The usual way to proceed is to expose the product to sequentially increased stresses such as:

36.2.1 Classical HALT™ Stress Application Sequence

- Apply monitoring with high coverage.
- Low temperature.
- High temperature.
- Voltage and frequency margining.
- All axis vibration (three linear axes and three angular axes, all broadband random and of appropriate spectra).
- Other stresses as appropriate for the product.
- Combine stresses a few at a time, then all at once.
- Modulated Excitaiton™ for detection of anything missed so far.
- Improve any weaknesses found if they will reduce field reliability or increase the cost of HASS.
- Do it all over again until an appropriately robust level is reached.

The above sequence is not the only one which could work, it is just the first one that I used and it works well, so why change it?

36.2.2 Rapid HALT™ Stress Application Scheme

- Apply monitoring with high coverage.
- Apply all stresses simultaneously in step-wise fashion.
- Modulated Excitation™ for detection of anything missed so far.
- Improve any weaknesses found if they will reduce field reliability or increase the cost of HASS.
- Do it all over again until an appropriately robust level is reached.

Both schemes require high coverage and resolution in order to be the least bit effective. That is, both high coverage and resolution are necessary in order to detect and then fix any problems that may have surfaced.

I have successfully used Rapid HALT™ since 1969 in my consulting roles, but only started to teach it in 2000 because the paradigm jump required to even perform Classical HALT was barely possible with most seminar attendees up until about 2000. I thought that it would be better to wait until the Classical HALT was widely accepted before attempting to teach the next quantum jump to Rapid HALT. By the way, Rapid HALT is not suggested for beginners, as it is likely

that many design flaws will be precipitated nearly simultaneously and trouble shooting will be extremely difficult to perform. Later, when the designers have learned the many lessons to be learned from a good HALT program, Rapid HALT will probably not precipitate several failures simultaneously because there will probably not be many design flaws present. Rapid HALT saves substantial time in precipitation of defects, but the "fix it time" which is the time required to determine the root cause of the problem and then to implement a fix, remains the same.

A major mistake that is observed today is that some of those attempting HALT will step stress until something is observed and then to just stop there and say "I did HALT!" Others step stress until the operational limits and/or destruct limits in temperature and vibration (only) are found and then just stop. These approaches are not HALT at all and are completely useless, maybe less than useless as they give the impression of accomplishing something when indeed they have not. The improvements are what HALT is all about. If there are no improvements, then there will be no gain.

HALT is an acronym for highly accelerated life test, which was coined by the author in 1988 after having used the term "design ruggedization" for several years. In HALT, every stimulus of potential value is used at accelerated test conditions during the design phase of a product in order to find the weak links in the design and fabrication processes very rapidly. Each weak link found provides an opportunity to improve the design or the processes which will lead to reduced design time, increased reliability and decreased costs. HALT compresses the design time and therefore allows earlier (mature) product introduction. Studies have shown that a six-month advantage in product introduction can result in a lifetime profit increase of 50% [3]. HALT may well accomplish such an earlier release to production.

The stresses applied in HALT and HASS are not meant to simulate the field environments at all, but are meant to expose the weak links in the design and processes using only a few units and in a very short period of time. The stresses are stepped up to well beyond the expected field environments until the "fundamental limit of the technology" [1, 2] is reached in robustness. Reaching the fundamental limit generally requires improving everything relevant found even if found at above the "qualification" levels! This means that one ruggedizes the product as much as possible without unduly spending money (which is sometimes called "gold plating"). Only those failures that are likely to occur in normal environments or ones that would increase the costs of HASS are addressed. One could easily overdo the situation and make the product much more rugged than necessary and spend unnecessary money and time in the process. Intelligence, technical skills and experience must all be used and a specification approach is totally incorrect in this technique. I believe that anyone who purports to have a "HALT specification" simply does not comprehend what the methods are all about. Most of the weaknesses found in HALT are simple in nature and inexpensive to fix; such as:

1. A capacitor which flew off of the board during vibration can be bonded to the board or moved to a node of the mode causing the problem, or
2. a particular component which is found to have a less than optimum value can be changed in value, or
3. an identified weak link component can be replaced with a more robust one, or
4. a screw which backs out during vibration and thermal cycling can be held in place with a thread locker of some kind.

There are many more examples in [1, 2]. The above were just illustrative.

HALT, or its predecessor, ruggedized design, has, on many occasions provided substantial (50 to 1000 times, and in a few cases, even higher) reductions in field failures, time to market, warranty expenses, design and sustaining engineering time and cost and also total development costs. One of the main benefits of HALT is that it minimizes the sample size necessary for HALT—a few will do. After a correct HALT program, the design will usually sail through DVT or Qual without any problems. The basic philosophy of HALT has been in use for many years and has been used by the author and others on many products from various fields. Some of these fields are listed in Table 36.1.

Many others exist, but cannot be mentioned due to non-disclosure agreements. Most of these companies have not published at all about their HALT successes.

Some attendees at the author's seminars have, in addition, used the techniques on thousands of products, so the *basic* methods are not new, but have not been publicized much until recently because of the tremendous advantages in reliability and cost gained by their use. The techniques continue to be improved and, in 1991, the author introduced precipitation and detection screens, decreasing screen cost by at least an order of magnitude and simultaneously increasing the effectiveness by several orders of magnitude. A precipitation screen uses screens well above the in-use levels in order to gain time compression and a detection screen attempts to find the patent or detectable defects in order to .determine the conditions under which an intermittent will be exposed. It is noted in passing that many soft failures are only detectable under a limited set of conditions. The industry average seems to be that over 50% of the defects cannot be detected on the test bench. Hence, the vast number of "cannot duplicate", "cannot verify", "no defect found" situations in the industries. Detection screens would expose most of these, saving lots of time and money for the customer and the manufacturer.

In 1996, the author introduced the concept of a search pattern which makes the detection of precipitated defects better by *at least* one order of magnitude, if not many orders of magnitude. This concept is called Modulated Excitation™. Briefly explained, it is a search pattern in the two space of temperature and vibration (or any other set of stresses such as voltage and frequency) for the combination wherein an intermittent will be observable and can then be fixed. Many flaws are only detectable within a narrow band of a combination of stresses and so trouble shooting must be accomplished in the chamber at temperature and at vibration. This is one fact that makes farming out HALT less than completely satisfactory.

Software HALT™ was introduced in 1998. In this software development technique, one exposes lack of coverage in the test hardware/software system by inserting faults intentionally, finding lack of coverage situations and then improving the test coverage. The results of Software HALT are currently being held as company private by the users and the author has seen only one publication on it through non-disclosure agreements with consulting clients. Paybacks measured in a few days are common in Software HALT, that is, the total cost of purchasing the test equipment and running the tests is recovered in a few days. The test equipment is then available for another series of tests and can again achieve a similar payback. This payback, assuming a two week payback, could be accomplished 26 times in one year on this one piece of equipment. Without compounding the rate of return, the simple rate of return is 2,600% per year! Reasons such as this are why the few leaders will not publish their results and give their competition the information necessary for them to start using the same techniques! Equipment to accomplish the methods is available [4].

HASS is an acronym for highly accelerated stress screens, which was also coined by the author in 1988 after using the term "enhanced ESS" for some years. These screens use the highest possible stresses (frequently well beyond the "QUAL" level) in order to attain time compression in the screens. Note that many stimuli exhibit an exponential relationship between stress level and "damage" done resulting in a much shorter duration of stress (if the correct stress is used). It has been proven that HASS generates extremely large savings in screening costs as much less equipment such as shakers, chambers, consumables (power and liquid nitrogen), monitoring systems and floor space are required due to time compression in the screens. The time compression is gained in a precipitation screen which utilizes stresses far above the field operational stresses. Enhanced detection is obtained in detection screens which are usually above the field stress levels if possible to enhance detection. Additionally, Modulated Excitation™ is used to improve detection. The screens must be, and are proven to be, of acceptable fatigue damage accumulation or lifetime degradation using Safety of HASS™ techniques. Safety of HASS demonstrates that repeated screening does not degrade the field performance of the unit under test and is a crucial part of HASS development. Safety of HASS, sometimes called SOS or safety of screen, is used as the term of choice as the author likes the connotation of a lifeboat.

HASS is generally not possible unless a comprehensive HALT has been performed as the margins would be too small to allow the overstress conditions required for time compression. Without HALT, fundamental design limitations would restrict the acceptable stress levels in production screens to a very large degree and will prevent the large accelerations of flaw precipitation, or time compression, which are possible with a very robust product. A less than robust product probably cannot be effectively screened by the "classical" screens without a substantial reduction in its field life.

It is only necessary that the products retain sufficient life in them to perform adequately in the real world after repeated screens. We care how much life is left, not how much life we took out during the screens. Focusing on the life removed is counterproductive and has been mentioned at many conferences as if it were the main concern. Focusing on the life removed is a typical mistake of mammoth proportions in a HALT and HASS program.

36.3 Why Perform HALT and HASS?

The general reason to perform accelerated stress conditions in the design phases is to find and improve upon design and process weaknesses in the least amount of time and correct the source of the weaknesses before production begins. The purposes of HASS are to discover and eliminate process related problems so as to take corrective action to eliminate the source of problems as soon as possible and to reduce the number of units which have to be reworked or recalled or even replaced in the field.

Table 36.1. Saving factors

Cost of Fixing a Design Defect	Savings Factor
\$35 during design	19,712:1
\$177 before procurement	3,898:1
\$368 before production	1,875:1
\$417,000 before shipment	41:1
\$690,000 on customer sites	1:1

In 1991, Horoshi Hamada, President of Ricoh, presented a paper at the EuroPACE Quality Forum. He gave costs of fixing problems at different stages during the design or during field service. Savings factors compared to the costs of failures in the field were calculated by me and are stated as "savings factor" shown in Table 36.1.

It is readily seen that fixing a problem during design is far more cost effective than fixing it later. This is what HALT is all about.

It is generally true that robust products will exhibit much higher reliability than non-robust ones and so the ruggedization process of HALT, in which large margins are obtained, will generate products of high potential reliability. In order to achieve the potential, however, defect free hardware must be manufactured or, at least, the defects must be found and fixed before shipment. In HASS, accelerated stresses are applied in production in order to shorten the time to failure of the defective units and therefore shorten the corrective action time and the number of units built with the same flaw. Each weakness found in HALT or in HASS represents an opportunity for improvement. The author has found that the application of accelerated stressing techniques to force rapid design maturity (HALT) results in paybacks that far exceed that from production stressing (HASS). Nonetheless, production HASS is cost effective in its own right until reliability is such that a sample HASS or highly accelerated stress audit (HASA) can be put into place. The use of HASA demands excellent process control as most units will be shipped without the benefit of HASS being performed on them, and only those units in the selected sample will be screened for defects. Corrective action is tantamount here.

The stresses used in HALT and HASS include but are not restricted to all axis simultaneous vibration, high rate broad-range temperature cycling, power cycling, voltage and frequency variation, humidity, and any other stress that may expose design or process problems. No attempt is made to simulate the field environment, one only seeks to find design and process flaws by any means possible. The stresses used generally far exceed the field environments in order to gain time compression, that is, shorten the time required to find any

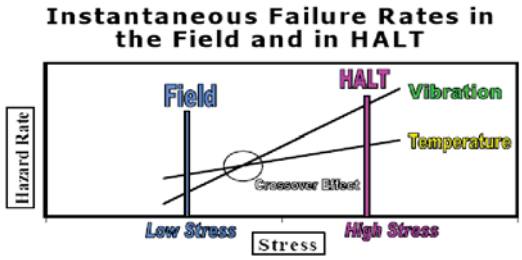


Figure 36.1. Instantaneous failure rates in the field and in HALT

problem areas. When a weakness is discovered, only the failure mode and mechanism are of importance, the relation of the stress used to the field environment is of no consequence at all. Figure 36.1 illustrates this point. In this figure, the hazard rate, λ, is the instantaneous failure rate for a given failure mode. The two curves illustrating a thermally induced failure rate and a vibration induced failure rate are located so that the field stresses at which failure occurs and the HALT stresses at which failures occur are lined up vertically for each stress. It is then seen that a failure mode that would most often be exposed by temperature in the field is likely to be exposed by vibration in the HALT environment. If one thinks of overlapping Venn diagrams in temperature and vibration, then one can see that the situation pictorially represented could occur as vibration usually occurs at hundreds of cycles per second and thermal cycles only occur at several cycles per hour in HALT. Therefore, fatigue damage occurs much more rapidly in vibration than in thermal cycling. This effect is called the Crossover Effect™ by the author. Knowledge of the crossover effect can save tremendous time and money. Many recently published papers totally miss the concept, however.

The Crossover Effect occurs frequently in HALT and HASS and should be expected. Many users who are not aware of this possibility miss this effect and, therefore, do not fix some design flaws uncovered by HALT and usually say "The product will never see that stress in the field so we do not have to fix it!" This erroneous thinking is at the root of many field failures even though the design defect was discovered in HALT, but not fixed.

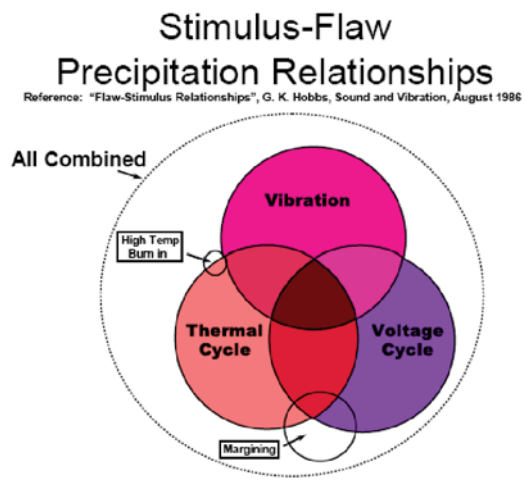


Figure 36.2. Stimulus–flaw precipitation relationship

There is another way to express the Crossover Effect and that is in Venn diagrams as shown in Figure 36.2.

Whenever the Venn diagrams overlap, then the Crossover Effect is present. It is very common to expose weaknesses in HALT with a different stress than the one that would make the weakness show up in the field. It is for this reason that one should focus on the failure mode and mechanism instead of the margin for the particular stress in use when deciding whether to fix a weakness or not.

"Mechanism" here means the conditions that caused the failure such as melting, exceeding the stable load or exceeding the ultimate strength. The corresponding failure mode could be separation of a conductor, elastic buckling and tensile failure, respectively. Considering the margin instead of the failure mode is a major mistake which is made by most engineers used to conventional test techniques, which I call "compliance" or "success" testing. In HALT and HASS, one uses extreme stresses for a very brief period of time in order to obtain time compression in the failures. In doing so, one may obtain the same failures as would occur in the field environments, but with a different stress. For example, a water sprinkler manufacturer had a weakness which was exposed by the diurnal thermal cycle in the field. HALT exposed the same weakness with all axis vibration after extensive thermal cycling failed to expose the

weakness. After the weakness was addressed, the field failures were eliminated, which proves that the weakness exposed by all axis vibration was a valid discovery. For another example, consider a reduction in cross sectional area of a conductor during forming of a bend. This reduction would create a mechanical stress concentration and an electrical current density concentration. This flaw might be exposed by temperature cycling or vibration in HALT or HASS and might also be exposed by electromigration during power cycling in HALT or HASS. Either way, flaw introduces a weakness that can be eliminated by changing the operation that introduced the reduction in area.

In addition to stresses, other parameters are used to look for weaknesses. In the author's experience, these have included the diameter of a gear, the pH of a fluid running through the product, contaminants in the fluid running through a blood analyzer, the thickness of a tape media, the viscosity of a lubricant, the size of a tube or pipe, the lateral load on a bearing, and an almost endless additional number of factors. What is sought is any information that could lead to an opportunity for improvement by decreasing the sensitivity of the product to any conditions that could lead to improper performance or to catastrophic failure. Anything that could provide information for an improvement in margin is appropriate in HALT. Accepting this philosophy is one of the most difficult shifts in thinking for many engineers not trained in the HALT/HASS approach. *Any* method for finding design and process weak links is OK.

Depending on the product and its end use environment, many "unusual" stresses could and should be used in HALT and HASS. For example, suppose that a product is to be used in a high magnetic field environment. Then strong magnetic fields should be used in HALT and maybe HASS as well. As another example, suppose that we are working on a military product that is supposed to function after a nuclear event or on a product that will reside near a CAT scanner which emits some radiation. It would be proper to expose the product to stepped up levels of radiation in order to determine if the product could successfully survive such events and then function normally. This same stress, namely radiation, would probably be nonsensical for a car radio. So, the stresses to use are tightly coupled to the real world environments considering the Crossover™ Effect.

Generally stated, one should use all field environments as well as any others that would help due to crossover effects in both HALT and HASS. This definitely is a paradigm shift from compliance testing. In addition, we use stresses far above the real world in order to attain time compression.

In the HALT phase of product development, which should be in the early design phase, the product should be improved in every way practicable bearing in mind that most of what is discovered in HALT as weaknesses will almost surely become field failures if not improved. This has been demonstrated thousands of times by users of HALT. Of course, one must always use reason in determining whether or not to improve the product when an opportunity is found and this is done by examining the failure mode and mechanism. Just because a weakness was found "out of spec" is no reason to reject the finding as an opportunity for improvement. There are numerous cases where weaknesses found "out of spec" were not addressed until field failures of the exact same type occurred. If you find it in HALT, it is probably relevant. In various papers from Hewlett-Packard over the years, it has been found that most of the weaknesses found in HALT and not addressed resulted in costs to the company in the neighborhood of $10,000,000 (in the 1990s) per failure mode to address later, when failure costs were included. It cannot be emphasized too much that it is imperative to focus on the failure mode and mechanism and not on the conditions used to make the weakness apparent. Focusing on the margin will usually lead one to allow a detected weakness to remain, resulting in many field failures of that type before a fix can be implemented. Learn from other's mistakes and do not focus on the stress type or level used, but on the failure mode and mechanism. This point is crucial to success and is frequently missed by those without sufficient knowledge of the HALT and HASS techniques.

36.3.1 An Example of the Crossover Effect

Suppose that our product contains a typical resistor, not surface mounted, but with leads on it.

Also suppose that someone has bent one lead into a very nice arc, the correct way to form the lead. However, the other end is very sharply kinked with an almost square corner on it. If we expose this defective resistor, mounted on a circuit board, to thermal cycling, it will fail at the sharp corner. One could perform extensive calculations of the fatigue damage done at the corner by the thermal cycles and differential thermal expansion in order to come to a conclusion as to whether or not to fix the shape in production, but this is hardly necessary once one sees the square corner as it is known to be a forming problem and should just be fixed with no further analysis work. Similarly, one could use vibration to precipitate a break at the square corner and then perform extensive vibration calculations to determine if the lead will break in the real service life, but, again, it is obvious that a forming problem exists and should be cured. As a last example, one could use increased current in the lead and would then obtain an electromigration induced failure at the square corner. If this lead were to be taken to the failure analysis lab, they would declare "excess current". One could then perform extensive current calculations in order to figure out how to reduce the current, including surges, so that the failure would not occur. This is all not necessary once the square corner is found as the whole problem is just a simple one of forming, nothing more difficult than that. Many failures and fixes in HALT and HASS are just as simple as discovering a poorly formed lead and taking corrective action in the forming process. It is important not make this whole thing really difficult when most of it is very simple. Some aspects, however, become complicated in terms of engineering and financial analyses. In this case, some real intellectual power is required.

36.4 A Historical Review of Screening

Many mistakes have been and currently are being made in screening and so a review of some historical events is educational in the sense that we want to go forward and learn from collective past errors. As Philosopher George Santayana said, "Those who cannot learn from history are doomed to repeat it."

In the 1970s, the U.S. Navy, which was not alone in this regard, experienced very poor field service reliability. In response to this, an investigation was performed and it was found that many of the failures were due to defects in production that could be screened out using thermal cycling and random vibration. The Navy issued a stress screening guideline, NAVMAT P-9492, which laid out guidelines for production screening on Navy programs. This document was included in most Navy contracts and so production screening became a requirement on most Navy programs. Although the document was frequently treated as a MIL-SPEC, which was not the intent, tremendous gains in reliability resulted from the techniques required by the Navy on some programs. I believe that reliability was severely compromised on many others due to precipitation without detection. Among other things, random vibration and thermal cycling were required, but were not required to be applied simultaneously. Data acquired later by many investigators would show that combined vibration and thermal cycling is more than ten times as effective as singular application of the stresses and is less expensive due to the reduction of test hardware and time. The author has found in many workshops with actual production hardware as well as on consulting assignments that no defects at all were found unless Modulated Excitation™ was used. This is fundamental to good detection.

In the late 1970s, the Institute of Environmental Sciences (IES), now the Institute of Environmental Sciences and Technology (IEST) began to have annual meetings which addressed the subject of environmental stress screening (ESS). The IES issued guidelines on the production screening of assemblies in 1981 and 1984 and on the screening of parts in 1985. There were three major problems with the survey and the published results [5, 6].

1. The companies surveyed were mostly under contract to the U.S. military and screens had been imposed by contract in many cases and had not been carefully tuned to be successful. Some had even been tuned *not* to be successful by those striving to "pass the specs". Most of the contracts issued even made it more

profitable for the contractors to produce hardware which did not have high field reliability but would pass the screens. In these cases, the contractor could sell almost everything produced; and, since the field reliability was poor, many spares were needed as was a rework facility to fix those units which failed in the field. It is readily apparent that the screens used in these types of contracts would not be the most effective screens that the technology of the day could produce. The thought process that led to the situation then still prevails today and will continue to exist until the military contractors are trained correctly in the HALT and HASS techniques and then are forced to use them, perhaps by contractual requirements regarding field failures or some other significant tests.

2. The IES polled the contractors doing screening and asked which screens were the most effective and also restricted voting to those stresses used. Since most specs required thermal cycling and many fewer required vibration, there were many more users of thermal cycling than of vibration. Therefore, when the IES then published the results as "effectiveness" of various screens instead of a more accurate term of "popularity" or "what was required to be done", it created much mis-understanding of the survey. See [7] for some details. Among the misconceptions in the guidelines was the concept that thermal cycling was the most effective screen. This misconception is present to a large extent today, however, many HALT results have shown that all axis vibration far surpasses the effectiveness of thermal cycling for the broad spectrum of faults found in many types of equipment including electronics. The last statement is only true if a six-axis shaker is used. The two stresses combined are much better than any one alone, so one should not beat the drum for vibration alone either.
3. The Guidelines emphasized 100% screening instead of emphasizing corrective action which would eventually allow the screening to be reduced to a sample. An interesting observation is that the definition of screening as a process on 100% of the production maximized the equipment, manpower and other costs! This led to a bonanza for some equipment manufacturers and for contractors working on a "cost plus fee" basis. This paradigm of incorrect and very expensive screening is firmly entrenched in the USA military manufacturers even today. This is a truly sad situation.

These three problems in the IES Guidelines led many novices to try the techniques which were relatively ineffective and inordinately expensive. With only the IES Guidelines as a source of information, many financially and technically unsuccessful screening programs were tried. Many companies simply gave up and went back to their old ways or simply complied with contractual requirements.

There was a further complication due to NAVMAT P-9492 which was issued by the Naval Material Command in June of 1979 [8]. This guideline, unfortunately, gave a vibration spectrum that was a qualification spectrum from Grumman used to qualify avionics which were hard mounted to the panel of a navy fighter aircraft. Also, unfortunately, MIL-STD 2164 gave the same spectrum as a requirement for qualification. Since this spectrum was in the MIL-STD and was in the guideline as well, it became an accepted profile by many companies all over the world. The author had warned the Navy about such an event but was ignored. Even today, the totally inappropriate vibration profile is required in many company specifications and still in some military specifications. This profile is inappropriate for several reasons:

a). It is a qualification level for a specific application and, therefore, is not an appropriate screen for other applications.
b). There is no mention of anything like Safety of Screen.

c). The vibration is only one linear axis whereas the real world is six axes, three linear and three angular.

The NAVMAT document did correctly point out that stimulation was intended, not simulation. This point seemed to be totally missed by readers, however, based on actions taken by them. Obviously, many companies had a "compliance" attitude then and some still do today.

The result of the MIL-SPEC mentality when the NAVMAT profile was applied was very ineffective and sometimes damaging at the same time using unproven screening profiles without detection. The author observed many programs wherein the NAVMAT approach was taken resulting in seriously degraded reliability as well as increased costs. Many became disgusted and simply quit trying; others generated massive field failures, sometimes upon first real use in the field. One result of the confusion was that some military (and civilian) contractors were required to build many spares for which they were paid and they were also required to repair all of those that failed in the field, for which they were also paid. This turned out to be a gold mine for many companies as the poorer their products, the better the profits. Some of these same companies today staunchly refuse to adopt the new techniques either because of ignorance or because the old method is so lucrative to them. The military created this situation themselves while all the time being advised by the author of what would happen if they proceeded on the then current path. We taxpayers are footing the bill and risk for such actions.

In the meantime, some very successful screening techniques were developed, tried, improved and retried. These techniques are so successful compared to the Guideline's methods that the most successful of the companies using the new techniques will not publish their results. Some companies are starting to publish to a limited extent but are omitting critical factors such as eliminated design flaws, warranty return rates, and returns on investments (ROIs). However, from knowledge gained in consulting under non-disclosure agreements, most of the truly outstanding successes are still not being published. Many disasters from the misapplication of HALT and HASS, almost always from incorrect training, are also not being published. The author has been called in as a consultant in many cases, many times by the customer, not the manufacturer, wherein HALT did not succeed in producing acceptable hardware. In every case, the techniques of HALT and/or HASS had not been properly applied and immediately obvious design defects were present as well. In one of those cases, the manufacturer had used HALT on one program and proceeded to produce the worst product ever made by that company! After an in-house seminar and one day of consulting, the company was on the right track and is now making some of the best-of-the-best for that industry. Unfortunately for that company, the very poor product produced early-on severely hurt the reputation of the company, and it may take decades to overcome the stigma of producing such a low reliability product. Properly applied, however, HALT and HASS always work!

Along with the technique improvements, equipment for performing the new techniques was developed. When the newer equipment was available, further technique improvements were possible. This confluence of technique and equipment improvements has been in effect for several cycles. The author sees no end to the development in sight and is currently in the development, patent, and production stages on equipment that far surpasses anything yet available for the techniques [9].

36.5 The Phenomenon Involved and Why Things Fail

HALT and HASS are not restricted to electronic boxes, but apply to many other technologies as well. Some of the technologies are listed at the end of the chapter and include such diverse products as shock absorbers, lipstick, bricks, airframes, auto bodies, exhaust systems, surgical equipment, and power steering hoses, to name just a few. Before getting into the techniques in general, it is beneficial to know the history of early attempts at stress screening that paralleled the development of HALT and HASS. Note that HALT addresses design and process weaknesses whereas classical ESS only addresses production weaknesses and then very inefficiently and perhaps even makes

things worse instead of better. HASS may expose design weaknesses if any remain or are introduced after production start.

HALT and HASS are tests aimed at discovering things incorrectly done whereas the MIL-SPEC type tests are usually performed with a view to passing; *i.e.*, compliance testing. The goals of HALT and HASS are therefore "discovery" and the MIL-SPEC tests are "compliance".

Several phenomena may be involved when screening occurs. Among these are mechanical fatigue damage, wear, electro-migration, chemical reactions as well as many others. Each of these has a different mathematical description and responds to a different stimulus or stimuli. Chemical reactions and some migration effects proceed to completion according to the Arrhenius model or some derivative of it. It is noted that many misguided screening attempts have assumed that the Arrhenius equation *always* applies; that is, that higher temperatures lead to higher failure rates, but this is not an accurate assumption. For many excellent discussions of the use and misuse of the Arrhenius concepts, one can refer to [10]. MIL-HDBK 217, a predictive methodology for electronic reliability without any scientific basis whatsoever, was based on these concepts. It is quite invalid for predicting the field reliability of the products which are built today. MIL-HDBK 217 is even less valid and completely misleading when used as a reverse engineering tool to improve reliability, as it will lead one to reduce temperatures even when a reduction will not reduce the failure rate and may even increase it due to changes made to decrease the temperature such as the addition of cooling fans. That is, new failure modes may be introduced and the basic reason for some existing failures may not be changed at all. Hakim [11] gives an excellent discussion of temperature sensitivities of many microelectronics parts which are stated to be insensitive to temperature below 150 degrees Centigrade.

If HALT and HASS are properly done, then the prediction approach has some validity as only component flaws will remain. In that case, one could use the prediction approach(es) to calculate a field reliability and then wait until field reliability numbers are available and then calculate a "fudge factor" that corrects for field usage stress intensity and mix of stresses. Then, if another product with the same mix of components were to be designed for the same field usage, the fudge factor would be correct and we could accurately estimate the field MTBF. However, by the time we have been able to calculate the fudge factor, the component mix may change, the product design may change and even the field usage environments may change. We would therefore be chasing an ever-changing fudge factor! Even this approach will, therefore, not work in the end.

Many failures in electronic equipment are mechanical in nature: the fatigue of a solder joint, the fatigue of a component lead, the fracture of a pressure bond or similar modes of failure. The mechanical fatigue damage done by mechanical stresses due to temperature, rate of change of temperature, vibration, or some combination of them can be modeled in many ways, the least complex of which is Miner's criterion. This criterion states that fatigue damage is cumulative, is non-reversible, and accumulates on a simple linear basis which in words are "The damage accumulated under each stress condition taken as a percentage of the total life expended can be summed over all stress conditions. When the sum reaches unity, the end of fatigue life has arrived and failure occurs." The data for percentage of life expended is obtained from S–N (number of cycles to fail *versus* stress level) diagrams for the material in question. A general relationship [12] based on Miner's criterion is as follows:

$$D \approx n s^{\beta},$$

where:
D is the fatigue damage accumulated, normalized to unity,
n is the number of cycles of stress,
s is the mechanical stress (in pounds per square inch, for example), and
ß is an exponent derived from the S–N diagram for the material and ranges from 8 to 12 for most materials.

Physically, it represents the negative inverse slope of the S–N diagram. David Steinberg uses ß = 3.4 for solder joints in some cases based on experience.

The flaws (design or process) that will cause field failures usually, if not almost always, will cause

a stress concentration to exist at the flaw location (and this is what causes the early failure). Just for illustrative purposes, let us assume that there is a stress which is twice as high at a particular location which is flawed due to an inclusion or void in a solder joint. According to the equation above with Beta assumed to be about 10, the fatigue damage would accumulate about 1,000 times as fast at the position with the flaw as it would at a non-flawed position having the same nominal stress level; that is, having the same applied load without the stress concentration. This means that the flawed area can fatigue and break and still leave 99.9% of the life in the non-flawed areas.

Our goal in environmental stress screening is to do fatigue damage to the point of failure at the flawed areas of the unit under test as fast as possible and for the minimum cost. With the proper application of HALT, the design will have several, if not many, of the required lifetimes built into it and so an inconsequential portion of the life would be removed in a HASS. This would, of course, be verified in Safety of HASS. Note that the relevant question is "How much life is left after HASS?" not "How much did we remove in HASS?" Also note that all screens remove life from the product and that even normal usage will contribute some life removal or fatigue damage. This is a fundamental fact that is frequently not understood by those unfamiliar with the correct underlying concepts of screening. A properly done HALT and HASS program will leave more than enough life remaining and will do so at a much reduced total program cost.

Flaws of other types have different equations describing the relationship between stress and the damage accumulation, but all seem to have a very large time compression factor resulting from a slight increase of the stress. This is precisely why the HALT and HASS techniques generate such large time compression.

36.6 Equipment Required

The application of the techniques mentioned in this chapter generally is very much enhanced by, if not impossible without, the use of environmental equipment of the latest design such as all axis exciters and combined very high rate thermal chambers (80°C/min. or more product rate). All axis means three translations and three rotations, all simultaneous, all broadband random. See Figure 36.3 of a HALT chamber.

Figure 36.3. HALT chamber. Courtesy of HALT&HASS Systems Corp, TC-2 Cougar Time Compression System

A single axis, single frequency shaker will only excite some modes in the particular direction of the vibration and only those nearby in frequency. For example, the second mode of a circuit board will not be excited as the modal participation factor is zero for pure linear motion in any one direction. It takes rotational motion to excite this mode. A swept sine will sequentially excite some modes in the one direction being excited. Single axis random will simultaneously excite some modes in one direction. A six-axis system will simultaneously excite all modes within the bandwidth of the shaker in all directions. If all modes in all directions are not excited simultaneously, then many defects can be missed. Obviously, the all axis shakers are superior for HALT and HASS activities as one is interested in finding as much as possible as fast as possible as we are doing discovery testing, not compliance testing.

In the very early days of design ruggedization (the precursor to HALT), a device had been severely ruggedized using a single axis random shaker system. This effort was reported in [13]. Then, in production, a very early all axis system

was used and three design weaknesses which had not been found on the single axis system were exposed almost immediately. Increasing the shaker vibration to the full bandwidth (which had been restricted on purpose) exposed even another design flaw. That experience showed the author the differences in the effectiveness of the various systems. Since then, the systems of choice have been an all axis broadband shakers of ever improving characteristics.

Other types of stresses or other parameters may be used in HALT. In these cases, other types of stressing equipment may be required. If one wanted to investigate the capability of a gearbox, one could use contaminated oil, out of specification gear sizes and a means for loading the gearbox in torsion either statically or dynamically. If one wanted to investigate various end-piece crimping designs on power steering hoses, one could use temperature, vibration and oil pressure simultaneously. This has been done and worked extremely well, exposing poor designs in just a few minutes. In order to investigate an airframe for robustness in pressurization, the hull could be filled with water and rapid pressure cycling done. This is how it is done at several aircraft manufacturers. Water is used as the pressurized medium as it is nearly incompressible and so when a fracture occurs, pressure drops quickly preventing an explosive type of failure as would occur if air were to be used. A life test simulating thousands of cycles can be run in just a few days using this approach.

In HALT and HASS, one tries to do fatigue damage as fast as possible; and the more rapidly it is done, the sooner it can stop and the less equipment is needed to do the job. It is not unusual to reduce equipment costs by *orders* of magnitude by using the correct stresses and accelerated techniques. This comment applies to all environmental stimulation and not just to vibration. An example discussed in [1] shows a decrease in cost from $22 million to $50 thousand on thermal chambers alone (not counting power requirements, associated vibration equipment, monitoring equipment and personnel) by simply increasing the rate of change of temperature from 5°C/min to 40°C/min. The basic data for this comparison is given in [14]. Another example shows that increasing the RMS vibration level by a factor of 1.4 times would decrease the vibration system cost from $100 million to only $100 thousand for the same throughput of product. With these examples, it becomes clear that HALT and HASS techniques, when combined with modern screening equipment designed specifically to do HALT and HASS provide quantum leaps in cost effectiveness. This reason is precisely why the real leaders in this field simply keep their results to themselves.

36.7 The Bathtub Curve

The pattern of failures that occur in the field can be approximated in three ways. When there are defects in the product, so called “infant mortalities”, or failures of weak items will occur. Another type of failure is due to externally induced failures where the loads exceed the strength. Finally, wear out will occur even if an item is not defective. When one superimposes all three types of failures, a figure called the bathtub curve results. One such curve is shown in Figure 36.4.

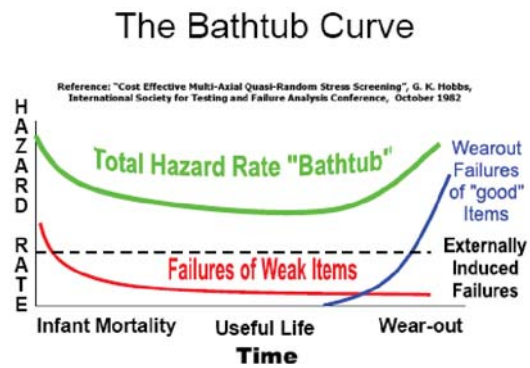


Figure 36.4. The bathtub curve

The bathtub curve is grossly affected by the HALT and HASS technique:

1. HALT and HASS will reduce the early segment of the curve by eliminating early life failures due to design weaknesses and manufacturing flaws and will also eliminate those failures due to gross weaknesses.

2. Ruggedization (HALT) of the product will lower the mid-portion of the curve which is due to externally induced failures.
3. HALT will extend the wear out segment far to the right.

Some typical results of HALT and HASS applied to product design and manufacturing are described in the following paragraphs. Some of these are from early successes and have been published in some form, usually technical presentations at a company. Later examples using the later technology in terms of technique and equipment have largely not been published. The later results are, of course, much better, but the early results will make the point well enough, since they represent a lower bound on the expected successes today when far better techniques and equipment are available than were present then.

36.8 Examples of Successes from HALT

a. In 1984, an electro-mechanical impact printer's MTBF was increased 838 times when HALT was applied. A total of 340 design and process opportunities for improvement were identified in the several HALTs which were run. All of these were implemented into the product before production began, resulting in an initial production system MTBF, *as measured in the field,* of 55 years! This product is about 10" x 18" x 27" and weighs about 75 lb. It is interesting that the MTBF never got better than it was at initial product release, but it did get worse when something went out of control. The out-of-control conditions were spotted by the 5% sample HASS called HASA for highly accelerated stress audit. The reason there was no reliability growth after product introduction is that the system was born fully mature due to HALT. This is one of the major goals of HALT and it is the case *if and only if* advantage is taken of all of the discovered opportunities for improvement. This product was produced by robots for ten years, after it was technically obsolete, at a rate of about $10,000,000 of product per hour!

b. A power supply which had been in production for four years in 1983 with conventional (IES Guidelines) low rate, narrow range thermal screening had a "plug and play" reliability of only 94% (That is, 6% failed essentially out of the box.) After HALT and HASS were applied using a six-axis shaker and 20°C/minute air ramp rates, the plug and play jumped to 99.6% (*i.e.*, 0.4% failed out of the box) within four months, a 15x improvement. A subsequent power supply, which had the benefit of HALT and HASS before production began, had a plug and play of 99.7% within two months of the start of production! This company has been able to simultaneously increase sales and to reduce the QA staff from 60 to 4 mostly as a result of HALT and HASS and the impact that it had on field reliability. The company also reports that the cost of running reliability demonstration tests (rel-demo) had been reduced by a *factor* of about 70 because all relevant attributable failures were found in HALT. After the application of HALT, seven products (as of 1986) had gone through rel-demo with *zero* attributable failures. Plug and play has been 100% since 1986!

c. In 1988, an electro-mechanical device was run through a series of four HALTs over a four month period. In these tests, 39 weaknesses were found using only all axis vibration, thermal cycling, power cycling and voltage variation. Revisions were made to the product after each HALT and then new hardware with revisions was built and then run through HALT. The designers refused to change anything unless it was verified in a life test. Extended life tests were run on 16 units for 12 weeks for 24 hours per day with three technicians present at all times to interact with the hardware. The tests revealed 40 problems,

39 of them the same as had been found in the HALTs. The HALTs had missed a lubricant degradation mode that only showed up after very extensive operation. A review of the HALT data revealed that the clues to this failure mode were in the data, but no actual failure had occurred because a technician had "helped out" and re-greased a lead screw every night (without the author's knowledge) so that the failure that he knew about would not occur, a success in the mind of the technician at that time, before he learned what HALT was all about. His well intended action caused an important failure mode to be missed. The author now locks up HALT units when not actually running the tests in order to prevent well meaning employees from "helping". Vibration to 20 GRMS all axis random, temperatures between -100°C and +127°C, and electrical overstress of +/- 50% were used along with functional testing in the HALT on the units in question. "Specs" were vibration of 1 GRMS and temperatures between 0–40°C. Standard commercial components were used.

d. In an informal conversation in February of 1991 between Charles Leonard of Boeing Commercial Aircraft and the author, the former said that a quote had been received for an electronics box to be built under two different assumptions. The first was per the usual Mil-Spec approach and the second was using "best practices" or the HALT and HASS approach. The second approach showed a price reduction from $1,100 to $80, a weight reduction of 30%, a size reduction of 30% and a reliability improvement of "much better". The choice as to which product to choose was obvious.

e. In 1992, the author gave a three-hour demonstration of Rapid HALT™ after a seminar. In this demonstration, three different products seen for the first time by the author were exposed to HALT. The three products had been under standard engineering investigation using normal stresses for five, four, and three years respectively. The products had been in field use for years with many field failures reported. Each product had one failure precipitated and detected in only one hour each. All of the failures reported were exposed in the three-hour demonstration HALT. *This means that in only one hour per product all major field failure modes had been determined.* The manufacturer had not been able to duplicate the field failures using classical simulation techniques and therefore could not understand the failure modes and determine the appropriate fixes before the abbreviated HALTs were performed. Two of the three failure modes were found just beyond the edge of the temperature spec, one hot and one cold, and the last one was found in ten minutes at four times the "spec" GRMS using an all axis shaker!

f. Boeing Aircraft Company reported [15] that the HALT "revealed a high degree of correspondence between failures induced in the lab and documented field failures". "Vibration appears to have been the most effective failure inducement medium, particularly in combination with thermal stress". "The 777 was the first commercial airplane to receive certification for extended twin-engine operations (ETOPS) at the outset of service. To a significant extent, this achievement was attributable to the extremely low initial failure trends of the avionics equipment resulting from the elevated stress testing and the corrective actions taken during development". In a conversation in December 1995, Charles Leonard of Boeing related that the "777 dispatch reliability after only two months of service was better than the next best commercial airliner after six years."

g. Nortel reported [16] a 19x improvement in field returns when a HASSed population of PCBAs was compared to a similar population run through burn-in.

h. In 1997, a car tail light assembly was subjected to HALT costing "x". The

improved assembly was run through an MTBF test costing 10 "x". The measured MTBF was 55 car lifetimes. Note that the HALT did much more good for the company than did the MTBF test and at a much lower cost. This result is fairly typical of the results of a properly run HALT which must include corrective action. A discussion of this is covered in [17].

i. In 1998, Otis Elevator reported on their web site that: "A test that would normally take up to three months to conduct can now be carried out in less than three weeks. HALT used for qualifying elevator components has saved Otis approximately US $7.5 million during the first 15 months of operation." In a presentation at a seminar by the author, an Otis employee related that a particular problem was found in a circuit board and, on one product, corrective action was taken while on another product it was not. On the non-improved product, failure occurred after six months of use in Miami with exactly the same failure mode found in HALT. From this the author jokingly says that two days in HALT is equivalent to six months in Miami! None of the improved products failed in service.

j. During a short course at an air conditioning manufacturer, a quick HALT was run on a rooftop compressor system which was experiencing over $2,000,000 per month in field failures (about 50% of them failed). A quick investigation with a strobe light and using a large hydraulic shaker for vertical excitation, determined that a coil was resonating at a very low frequency and that it was the cause of the field failures. A support strut was fabricated of a tube of aluminum from the trash can in the machine shop, squashed flat at the ends and bent at 45 degrees so that it could be screwed to the housing and to the coil so as to stop the troublesome mode of vibration. Tests showed the mode gone (of course!). The improvement was on hardware shipped that day and the corresponding failure mode dropped to zero. This experience is quite typical of the situation when the product has a substantial defect and the correct techniques are applied in order to expose the defect.

Some product lines to which HALT and HASS have been successfully applied are listed in Table 36.2.

36.9 Some General Comments on HALT and HASS

The successful use of HALT or HASS requires several actions to be completed. In sequence these are: precipitation, detection, failure analysis, corrective action, verification of corrective action, and then entry into a database. All of the first five must be done in order for the method to function at all, adding the sixth results in long-term improvement of future products.

1. Precipitation means to change a defect which is latent or undetectable to one that is patent or detectable. A poor solder joint is such an example. When latent, it is probably not detectable electrically unless it is extremely poor. The process of precipitation will transpose the flaw to one that is detectable, that is, cracked. This cracked joint may be detectable under certain conditions such as modulated excitation. The stresses used for the transformation may be vibration combined with thermal cycling and perhaps electrical overstress. Precipitation is usually accomplished in HALT or in a precipitation screen.
2. Detection means to determine that a fault exists. After precipitation by whatever means, it may become patent, that is, detectable. Just because it is patent does not mean that it will actually be detected, as it must first be put into a detectable state, perhaps using Modulated Excitation™, and then it must actually be detected. Assuming that we actually put the fault into a detectable state and that

Table 36.2. Some products successfully subjected to HALT and HASS

Abs systems	Distance measuring equipment	Portable communications
Accelerometers	Down hole electronics	Portable welding systems
Air conditioners	Electronic controls	Power tools
Air conditioner control systems	Electronic carburetors	Power supplies
Air bag control modules	Electronics	Power control modules
Aircraft avionics	Fax machines	Printers
Aircraft flap controllers	Fire sensor systems	Prostate treatment system
Aircraft hydraulic controls	Flight control systems	Proximity fuses
Aircraft instruments	Flow sensing instruments	Racks of electronics
Aircraft pneumatic controls	Fm tuners	Radar systems
Aircraft engine controls	Garage door openers	Refrigerators
Aircraft antenna systems	Global positioning systems	Respiratory gas monitors
Anesthesiology delivery devices	Guidance and control systems	Safety and arming devices
Anti skid braking systems	Heart monitoring systems	Shaker tables
Area navigation systems	Impact printers	Solid state memory systems
Arrays of disk drives	Ink jet printers	Spectrum analyzers
Asics	Instant cameras	Speed brake controls
Audio systems	Invasive monitoring devices	Stationary welding systems
Automation systems	Iv drip monitors	Stereo receivers
Automotive dashboards	Jet engine controllers	Switching power supplies
Automotive engine controls	Laptop computers	Tape drive systems
Automotive exhaust systems	Laser printers	Tape players
Automotive interior electronics	Lipstick	Target tracking systems
Automotive speed controls	Ln2 thermal cycling chambers	Telecommunications equipment
Automotive traction controls	Locomotive engine controls	Telephone systems
Blood analysis equipment	Locomotive electronics	Televisions
Calculators	Loran systems	Thermal control systems
Cameras	Magnetic resonance instruments	Thermal imaging gun sight
Card cages	Manual transmissions	Thermostats
Casagranian telescope structure	Mainframe computers	Torpedo electronics
Cash registers	Medical electronics	Traction control systems
Cassette players	Meters	Tractor engine control modules
Cat scanner	Microwave communication systems	Tractor instrumentation
Cb radios	Microwave ranges	Transmission controls
Centrifuges	Missiles	Trash compactors
Check canceling machines	Modems	Turbine engine monitoring equip
Circuit boards	Monitors	Turbine engine control modules
Climate control systems	Mri equipment	Typewriters
Clothes washing machines	Navigation systems	Ultrasound equipment
Clothes dryers	Notebook computers	Urine analysis machines
Clothes washers	Oscilloscopes	Vibration control systems
Computers	Ovens	Vibration monitoring systems
Computer keyboards	Oximeters	Vibrators
Communication radios	Pacemakers	Video recorders
Copiers	Personal computers	Vital signs monitors
Dialysis systems	Plotters	Water sprinkler systems
Dish washers	Pneumatic vibration systems	Work stations
Disk drives	Point of sale data systems	X-ray systems

the built in test or external test setup can detect the fault, we can then proceed to the most difficult step, which is failure analysis. If coverage does not exist for such a fault, then it will not be detected and nothing will be done about it.

3. Failure analysis means to determine why the failure occurred. In the case of the solder joint, we need to determine why the joint failed. If doing HALT, the failed joint could be due to a design flaw; such as, an extreme stress at the joint due to

vibration or maybe due to a poor match of thermal expansion coefficients. When doing HASS, the design is assumed to be satisfactory (which may not be true if changes have occurred) and in that case, the solder joint was probably defective. In what manner it was defective and why it was defective need to be determined in sufficient detail to perform the next step which is corrective action.

4. Corrective action means to change the design or processes as appropriate so that the failure will not occur again in the future. This step is absolutely essential if success is to be accomplished. In fact, corrective action is the main purpose of performing HALT or HASS. A general comment is appropriate here. One of the major mistakes that the author sees happening in industry is that they "do HALT" and discover weaknesses and then dismiss them as due to overstress conditions. This is a major blunder! It is true that the failures occurred sooner than they would in the field due to the overstress conditions, but they would have occurred sooner or later in the field at lower stress levels.
5. Verification of corrective action needs to be accomplished by testing to determine that the product is really fixed and that the flaw which caused the problem is no longer present. The fix could be ineffective or there could be other problems causing the anomaly which are not yet fixed. Additionally, another fault could be induced by operations on the product and this necessitates a repeat of the conditions that prompted the fault to be evident. Note that a test under zero stress conditions will usually not expose the fault. One method of testing a fix during the HALT stage is to perform HALT again and determine that the product is at least as robust as it was before and it should be somewhat better. If one is in the HASS stage, then performing HASS again on the product is in order. If the flaw is correctly fixed, then the same failure should not occur again.
6. The last step of the six is to put the lesson learned into a database from which one can extract valuable knowledge whenever a similar event occurs again. Companies which practice correct HALT and utilize a well kept data base soon become very adept at designing and building very robust products with the commensurate high reliability and much lower costs. These companies usually are also very accomplished at HASS and so can progress to HASA, the audit version of HASS.

It is essential to have at least the first five steps (1–5) completed in order to be successful in improving the reliability of a product. If any one of the first five steps is not completed correctly, then no improvement will occur and the general trend in reliability will be toward a continuously lower level. The second law of thermodynamics verifies this when stated as "A system will always go to a lower organizational state unless something is done to improve that state."

A comparison of the HALT and HASS approach and the classical approach is presented in Table 36.3. Note that HALT and HASS are proactive; that is, seek to improve the product's reliability, and much of the classical approaches are intended to measure the product's reliability, not to improve it.

36.10 Conclusions

Today, HALT and HASS are required on an ever increasing number of commercial and military programs. Many of the leading commercial companies are successfully using HALT and HASS techniques with all axis broadband vibration and moderate to very high rate thermal systems as well as other stresses appropriate to the product and to its in-use environment. However, most are restricting publication of results because of the phenomenal improvements in quality and reliability and vast cost savings attained by using the methods. HALT and HASS is very difficult to

Table 36.3. Comparision of HALT (discovery) and classical (compliance) approaches

STAGE	DESIGN		PRE-PRODUCTION			PRODUCTION		
TEST TYPE	**QUALIFI-CATION**	**HALT**	**LIFE TEST**	**HASS DEV-ELOPMENT**	**SAFETY of HASS**	**REL-DEMO**	**HASS**	**HASS OPTI-MIZATION**
Purpose	Satisfy customer requirements	Maximize margins, minimize sample	Demo life	Select screens and equipment	Prove OK to ship	Measure reliability	Improve reliability	Minimize cost, maximize effectiveness
Desired outcome	Customer acceptance	Improve margins	MTBF & spares required	Minimize cost, maximize reliability	Life left after test	Pass	Root cause corrective action	Minimize cost, maximize effectiveness
Method	Simulate field environment sequentially	Step stress to failure	Simulate field	Maximize time compression	Multiple repeats without wearout	Simulate field	Accelerated stimulation	Repeat HASS, modify profiles
Duration	Weeks	Days	Months	Days	Days	Months	Minutes	Weeks
Stress level	Field	Exceeds field	Field	Exceeds field	Exceeds field	Field	Exceeds field	Exceeds field

specify or to interpret in contractual language. This is one of the reasons why the aerospace and military have been slower to accept these advanced techniques. Training of vendors is crucial as most vendors have the compliance testing mindset, not the discovery testing mindset. Without proper training in the HALT and HASS techniques, the vendors usually just say "Tell me exactly what to do and then pay me for it". After reading [1], it should be obvious that it is impossible to tell anyone exactly how to perform HALT on their product, so it is imperative to train them on the discovery techniques and on how the techniques will benefit their company.

The best-known method to determine the actual reliability of a product is to test numerous samples of the product in field environments for extended periods of time. This would, of course, either delay the introduction of the product, or provide reliability answers far too late in order to take timely corrective action. Significant time compression can be obtained by eliminating low stress events which create little fatigue damage and simulating only the high stress events. This approach [18] may reduce the test time from years to months. The HALT and HASS approach accelerates this even further by increasing the stresses far beyond the actual field levels and decreases the time to failure to a few days or even hours, sometimes only a few seconds. The use of accelerated testing and Weibull analysis combined can help to estimate lifetimes in the field environments before wear out [15].

One has to want to obtain top quality in order to adopt the cultural change necessary for the adoption of HALT and HASS. The basic philosophy is, simply stated, "find the weaknesses however one can and use their discoveries as opportunities for improvement". This constitutes a new paradigm compared to the old "pass the test" approach! HALT and HASS focus on improving reliability, not on measuring or predicting it. Many companies have saved millions of dollars using these techniques. It is now time for you to try them.

References

[1] Hobbs GK. HALT and HASS, the new quality and reliability paradigm. Hobbs Engineering Corporation. www.hobbsengr.com.

[2] Comprehensive HALT & HASS and HALT & HASS Workshop, Seminar and Workshop by Hobbs Engineering Corporation. www.hobbsengr.com

[3] Bralla JG. Design for excellence. McGraw-Hill, New York, 1996; 255.
[4] Proteus Corporation. www. Proteusdvt.com
[5] IES Environmental stress screening guidelines. Institute of Environmental Sciences, 940 E Northwest Highway, Mount Prospect, IL 60056, 1981.
[6] Bernard A. The French environmental stress screening program. Proceedings, 31st Annual Technical Meeting, IES 1985; 439–442.
[7] Hobbs GK. Development of stress screens. Proc. of Ann. Reliability & Maintainability Symposium, New York 1987:115.
[8] Dept. of the Navy, NAVMAT P-9492, May 1979.
[9] HALT & HASS Systems Corporation. www.haltandhass.com
[10] International Journal of Quality and Reliability Engineering. John Wiley. Sept–Oct.1990; 6(4) (This whole issue is must reading for anyone using MIL-HBK 217 type methods).
[11] Hakim EB. Microelectronic reliability/ temperature independence. U.S. Army LABCOM, Quality and Reliability Engineering 1991; 7:215–220.
[12] David Steinberg. Vibration analysis of electronic equipment. Wiley, New York, 1973.
[13] Hobbs GK, Holmes J. Tri-axial vibration screening– An effective tool. IES ESSEH, San Jose, CA; Sept. 21–25, 1981.
[14] Smithson SA. Effectiveness and economics– yardsticks for ESS decisions. Proceedings of the Institute of Environmental Sciences 1990.
[15] Minor EO. Accelerated quality maturity for avionics. Proceedings of the Accelerated Reliability Technology Symposium, Hobbs Engineering Corporation, Denver, CO 1996; Sept. 16–20.
[16] Cooper MR, Stone KP. Manufacturing stress screening results for a switched mode power supply. Proceedings of the Institute of Environmental Sciences 1996.
[17] Edson L. Combining team spirit and statistical tools with the HALT process. Proceedings of the 1996 Accelerated Reliability Technology Symposium, Hobbs Engineering Corporation, Denver, CO 1996; 16–20 September.
[18] Hobbs GK. Accelerated Reliability Engineering: HALT and HASS. John Wiley & Sons, 2000.

37

Modeling Count Data in Risk Analysis and Reliability Engineering

Seth D. Guikema and Jeremy P. Coffelt

Texas A&M University, USA

Abstract: This chapter presents classical (non-Bayesian) regression models for count data. This includes traditional multivariate linear regression, generalized regression models, and more recent semi-parametric and non-parametric regression models used in data mining. Then, the Bayesian approach for handling count data is also presented. The focus here is on formulating priors. Finally, the chapter concludes with a discussion of computational issues involved in using these models.

37.1 Introduction

One of the main goals of risk analysis and reliability engineering is to estimate the probabilities and consequences of possible adverse outcomes in a given situation in order to support the allocation of limited resources to best reinforce technical systems and manage the situation. For example, risk analysis can be used to help allocate resources in managing the development of inter-planetary space missions [1, 2]. There are two basic sources of information to support risk analysis and reliability engineering – expert knowledge and data.

In some cases, expert knowledge is the best information available. For example, the system being designed may be much different from any previous system, making existing data about the performance of the previous systems problematic as a basis for risk and reliability analysis. If the new system is also difficult to test under the conditions it will face in use, one is left with a situation in which expert knowledge and engineering models represent the best available information. An example of this is the main mirror on the Hubble Space Telescope (HST). At the time it was on ground, the HST main mirror was unique in both its size and the tightness of the tolerances to which it was to be manufactured. No particularly good way existed to test the mirror in zero-gravity, so no test was conducted. Instead, the engineers relied on their best judgment and concluded that the mirror would perform as expected in space. However, the mirror subsequently distorted in zero-gravity, necessitating a very costly and difficult in-orbit repair. Expert opinion can be used in risk analysis through the methods of probabilistic risk analysis (PRA). Modarres [3] provides a recent overview of these methods. However, if relevant data are available, these data can significantly strengthen the results of the risk analysis or reliability assessment.

When the system is not a unique, one of a kind system, there is often data available about the performance of it or similar systems under similar loadings. This information might come from records from past use of the same system, records

from similar systems, or testing of the system being analyzed. In all cases, the goal of using the data in risk analysis or reliability engineering is to use the past data to probabilistically predict the likely performance of the system in the future. One particular type of data that arises frequently in risk analysis and reliability engineering is count data.

Count data arises whenever one is concerned with the number of occurrences of some discrete event, and an analyst wishes to use relevant past data to estimate the likelihood of different numbers of events in the future. Examples include using records of past breaks in a water distribution system to estimate which pipes are most likely to break in the next planning period [4, 5] and using past data about power outages during hurricanes to estimate the number and location of outages in an approaching hurricane [6, 7]. Further examples are the use of launch records for space launch vehicles to estimate the probability that a given vehicle will fail on its next launch [8, 9], and the use of past data about mercury releases and autism counts in schools to estimate the impact of mercury releases on autism rates [10].

Count data is common in risk analysis and reliability engineering, and recent research advances have created a number of promising, state of the art modeling frameworks for analyzing count data. However, these methods have not been widely used in risk analysis and reliability, especially the more recent advanced methods. The purpose of this chapter is to give an overview of these methods, concentrating especially on those that involve modeling a relationship between the counts of interest, y, and a set of variables, x, that might help to explain the variability in y and predict the likelihood of different values of y in the future. This is a type of regression problem in which $y = f(x)$ where $f(x)$ is an unknown function of the explanatory variables in x.

37.2 Classical Regression Models for Count Data

The purpose of regression modeling is to find a relationship between predicting or explanatory variables $x = (x_1,x_2,\ldots,x_n)$ to a variable y referred to as the response variable. More specifically, the goal is to find the best approximation of the function f satisfying $y= f(x)$. Bayesian methods involve utilizing information relevant to the model and then updating this information based on available data. This allows for additional information such as expert opinion and historic data sets not included in the data set being analyzed. In contrast, classical approaches rely entirely on data to determine models. Another difference resulting from the theoretical foundations of these two approaches is in how the models are fit. Classical models are generally fit by analytically or numerically maximizing the likelihood of the observed data in selecting parameter values. This is quite different from the Bayesian methods described in the following section, which generally rely on much more involved computation. These differences and tradeoffs are discussed further in the following section.

The classical models considered in this section vary over a wide range of interpretability and flexibility. The simplest to formulate, least flexible, and most well known is ordinary least squares regression (OLS). On the other end of the spectrum is multivariate adaptive regression splines (MARS), which offer the most flexibility, but may also substantially sacrifice interpretability. Compromises between these two extremes include generalized linear models (GLMs), generalized linear mixed models (GLMMs), and generalized additive models (GAMs).

37.2.1 Ordinary Least Squares Regression (OLS)

The most common regression model, OLS, is also the simplest to state. OLS requires only that the response variable is somehow distributed around a linear combination of the predicting covariates. That is, this model has the form

$$y = \beta_0 + \sum_i \beta_i x_i + \varepsilon \,, \tag{37.1}$$

where ε is a residual error term. The least squares nomenclature follows from the traditional assumption that the residuals are normally distributed, which results in maximum likelihood

estimators (MLEs) for the parameters $\beta = (\beta_1,\beta_2,,\ldots,\beta_n)$ that minimize the sum of the squares of the residuals. To be consist with the notation to follow, note that (37.1) can be rewritten as

$$y \sim Normal\left(\mu, \sigma^2\right), \tag{37.2}$$

with

$$\mu = \beta_0 + \sum_i \beta_i x_i . \cdot \tag{37.3}$$

The flexibility of the OLS model can be substantially increased by transforming and combining the data into more suitable covariates. For example, when modeling count data it is assumed that y is nonnegative. Therefore, one might consider in place of (37.1), a relationship more along the lines of

$$\ln(y+1) = \beta_0 + \sum_i \beta_i x_i + \varepsilon \tag{37.4}$$

ensuring the predicted y is at least a nonnegative real number. Notice that this transformation and others like it can only address the non–negativity, not the discreteness of count data. Other common transformations of predicting covariates include taking logarithms, reciprocation, and various other simple algebraic manipulations.

There are several limitations of the OLS framework that are overcome by the models to follow. The first is that the distribution of y conditional on the observed data x is required to be normal. This assumption is often invalid as is certainly the case when considering the integral nature of count data. Also, even though count data typically demonstrate heteroskedasticity, the magnitude of the errors in the OLS model is implicitly assumed to be independent of the magnitude of y. Perhaps most importantly, though, is that the predicting covariates are assumed independent of each other and can therefore only result in linear impacts on the response variable.

Despite such shortcomings, the OLS model has found numerous applications in risk analysis and reliability engineering. Two particular examples given in the introduction and found in the literature involve the reliability of utility distribution systems. In Radmer *et al*. [11], OLS was used to predict outages in electric power distribution systems. Pipe breaks in water distribution systems have also been modeled using OLS models (see in particular [12–15]).

37.2.2 Generalized Linear Models (GLMs)

GLMs, which consist of three components, are a natural extension of the OLS model. The first component, referred to as the random component, specifies the behavior of the response variable for fixed predicting variables. More formally, it allows the normal distribution in (37.2) to be replaced with any distribution from the exponential family. Almost all familiar distributions, including the normal, binomial, exponential, Poisson, and negative binomial distributions are members of the exponential family. Therefore, the random component of GLMs allows for the type of response variable to be taken into account when formulating the model. For example, count data can be modeled as such by using the Poisson or negative binomial distributions in place of the continuous normal distribution required in the OLS model. Also of interest to those in reliability engineering and risk analysis is that the probability of a binomial response, such as success/failure outcome, can be modeled using the Bernoulli distribution. Another component in a GLM specifies the predicting variables and the relationships between them. This systematic component is typically of the same form as in (37.3), *i.e.,*

$$\eta = \beta_0 + \sum_i \beta_i x_i . \tag{37.5}$$

The final component links the systematic and random components. This link component generally is of the form

$$g(\eta) = \alpha , \tag{37.6}$$

where α is some parameter of the underlying distribution specified in the random component and g is referred to as the link function. Two important examples include the Poisson and logistic regression models. The Poisson model is specified by:

$$y \sim Poisson\left(\lambda\right) \tag{37.7}$$

with the log link given by (37.8).

$$\log \lambda = \beta_0 + \sum_i \beta_i x_i. \tag{37.8}$$

The logistic model is specified by

$$y \sim Binomial(p, n) \tag{37.9}$$

and the logit link

$$\begin{aligned} \text{logit}\, p &= \log \frac{p}{1-p} \\ &= \beta_0 + \sum_i \beta_i x_i, \end{aligned} \tag{37.10}$$

where p is the probability of a success. Two good references for these models introduced by Nelder and Wedderburn [16] are the books by Cameron and Trivedi [17] and Agresti [18].

The Poisson GLM defined above is by far the most common regression model used for count data. However, this model has several shortcomings. Most significantly is the assumption of equidispersion inherent to the Poisson distribution. This assumption that the mean and variance are equal is commonly contradicted by the observed data. In fact, the situation in which the variance of the counts is greater than the mean, called overdispersion, is common enough that numerous studies have been devoted to generalizing the Poisson GLM to properly deal with it. The simplest and most common of these is the negative binomial GLM, which is appropriate when overdispersion is present. The formulation of the negative binomial GLM is the same as that for the Poisson GLM except that (37.7) is replaced with

$$y \sim Negative\ Binomial(\lambda, \alpha). \tag{37.11}$$

where α is a parameter related to the variance of the distribution.

As in the case of OLS, GLMs have been widely applied in reliability engineering and risk analysis. For example, Liu *et al.* [6] used a negative binomial GLM to estimate power outages during hurricanes, Guikema *et al*. [19] used a negative binomial GLM to relate power outage frequencies to system maintenance practices, and Andreou *et al*. [4, 5] used a Poisson GLM to estimate pipe break frequency in water distribution systems.

37.2.3 Generalized Linear Mixed Models (GLMMs)

GLMMs extend GLMs through the addition of error terms to the systematic component of a GLM. One purpose of this extra structure is to specifically account for temporal or spatial correlation in the counts [18, 20]. More generally, though, this additional random term helps explain variances in the counts caused by any unknown or unobserved variables. The mixing of distributions in the random and systemic components allows for greater flexibility in describing hierarchical effects and the randomness associated with modeling complex systems.

The most familiar GLMM to those modeling count data is the Poisson GLMM with a single–level random structure given by

$$y_j \sim Poisson(\lambda_j), \tag{37.12}$$

$$\log \lambda_j = \beta_0 + \sum_i \beta_i x_{j,i} + \varepsilon_j, \tag{37.13}$$

where ε_j is a random term for the *j*th measurement. Generally, the error terms are assumed to be Normally distributed, though other distributions such as the Student's *t*–distribution can offer greater flexibility [21].

GLMMs have found much more limited applications in the risk and reliability analysis literature. Examples relevant to engineers and risk analysts include modeling the impacts of traffic on human health [22] and modeling failures of electric power distribution systems [19, 21].

37.2.4 Zero–inflated Models

Often the number of observed zero counts is much larger than would be predicted by any common statistical distribution. Examples can be found in many of the applications already discussed, but others include pathogen counts in water treatment plants and deaths from exposure to a specific carcinogen. Inflations in zero accounts frequently occur as a result of limits in the operational range of measurement devices, but are also common in situations where some activation point must be reached in order to trigger an event. In such situations, zero-inflated models may often be more

appropriate than those discussed above. There are several zero-inflated models available and most require only simple modifications to the models already introduced. Perhaps the simplest is to ignore the zero counts and model $y-1$ according to the methods discussed above. However, a more desirable approach might be to treat zeros as if occurring because of two separate processes. For example, suppose with probability δ a count y occurs according to a Poisson distribution p(y) and otherwise only a zero count can occur. Then the probability of observing a zero count is

$$(1-\delta)+\delta \cdot p(0), \tag{37.14}$$

while for any other y the probability is simply

$$\delta \cdot p(y). \tag{37.15}$$

37.2.5 Generalized Additive Models (GAMs)

One assumption of each of the models introduced so far is that the explanatory variables have only linear effects on the response variable. GAMs extend GLMs by subdividing the domain of the predicting covariates and specifying the local behavior of the response surface on each subregion. Though still requiring independence of the explanatory variables, GAMs can permit arbitrary and nonparametric dependencies on the explanatory variables. For example, a Poisson GAM can be written as

$$y \sim Poisson(\lambda), \tag{37.16}$$

$$\log \lambda = \beta_0 + \sum_i f_i(x_i), \tag{37.17}$$

where f_i is generally approximated by a continuous parametric spline. GAMs can not only involve any other distribution function such as the negative binomial distribution, but can also allow for interaction between explanatory variables through the proper choice of spline [23]. In fact, numerous splines exist and almost as many methods exist for fitting them. A common choice for the functions in (37.17) is penalized regression splines, which penalize excessive "wiggliness" to avoid over fitting the data.

GAMs often significantly improve the fit over more traditional models such as GLMs by capturing interactions not permitted in the less flexible models. However, this increase in flexibility typically results in a significant loss of interpretability. Both of these measures depend highly on the types of splines chosen in (37.17) and the bounds placed on the parameters specifying them. The most substantial benefit of GAMs is that interactions between predicting variables and their effects on the response variable can be captured when otherwise missed by using less flexible methods such as GLMs.

37.2.6 Multivariate Adaptive Regression Splines (MARS)

MARS models, introduced by Friedman in 1991 [24], further extend GAMs by allowing much more complex interactions between the responses and predicting covariates. More importantly, though, is that the data determines the interactions necessary, be it linear, additive, or a more complicated nature [25–27]. Therefore, MARS models can allow both non-linear and interdependent explanatory effects. In Holmes and Mallick [26] it was shown, based on random hold-out sample testing, that GLMs and GAMs can have significantly less predictive accuracy than the MARS approach. However, as is the case of GAMs, this increase in flexibility over simpler models comes at a price in interpretability.

MARS models have a similar structure to GAMs. For example, a MARS model used for count data could be of the same form as the Poisson GAM given in (37.16) and (37.17). The difference between MARS models and GAMs is that the functions f are not approximated by splines, but would instead be of the form

$$f(x_i) = \sum_{j=1}^{k} \beta_j B(x_i, \theta_j), \tag{37.18}$$

where the β are regression coefficients and the $B(x_j,\theta_j)$ are non-linear basis functions. Choices for basis functions include cubic and thin-plate splines, neural nets, and wavelets. In the literature, the parameter θ_j is often referred to as the knot point or knot location of the jth basis and determines the points in the domain of x that determine the changes in behavior of B.

37.2.7 Model Fit Criteria

Numerous statistics exist for determining the "best" model for the given data. Most involve the likelihood that the given parameters of the model are correct for the observed data. One of the most common is the deviance

$$D = -2(L - L^*), \tag{37.19}$$

where L is the log–likelihood of the given parameters and L^* is the log–likelihood of the saturated model with one parameter per observation. Another common fit statistic is the Akaike information criterion defined as

$$AIC = -2L + 2\nu, \tag{37.20}$$

where ν is the number of independent parameters in the model. Both of these statistics assess how well the specified model fits the given data. Both also require an underlying probability distribution and can therefore be inappropriate for models such as GAMs and MARS. An alternative goodness-of-fit statistic appropriate for all of the models is the generalized cross-validation

$$GCV = \frac{1}{(1-\nu/n)^2}\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2, \tag{37.21}$$

where n is the number of observations, ν is the number of independent parameters in the model, and y_i is the predicted approximation to y_i

Other statistics such as the root mean square error

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2} \tag{37.22}$$

and the mean absolute relative error

$$MARE = \frac{1}{n}\sum_{i=1}^{n}\frac{|y_i - \hat{y}_i|}{\hat{y}_i} \tag{37.23}$$

quantify instead how well the predicted values of the model fit the observed values in the given data.

37.2.8 Example: Classical Regression for Power System Reliability

A data set involving power system reliability will be used to compare the different classical parametric regression methods discussed above. A similar analysis to that in this example can be found in Guikema *et al*. [19] and Guikema and Davidson [21] where the counts of electrical outages are related to various system, maintenance, and population factors. The data set consists of information collected over several years from a large U.S. electric company and includes lengths of overhead and underground wire, frequency of tree trimming, and population information for approximately 650 circuits serviced by the company.

Using traditional systematic and link components of the form

$$\log(\mu) = \beta_0 + \sum_i \beta_i x_i. \tag{37.24}$$

Table 37.1 and Figures 37.1 and 37.2 were obtained. As can be seen from the residual plots, the OLS model and Poisson GLM offer the poorest fit of the models considered, while the negative binomial GLM and Poisson GLMM fit reasonably well. In every model examined, all predicting variables were standardized without any other transformation being applied.

Table 37.1. Fit statistics for classical parametric regression models fit to power outage data set

Fit Criteria	Deviance	AIC	GCV	RMSE	MARE
OLS model	173848	5479	274	16.4	0.49
Poisson GLM	6032	9073	316	17.6	0.50
Negative binomial GLM	684	5052	463	21.3	0.50
Poisson GLMM	6844	1188	429	20.4	0.58

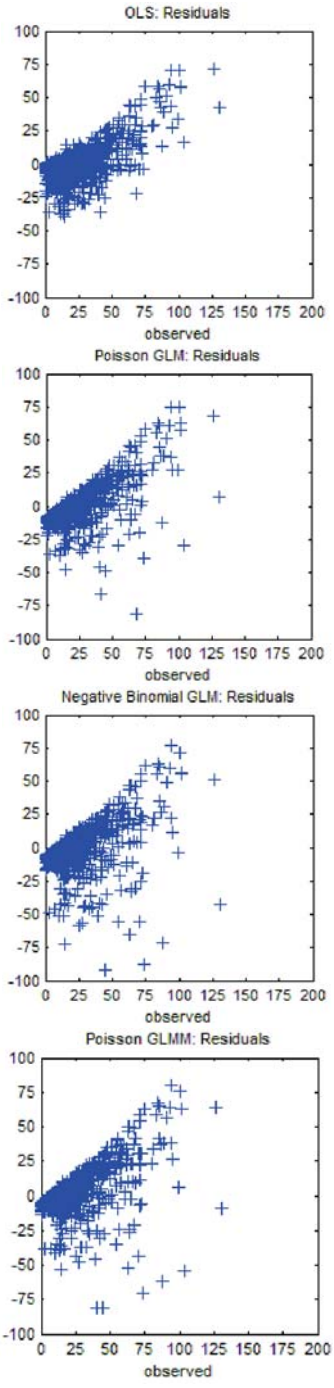


Figure 37.1. Residual plots for classical regression models fit to power outage data set

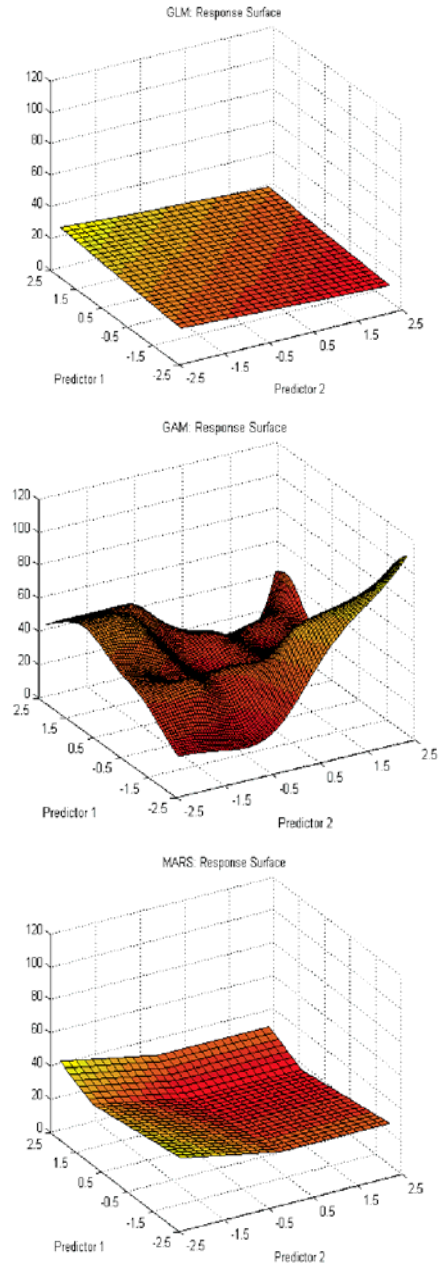


Figure 37.2. Predicted counts estimated from GLM, GAM, and MARS models for the example tree trimming data set

The link function for λ predicted by the Poisson GLMM is given by

$$\log \lambda = 25.8225 + 0.9112 \cdot ftrim - 1.2785 \cdot ltrim + 11.4139 \cdot oh + 1.3275 \cdot ug + 6.4864 \cdot cust + 4.4905 \cdot popdens \quad (37.25)$$

where ltrim is the standardized number of years since the most recent tree trimming, ftrim is the standardized number of years since the next most recent tree trimming, oh is the standardized length of overhead wire, ug is the standardized length of underground wire, cust is the standardized number of customers served by the given circuit, and popdens is the standardized density of the zip code in which the given circuit is located.

Though the magnitudes varied, all but one of the regression coefficients in (37.25) was positive. The exception is the covariate associated to the number of years since the most recent trimming of trees near power lines. The coefficient associated with this covariate is, in contrast, negative in all of the models. Therefore, as would be expected, increases in customers served, lengths of overhead and underground wire, time since most recent tree trimmings all result in an increase in the expected number of power outages. On the other hand, the models suggest that decreasing the time since the most recent tree trimming decreases the average number of power outages on a given circuit.

It is also instructive to examine the inferences that can be drawn from the estimated model response surfaces. As shown in the results from the example data set shown in Figure 37.2, GLMs produce a simple plane as their response surface while GAMs and MARS models can capture non-linearities in their response surfaces. The increased flexibility of the GAM and MARS approaches makes them more appealing for complex, non-linear systems. However, as previously discussed, this increased flexibility comes at the cost of decreased interpretability and increased computational burden in the fitting process.

37.3 Bayesian Models for Count Data

Bayesian methods represent a fundamentally different approach to modeling uncertainty than the classical methods discussed in the previous section. Bayesian methods start with a probability density function, the prior, which represents the analyst's *a priori* knowledge about the situation [27–29]. This prior is then updated with a probability density function that represents the likelihood of obtaining the observed data given the initial beliefs. Mathematically, Bayesian updating is done through Bayes' theorem, given in (37.26) where the data is represented by D, a is the parameter of interest in the problem, and A is the random variable from which a is drawn.

$$f_{A|D(t)}\left(a \mid D(t)\right) = \frac{\left(likelihood\right) \times \left(prior\right)}{\left(total\ probability\ of\ the\ data\right)} = \frac{f_{D|A}\left(D \mid a\right) f_A\left(a\right)}{\int_x f_{D|A}\left(D \mid x\right) f_A\left(x\right) dx} \quad (37.26)$$

Bayesian methods offer two main advantages over classical (frequentist) methods. The first advantage of Bayesian methods over classical methods is that they allow expert knowledge and other forms of imprecise information to be included in a model. Expert knowledge and imprecise data can be directly incorporated into a Bayesian analysis through the use of informative prior distributions for model parameters. The second advantage of Bayesian methods is that they provide a more complete characterization of the uncertainty present in a modeling problem. Unlike classical methods, which typically yield estimates of parameters or moments of an assumed distribution, Bayesian methods yield a full posterior density function for the measures of interest. This posterior may be a complex density function that is not approximated well by standard distributions. Modeling the posterior density directly removes the need to appeal to asymptotic arguments to make inferences about measures of interest.

The advantages of Bayesian methods do come at a cost though. For complex models, simulation-based approaches such as Markov chain Monte Carlo Methods (MCMC) are needed to estimate the posterior distributions of interest [29]. This imposes a computational burden on the analyst that is not present with classical methods.

37.3.1 Formulation of Priors

Because the prior probability density functions are the way in which expert knowledge and imprecise data are incorporated into a Bayesian analysis, these priors play a critical role in Bayesian modeling. There are two main classes of priors – informative priors and non-informative priors. Informative priors contain some degree of information about the measure(s) of interest that is not contained in the data used in the likelihood function.

Non–informative priors, onthe other hand, contain the minimum amount of information possible. Informative priors are used when the analyst has additional information not included in the data being analyzed. For example, Paté-Cornell *et al.* [2] needed to assess the likelihood that a rover spacecraft would be able to land successfully on Mars as part of a risk analysis. Little data is available about past landings of this type of spacecraft on Mars because only a handful of spacecraft have attempted Mars landings of this sort. However, a considerable amount of information is available from engineering models of system behavior, testing of the system done on earth, and the expert knowledge of senior engineers on the design team. This type of information can be incorporated through an informative prior.

Non-informative priors are used when either (i) the analyst does not have any additional information or knowledge about the measure(s) of interest beyond the information contained in the data used in the likelihood, or (ii) the analyst wishes to assume no additional information to let the data drive the analysis. Often the second of these, letting the data drive the analysis, is done to facilitate comparisons with classical models. Non-informative priors generally spread the probability density evenly over the possible sample space. For example, a non–informative prior for a parameter that must lie between 0 and 1 (*e.g.*, the unknown probability of a discrete event) can be a uniform (0,1) variable. Similarly, an approximately non-informative prior for a parameter that can take on any real value is a normal distribution with a mean of 0 and a large variance. However, Jeffreys [30] argued that in the case of continuous positive parameter α, the prior probability should be proportional to $(1/\alpha)$ (see [31] p. 423 for a discussion). Regardless of which form of non-informative or minimally informative prior is used, the goal is the same: to use the Bayesian framework without including any additional information in the prior distribution.

If, instead of using a non-informative prior, an analyst wishes to formulate and use an informative prior, different approaches exist. Each of these has strengths and weaknesses. However, a fundamental distinction is between those priors that are based solely on expert knowledge and those priors that are based on data from related situations.

Priors based solely on expert knowledge can be formulated. A number of approaches exist for formulating priors, and these approaches generally rely onassessing the parameters, moments, quartiles, or other summary statistics of a distribution directly with the expert(s). Spetzler and von Holstein [32] give an overview of the early development of these methods.

The basic approach is to present the expert with a series of trade-offs. For example, if the probability p, of some event, is to be assessed, the expert is asked to choose between two lotteries. In one lottery, he or she would win a prize X with a specified probability q but win nothing with probabiltiy $1-q$. In the other lottery, he or she would win X if some well known event occurs (*e.g.*, a 2 is drawn from a shuffled deck containing 52 cards) and win nothing if that event did not occur. The probability of the known event is changed and the choice iteratively offered until the expert is indifferent between the two lotteries. When the decision-maker is indifferent between the lotteries, q equals p.

When data is to be used in formulating a prior distribution, the question becomes one of how to best use the available information to formulate priors without adding any information to the data in the process of formulating priors. The greater the amount of data that is available, the stronger (*i.e.*, less variable) the prior distribution can be.

There are a number of methods available for formulating an informative prior on the basis of past data. These include using traditional distribution fitting methods such as maximum

likelihood estimation and the method of moments, as well as approaches such as maximum entropy methods and confidence interval matching. In all cases, the goal is to match some subset of the parameters, moments, or quantiles of a density function to the data as a basis for using that density function as a prior in the analysis. Guikema [33] reviewed these approaches. The general conclusions from Guikema [33] were:

1. If strong prior information is available, it should be used to formulate a prior with a relatively small variance. Doing so will increase the strength of the inferences, provided that the prior information is an accurate reflection of the underlying situation.
2. If there is uncertainty about whether or not the prior data is representative or if there is considerable uncertainty in the prior data, a method that assumes as little information as possible while maintaining consistency with the prior data is preferable. Such an approach will maximize the flexibility of the prior, allowing the data to more easily 'guide' the results of the analysis.

A brief overview of four methods will be given here. These are maximum likelihood estimation, the method of moments, maximum entropy estimation, and the preprior approach from Guikema and Paté-Cornell [2].

37.3.1.1 Maximum Likelihood

A maximum likelihood estimate (MLE) maximizes the likelihood of the observed data. That is, the parameters of an assumed distribution are chosen such that the likelihood of the data is maximized. A common prior formulation problem in risk analysis is the formulation of a prior for the probability of a binary failure/success event such as the success or failure of a system component. An appropriate likelihood to use to update the prior is the Binomial distribution. A conjugate prior, the prior that leads to a posterior from the same distribution family as the prior, is the Beta distribution. If an analyst has data about the mean rate of occurrence of the failure event in the past, bootstrapping can be used and a MLE prior for the probability of failure can be formulated according to (37.27) where α and β are the two parameters of the Beta distribution [33]. As discussed by Sorenson [34], an MLE is consistent and it is asymptotically efficient. However, little can be concluded about the efficiency of MLEs for situations with little data. In some situations the ML approach can be computationally intensive to implement.

$$\begin{aligned}(\alpha,\beta) &= \arg\max_{\alpha',\beta'}\left[\prod_i Beta\left(\mu_i^{(b)} \mid \alpha',\beta'\right)\right] \\ &= \arg\max_{\alpha',\beta'}\left[\prod_i\left[\frac{\Gamma(\alpha'+\beta')}{\Gamma(\alpha')\Gamma(\beta')}\left(\mu_i^{(b)}\right)^{\alpha'-1}\left(1-\mu_i^{(b)}\right)^{\beta'-1}\right]\right]\end{aligned} \tag{37.27}$$

37.3.1.2 Method of Moments

The method of moments (MM) approach was developed early as an approach for fitting a distribution to data [35]. The basic idea of MM is to match the moments of the data to the moments of the distribution being fit to that data. For example if $\mu_{d'}$ and $\sigma_{d'}^{(b)}$ are the estimated mean and standard deviation of the failure rate based on the data and bootstrap resample of the data, and a two-parameter distribution (*e.g.*, a Beta distribution) is to be used, the parameters are adjusted to yield a density function with a mean and variance equal to the sample mean and variance of the failure rate. Continuing with the Beta-binomial Bayesian example started in the MLE discussion, the mean and variance of a Beta distribution can be fit to a data sample by setting α and β equal to [33]:

$$\alpha = \frac{\hat{\mu}^2 - \hat{\mu}^3}{\left(\hat{\sigma}^{(b)}\right)^2} - \hat{\mu}^2, \tag{37.28}$$

$$\beta = \frac{\alpha\left(1-\hat{\mu}\right)}{\hat{\mu}}. \tag{37.29}$$

The MM approach is intuitively appealing, generally easy to implement, and provides estimators that asymptotically converge in probability to the true parameter as the amount of data increases. However, the MM estimators do

not, in general, have the smallest error covariance of all unbiased estimators.

37.3.1.3 Maximum Entropy

Entropy, defined in (37.30) for a given density function *f*, can be used as a measure of the amount of uncertainty contained in a probability distribution [36–38].

$$S = -\int_{-\infty}^{\infty} f(x) \log f(x)\, dx \qquad (37.30)$$

In assessing a probability density function based on a set of information, maximizing the entropy yields the density function that minimizes unwarranted assumptions of accuracy based on the data. The resulting distribution is consistent with the available data while maximizing the variability in the data. This approach has been applied in a number of areas such as image fusion [39] and composing priors for reliability analysis [33].

37.3.1.4 Pre-prior Updating

Guikema and Paté-Cornell [8] developed a method for composing a prior based on past data by using a two stage Bayesian updating approach. The analyst starts with a suitable non-informative prior. In the case of a Beta prior, this could be either a Beta (0.5, 0.5) prior, the Jeffreys prior, or a Beta (1,1), a uniform prior. This non-informative prior is then updated with the initial data sample, the data to be used in formulating the prior. This informative prior is then updated with the new data through the likelihood function to yield the posterior distribution for the problem. This approach has the advantage of being truly Bayesian in that the change in information state from no information (the pre-prior) to some information (the prior) to the final state of information (the posterior) is explicitly modeled. However, this approach does not involve both likelihood or entropy arguments; and it thus does not share the same theoretical basis as either of these other approaches.

Guikema [33] compared the results from using these prior formulation methods. The general conclusion is that the stronger the prior (*e.g.*, the smaller the variance) the greater the amount of data required to modify the prior through the likelihood if the prior information does not match that in the likelihood. However, if the prior information does match the likelihood information, a stronger prior leads to stronger posterior inferences than a prior with a higher variance. This means that the higher variance priors tend to be the most flexible, while the lower variance priors are better suited for situations with strong prior information. The most flexible informative priors tend to be those formulated on the basis of maximum entropy using minimal information from the prior data (*e.g.*, using only the mean rather than the mean and the variance). On the other hand, MLE priors tend to be more precise. There is a trade-off between precision and flexibility in formulating priors for Bayesian analysis, and an analyst must carefully weigh this trade-off on the basis of his or her degree of confidence in the prior data.

37.3.1.5 Example: Bayesian Analysis of Launch Vehicle Reliability

A Bayesian analysis of space launch vehicle success rates will be used as an example of the prior formulation process. This example is from Guikema and Paté-Cornell [8], where the probability of failure of 33 of the major families of launch vehicles in the world was analyzed. Data was collected about their past launch records, and the goal was to use this data to estimate the probability of failure of any given launch vehicle in its next flight. Launch vehicles were assumed to be binary failure/success systems, where a success occurs only if the payload is released into the intended orbit or interplanetary trajectory. This led to a model with a binomial likelihood distribution for the k successes in n trials, each with an unknown probability of occurrence of p. A prior was placed on the parameter p. Three different approaches were used for formulating the prior.

The first approach involved using a non-informative Beta prior for the p for each launch vehicle. This corresponds to the assumption that we know nothing about launch vehicle reliability before observing actual launches, or at least we will assume we know nothing. Both a uniform, or Beta (1,1), prior and a Jeffreys, or Beta (0.5,0.5),

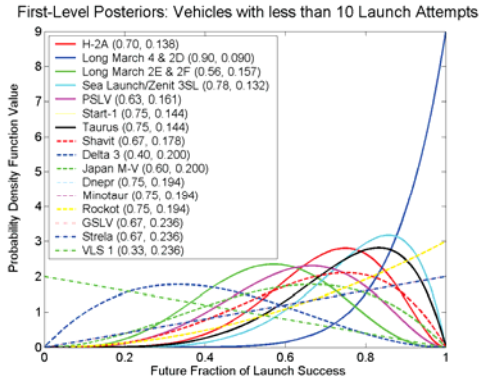


Figure 37.3. First–level posterior probability density functions for vehicles with less than 10 launch attempts. Mean, standard deviation for each distribution described in the legend. Taken from Guikema and Paté-Cornell [8]

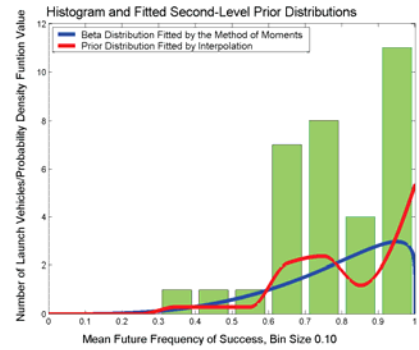


Figure 37.4. Histogram of first–level posterior means and fitted second–level prior distributions. Taken from Guikema and Paté-Cornell [8]

prior were used. Figure 37.3 shows the results of the analysis for launch vehicles with less than 10 launch attempts. The posterior density functions are quite broad for these vehicles, reflecting the lack of a large data set that would impart significant information for these vehicles.

The second approach involved plotting a histogram of the posterior means from the first approach, fitting a Beta density function to this histogram, and using this density function as the prior. This approach makes use of a basic summary statistic from the past data from all of the launch vehicles in order to develop a prior for analyzing a given launch vehicle. The implicit assumption is that the reliability of a given launch vehicle is, in some sense, believed to be similar to the average reliability of the other vehicles until data from the given launch vehicle proves otherwise. However, this approach does double-count the data from the vehicle being analyzed in the sense that the data enters into both the prior formulation (the posterior mean from that vehicle in the first level approach is included in the prior formulation) and the likelihood. Figure 37.4 shows the two priors used in this second approach. One was fit based on the method of moments, while the other used an interpolation of the means, rescaled to be a valid density function.

Figure 37.5 shows the results of the second-level analysis for vehicles with at least 96 launch attempts. The graphs show that when significant amounts of data are available, the form of the prior does not have a large impact on the results. The data "swamps" the prior information.

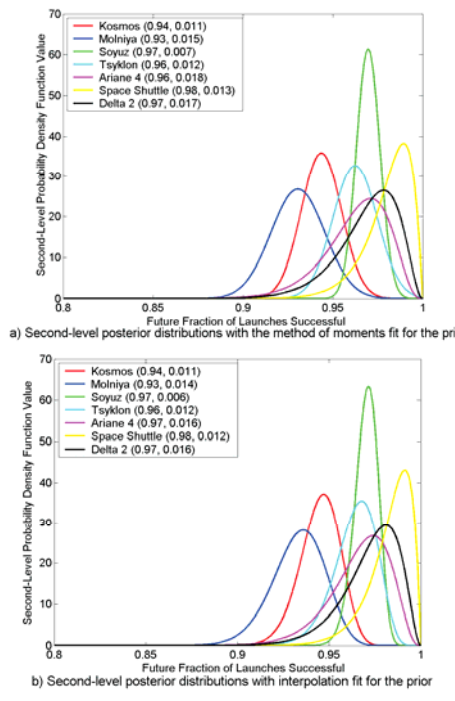


Figure 37.5. Second–level posterior probability density functions for vehicles with at least 96 launch attempts. Mean, standard deviation for each distribution described in the legend

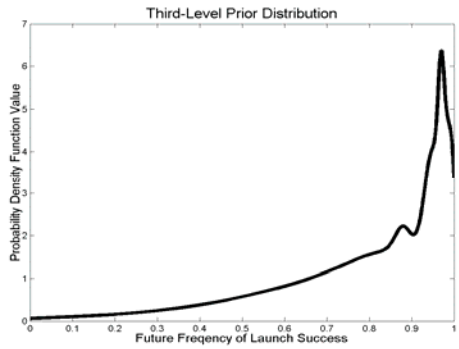


Figure 37.6. Third-level prior probability density function for a new vehicle. Taken from Guikema and Paté-Cornell [8]

Figure 37.6 shows the third approach prior for a new vehicle, and Figure 37.7 shows the third approach posterior distributions for each of the launch vehicles with less than ten launches. We see that the distributions have been shifted to the right relative to the first approach. This occurs because the prior distribution is both substantially more informative and suggests *a priori* a higher success rate in this case. This again highlights the usefulness of prior distributions for improving inferences in Bayesian analysis, especially when strong prior information is available.

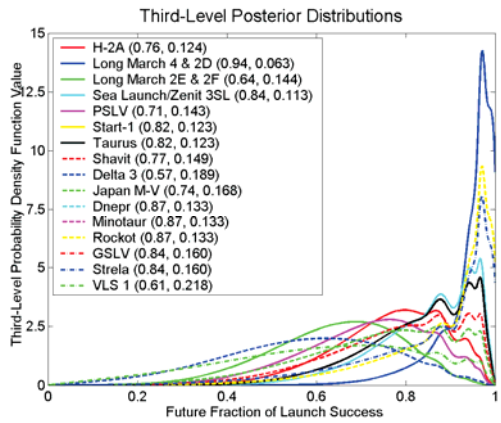


Figure 37.7. Third–level posterior probability density functions for vehicles with less than ten launch attempts. Mean, standard deviation for each distribution described in the legend. Taken from Guikema and Paté-Cornell [8]

37.3.2 Bayesian Generalized Models

Bayesian methods can also be used with the types of generalized regression models for count data discussed earlier in this chapter. There are a number of excellent textbooks written on this subject [40], and we do not duplicate these by giving an in–depth discussion of Bayesian count regression models here. Rather, we introduce the subject through a relatively simple example – a Bayesian Poisson GLMM. The model was originally presented in Guikema and Davidson [21],. Guikema and Davidson [21] used a Poisson GLMM to analyze the data set about electric power distribution reliability discussed earlier in this chapter.

The link function used in Guikema and Davidson [21] was

$$\lambda_i = \sum_j \beta_j x_{ij} + u_j \qquad (37.31)$$

where $u \sim t(0,df)$ with df considered an unknown parameter to be estimated based on the data. Non–informative normal $(0,1x10^6)$ priors were used for the regression parameters (the βs), and a non-informative Gamma distribution was used for the parameter df. These non-informative parameters were used to facilitate comparisons with classical models. Note that the major differences between this model and the classical Poisson GLMM are (i) the model was estimated within the Bayesian paradigm, and (ii) the random term in the link function used the more flexible Student's t–distribution rather than the standard normal distribution.

Figure 37.8 gives the comparison of the distributions of the random terms from the classical model with a Normally distributed random term and the posterior Bayesian density with an error term having a Student's t–distribution.

The results, especially the heavier tails in the Student's t-distribution, suggest that the Student's t–based random term captures additional variability that the normally distributed random terms do not. However, in this case, the β parameter estimates were similar in the two models.

Informative priors may also be used for the regression parameters of a GLM or GLMM or the knot points in a GAM or MARS approach. Holmes

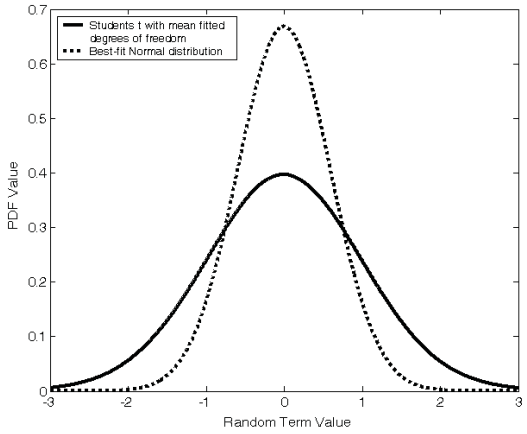


Figure 37.8. Comparison of posterior Student's *t* PDF with the estimated standard normal distribution. Taken from Guikema and Davidson [21]

and Mallick [26] discuss Bayesian approaches for the MARS approach, and similar methods may be useful for GAM approach. However, Bayesian approaches for GLMs, GLMMs, GAMs, and MARS models have generally used non–informative priors. If one wished to use informative priors, the process used to formulate these priors could potentially have large impacts on the results of the analysis, particularly if there was not a great deal of data available. One approach would be to use a pre-prior approach with a segmented data set. Another approach would be to directly assess density functions for the parameters with an expert in the subject matter being analyzed. Additional research is needed explore these different options and their impacts on modeling and model conclusions.

37.4 Conclusions

Properly accounting for and modeling count data in risk analysis and reliability engineering has the potential to significantly improve inferences and risk management decision-making. This chapter has given an introduction to these models and provided direction to more detailed discussions in the research literature and statistics textbooks. However, no discussion of modeling count data would be complete without at least a brief mention of computational issues.

Models for count data can be computationally expensive, especially Bayesian models. The basic classical models such as OLS, Poisson GLMs, and binomial GLMs can be easily fit in Matlab for small and moderate size data sets. However classical GLMMs, GAMs, and MARS models require the use of specialized statistical packages. SAS, S-plus, and R all have the capabilities needed to fit these models. R is particularly attractive to practicing engineers because it provides an open-source statistical platform that is available at no cost from http://www.r-project.org/. With the exception of the computationally simplest models (*e.g.,* models with conjugate priors), Bayesian modeling requires either numerical integration or a simulation–based approach. In the launch vehicle example, numerical integration was used to estimate the posterior distributions. In more complex regression–type problems, simulation–based Markov chain Monte Carlo (MCMC) approaches will likely be needed. This was the approach used in the Bayesian GLMM example. WinBUGS is an open–source Bayesian analysis package available at http://www.mrc–bsu.cam.ac.uk/bugs/, and it enables MCMC methods for a wide variety of models without programming the simulation. Among others, Gelman *et al.* [29] provides an overview of MCMC techniques.

Despite the computational challenges inherent in some count modeling techniques, properly accounting for and modeling count data can improve risk analysis and reliability engineering models. Stronger inferences can be drawn, and more informed risk management decisions can be made. A variety of models and techniques have been introduced in this chapter, and it is hoped that these tools will form the basis for continuing use and exploration of count modeling techniques in risk analysis and reliability engineering.

References

[1] Gaurro, Bream SB, Rudolph LK, Mulvihill RJ. The Cassini mission risk assessment framework and application techniques. Reliability Engineering and System Safety 1995; 49(3): 293–302.

[2] Paté–Cornell M.E, Dillon R.L, Guikema S.D. On the limitations of redundancies in the improvement of system reliability. Risk Analysis 2004; 24(6):1423–1436.
[3] Modarres M. Risk analysis in engineering: techniques, tools, and trends. Taylor and Francis, Boca Raton, FL, 2006
[4] Andreou SA, Marks DH, Clark RM. A new methodology for modelling break failure patterns in deteriorating water distribution systems: Theory. Advances in Water Resources 1987; 10:2–10.
[5] Andreou SA, Marks DH, Clark RM. A new methodology for modelling break failure patterns in deteriorating water distribution systems: Applications. Advances in Water Resources 1987; 10:11–20.
[6] Liu H, Davidson RA, Rosowsky DV, and Stedinger JR. Negative binomial regression of electric power outages in hurricanes. ASCE Journal of Infrastructure Systems 2005; 11(4): 258–267.
[7] Han SR, Guikema SD, Quiring S, Davidson RA, Lee KH., Rososwky DV. Estimating power outage risk during hurricanes in the gulf coast region. Disaster Recovery and Redevelopment Interdisciplinary Student Research Symposium, 6 and 7 Oct., 2006 Texas A&M University, College Station, TX 2006.
[8] Guikema SD, Paté–Cornell ME. Bayesian analysis for launch vehicle reliability. Journal of Spacecraft and Rockets 2004; 41(1): 93–102.
[9] Guikema SD, Paté–Cornell ME. Probability of infancy problems for space launch vehicles. Reliability Engineering and System Safety 2005; 87(3):303–314.
[10] Palmer RF, Blanchard S, Stein Z, Mandell D, Miller C. Environmental mercury release, special education rates, and autism disorder: An ecological study of Texas. Health and Place 2006; 12: 203–209.
[11] Radmer T, Kuntz PA, Christie RD, Venkata SS, Fletcher RH. Predicting vegetation–related failure rates for overhead distribution feeders. IEEE Trans. Power Delivery 2002; 17(4):1170–1175.
[12] Shamir U, Howard CDD. An analytic approach to scheduling pipe replacement. Journal of the American Water Works Association 1979; 71(5): 248–258.
[13] Walaski TM, Pelliccia A. Economic analysis of water main breaks. Journal of the American Water Works Association 1982; 71(3):140–147.
[14] Kettler AJ, Goulter IC. Analysis of pipe breakage in urban water distribution systems. Canadian Journal of Civil Engineering 1985; 12(2):286–293.
[15] Kleiner Y, Rajani. Forecasting variations and trends in water main breaks. Journal of Infrastructure Systems, 2002; 8(4):122–131.
[16] Nelder JA, Wedderburn RWM. Generalized linear models. Journal of the Royal Statistical Society, Series A 1972; 135(3):370–384.
[17] Cameron AC, Trivedi PK. Regression analysis of count data. Econometric Society Monographs No. 30, Cambridge, UK, Cambridge University Press, 1998.
[18] Agresti A. Categorical data analysis. 2nd Ed. Hoboken, NJ, Wiley–Interscience, New York, 2002.
[19] Guikema SD, Davidson RA, Liu H. Statistical models of the effects of tree trimming on power system outages. IEEE Transactions on Power Delivery 2006; 21(3):1549–1557.
[20] Faraway JJ. Extending the linear model with R: Generalized linear, mixed effects, and nonparametric regression models. Chapman and Hall, Boca Raton, FL, 2006.
[21] Guikema SD, Davidson RA. Modeling critical infrastructure reliability with generalized linear mixed models. Probabilistic Safety Assessment and Management (PSAM) 8, New Orleans, 2006; May.
[22] Zhu L, Carlin BP, English P, Scalf R. Hierarchical modeling of spatio-temporally misaligned data: Relating traffic density to pediatric asthma hospitalizations. Envirometrics 2000; 11(1): 43–61.
[23] Wood SN. Thin plate regression splines, Journal of the Royal Statistical Society Part B, 2003; 65(1): 95–114.
[24] Friedman J. Multivariate adaptive regression splines. Annals of Statistics 1991; 19(1):1–141.
[25] Hatie T, Tibshirani R, Friedman J. The elements of statistical learning: data mining, inference, and prediction. Springer, New York, 2001.
[26] Holmes C, Mallick BK. Generalized nonlinear modeling with multivariate smoothing splines. Journal of the American Statistical Association 2003a; 98:352–368.
[27] Holmes CC, Mallick BK. Generalized nonlinear modeling with multivariate free–knot regression splines. Journal of the American Statistical Association 2003b; 98(462):352–368.
[28] Howard RA. Decision analysis: Perspective on inference, decision, and experimentation. Proceedings of the IEEE 1970; 58(6): 823–834.

[29] Gellman AB, Carlin JS, Stern HS, Rubin DB. Bayesian data analysis. Chapman and Hall/CRC, Boca Raton, FL, 1995.
[30] Jeffreys H.. Theory of probability. Clarendon Press, Oxford, 1939.
[31] Jaynes ET. Probability theory: The logic of science. Cambridge University Press, Cambridge, 2003.
[32] Spetzler CS, Holstein CAS von. Probability encoding in decision analysis. Management Science 1975; 22:340–354.
[33] Guikema SD. Formulating informative, data-based priors for failure probability estimation in reliability analysis. Reliability Engineering and System Safety (in press) 2007, Preprint available electronically at dx.doi.org/10.1016/ j.ress.2006. 01.002.
[34] Sorenson HW. Parameter estimation: Principles and problems. Marcel Dekker, New York, 1980.
[35] Stigler SM. The history of statistics. Harvard University Press, Cambridge, MA, 1986.
[36] Shannon CE. A mathematical theory of communication. Bell Systems Technology Journal 1948; 27:379–423 and 623–656.
[37] Jaynes ET. Information theory and statistical mechanics. In Statistical physics: Ford K (editor), W. A. Benjamin Inc, New York, NY, 1963; 181–218.
[38] Katz A. Principles of statistical mechanics: The Information Theory Approach. W. H. Freeman and Company, San Francisco. 1967.
[39] Tapiador FJ, Casanova JL. An algorithm for the fusion of images based on Jaynes' maximum entropy method. International Journal of Remote Sensing 2002; 23(4): 777–785.
[40] Dey DK, Ghosh SK, Mallick BK. (editors) Generalized linear models: A Bayesian perspective. Marcel Dekker, New York, 2000.

38

Fault Tree Analysis

Liudong Xing[1] and Suprasad V. Amari[2]

[1] Department of Electrical and Computer Engineering, University of Massachusetts-Dartmouth, USA
[2] Relex Software Corporation, Greensburg, USA

Abstract: In this chapter, a state-of-the-art review of fault tree analysis is presented. Different forms of fault trees, including static, dynamic, and non-coherent fault trees, their applications and analyses will be discussed. Some advanced topics such as importance analysis, dependent failures, disjoint events, and multistate systems will also be presented.

38.1 Introduction

The fault tree analysis (FTA) technique was first developed in 1962 at Bell Telephone Laboratories to facilitate analysis of the launch control system of the intercontinental Minuteman missile [1]. It was later adopted, improved, and extensively applied by the Boeing Company. Today FTA has become one of the most widely used techniques for system reliability and safety studies. In particular, FTA has been used in analyzing safety systems in nuclear power plants, aerospace, and defense.

FTA is an analytical technique, whereby an undesired event (usually system or subsystem failure) is defined, and then the system is analyzed in the context of its environment and operation to find all combinations of basic events that will lead to the occurrence of the predefined undesired event [2]. The basic events represent basic causes for the undesired event; they can be events associated with component hardware failures, human errors, environmental conditions, or any other pertinent events that can lead to the undesired event. A fault tree thus provides a graphical representation of logical relationships between the undesired event and the basic fault events. From a system design perspective, FTA provides a logical framework for understanding the ways in which a system can fail, which is often as important as understanding how a system can operate successfully.

In this chapter, we first compare the FTA method with other existing analysis methods, in particular, reliability block diagrams, and then describe how to construct a fault tree model. Different forms of fault trees, including static, dynamic, and non-coherent fault trees and their applications will also be discussed. We then discuss different types of FTA as well as both classical and modern techniques used for FTA. We also discuss some advanced topics such as importance analysis, common-cause failures, generalized dependent failures, disjoint events, as well as application of fault trees in analyzing multistate systems and phased-mission systems. Some FTA software tools will be introduced at the end of this chapter.

38.2 A Comparison with Other Methods

System analysis methods can be classified into two generic categories: inductive methods and deductive methods. Induction constitutes reasoning from specific cases to a general conclusion. In an inductive system analysis, we postulate a particular fault or initiating event and attempt to find out the effect of this fault on the entire system failure. Examples of inductive system analysis include failure mode and effect analysis (FMEA) [2–4], failure mode effect and criticality analysis (FMECA) [2, 4, 5], preliminary hazards analysis (PHA) [2], fault hazard analysis (FHA) [2], and event tree analysis [4, 6]. In a deductive system analysis, we postulate a system failure and attempt to find out what modes of system or component behavior contribute to the system failure. In other words, the inductive methods are applied to determine what system states (usually failed states) are possible; the deductive methods are applied to determine how a particular system state can occur. FTA is an example of deductive method and is the principle subject of this chapter. Similar to FTA, we can also use reliability block diagrams (RBD) [7] to specify various combinations of component successes that lead to a specific state or performance level of a system. Therefore, RBD can also be viewed as a deductive method. In the following subsection, we give a brief comparison between fault trees and RBD.

38.2.1 Fault Trees *Versus* RBD

The most fundamental difference between fault trees and RBD is that an RBD is a success-oriented model, while a fault tree is failure-oriented. Specifically, in an RBD, one works in the "success space" and thus looks at system success combinations, whereas in a fault tree one works in the "failure space" and thus looks at system failure combinations. For practical applications in which the system failure depends only on combinations of its component failures, we may choose either a fault tree or an RBD to model the system structure. Both methods will produce the same results. But in most applications, particularly for safety critical systems, it is recommended to start by constructing a fault tree instead of an RBD because thinking in terms of failures will often reveal more potential failure causes than thinking from the function point of view [4].

In most cases, we may convert a fault tree to an RBD or *vice versa*. Particularly, the conversion is possible for all static coherent structures. In the conversion from a fault tree to an RBD, we start from the TOP event of the fault tree and replace the gates successively. A logic AND-gate is replaced by a parallel structure of the inputs of the gate, and an OR gate is replaced by a series structure of the inputs of the gate. In the conversion from an RBD to a fault tree, a parallel structure is represented as a fault tree where all the input events are connected through an AND-gate, and a series structure is represented as a fault tree where all the input events are connected through an OR-gate. Figure 38.1 shows the relationship between a fault tree and an RBD. Note that the events in the fault tree are failure events. Blocks in the RBD means the components represented by the blocks are functioning.

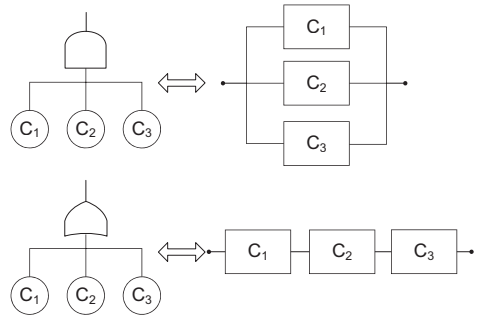


Figure 38.1. Conversion between RBDs and fault trees

Both FTA and RBD are evolutionary in nature, meaning that their modeling capabilities are enhanced as needed to support a wide range of scenarios. For example, introducing new gates, the FTA is enhanced to support sequence dependent failures. However, RBDs are not enhanced to support these modeling features. Similarly, there are some other enhancements to RBDs that are not available in FTA. Hence, it is not possible or practical to covert all fault trees into equivalent RBDs and *vice-versa*.

38.3 Fault Tree Construction

FTA is a deductive technique where we start with the failure scenario being considered, and decompose the failure symptom into its possible causes. Each possible cause is then investigated and further refined until the basic causes of the failure are understood. For more details, one can refer to [21, Chapter 8] or [32, Chapter 7]. The failure scenario to be analyzed is normally called the TOP event of the fault tree. The basic causes are the basic events of the fault tree. The fault tree should be completed in levels, and they should be built from top to bottom. However, various branches of a fault tree can be built to achieve different levels of granularity.

38.3.1 Important Definitions

The following concepts are critical for the proper selection and definition of fault tree events, and thus for the construction of fault trees:

- An *undesired event* constitutes the TOP event of a fault tree model constructed for a system. Careful selection of the undesired event is important to the success of FTA. The definition of the TOP event should be neither too general nor too specific. Here are several examples of undesired events that can be suitable for beginning FTA: overflow of a washing machine [8], no signal from the start relay of a fire detector system when a fire condition is present [4], car does not start when ignition key is turned [2], and loss of spacecraft in the space exploration [2].
- A *primary (or basic) failure* is a failure caused by natural aging of the component. For example, fatigue failure of a relay spring within its rated lifetime, and leakage of a valve seal within its pressure rating.
- A *secondary failure* is a failure induced by the exposure of the failed component to environmental and/or service stresses exceeding its intended ratings. The stresses may be shocks from mechanical, electrical, chemical, thermal, or radioactive energy sources. The stresses may be caused by neighboring components within the system, external environment, or system operators. For example, the component has been improperly designed, or selected, or installed for the application, and a failed component is overstressed or under-qualified for its burden.

38.3.2 Elements of Fault Trees

The main elements of a fault tree include:

- A TOP event: represents the undesired event, usually the system failure or accident.
- Basic events: represent basic causes for the undesired event, usually the failures of components that constitute the system, human errors, or environmental stresses. No further development of failure causes is required for basic events.
- Undeveloped events: represent fault events that are not examined further because information is unavailable or because its consequence is insignificant;
- Gates: are outcomes of one or a combination of basic events or other gates. The gate events are also referred to as intermediate events.

Readers may refer to [2, 8, 9, 21, and 32] for more details of these elements as well as their graphical representation in the fault tree model.

38.3.3 Construction Guidelines

To achieve a consistent analysis, the following steps are suggested for constructing a successful fault tree model:

1) Define the undesired event to be analyzed. The description of it should provide answers to the following questions:
   a. What: describe what type of undesired event is occurring (*e.g.*, fire, crash, or overflow).
   b. Where: describe where the undesired event occurs (*e.g.*, in a motor of an automobile).
   c. When: describe when the undesired event occurs (*e.g.*, when the power is applied, when a fire condition is present).

2) Define boundary conditions for the analysis, including
   a. Physical boundaries: define what constitutes the system, *i.e.* which parts of the system will be included in the FTA.
   b. Boundary conditions concerning environmental stresses: define what type of external stresses (*e.g.*, earthquake and bomb) should be included in the fault tree.
   c. Level of resolution: determine how far down in detail we should go to identify the potential reasons for a failed state.
3) Identify and evaluate fault events, *i.e.,* contributors to the undesired TOP event: if a fault event represents a primary failure, it is classified as a basic event; if the fault event represents a secondary failure, it is classified as an intermediate event that requires a further investigation to identify the prime causes.
4) Complete the gates: all inputs of a particular gate should be completely defined before further analysis of any one of them is undertaken (complete-the-gate rule) [2]. The fault tree should be developed in levels, and each level should be completed before any consideration is given to the next level.

38.3.4 Common Errors in Construction

Errors observed frequently in constructing fault trees are listed. The mistakes listed here are not intentional. Instead, they happen due to simple oversights, misconceptions, and/or lack of knowledge about the fault trees.

- *Ambiguous TOP event*: the definition of the undesired TOP event should be clear and unambiguous. If it is too general, the FTA can become unmanageable; if it is too specific, the FTA cannot provide a sufficiently broad view of the system.
- *Ignoring significant environment conditions*: another common mistake is to consider only failures of components that constitute the system and ignore external stresses, which sometimes can contribute significantly to the system failure.
- *Inconsistent fault tree event names*: the same name should be used for the same fault event or condition throughout the analysis.
- *Inappropriate level of detail/resolution*: the level of detail has a significant impact on the problem formulation. Avoid the formulations that are either too narrow or too broad. When determining the preferred level of resolution, we should remember that the detail in the fault tree should be comparable to the detail of the available information.

38.4 Different Forms

Fault trees can be broadly classified into coherent and noncoherent categories. Coherent fault trees do not use inverse gates, that is to say, the inclusion of inversion may lead to a noncoherent fault tree. Coherent trees can be further classified as static or dynamic trees depending on the sequence relationship between the input events. We describe these three types of fault trees in this section and their evaluation methods in Sections 38.6, 38.7, and 38.8, respectively.

38.4.1 Static Fault Trees

In a static fault tree, logical gates are restricted to static coherent gates, including AND, OR, and *K*-out-of-*N* gates. Static fault trees express the failure criteria of the system in terms of combinations of fault events. Moreover, the system failure is insensitive to the order of occurrence of component fault events [8].

38.4.2 Dynamic Fault Trees

In practice, the failure criteria of a system may depend on both the combinations of fault events and sequence of occurrence of input events. For example, consider a fault-tolerant system with one primary component and one standby spare connected with a switch controller (Figure 38.2) [10]. If the switch controller fails after the primary component fails and thus the standby is switched into active operation, then the system can continue to operate. However, if the switch controller fails

before the primary component fails, then the standby component cannot be activated, and the system fails when the primary component fails even though the spare is still operational. Systems with sequence dependence are modeled with dynamic fault trees (DFT). Dugan and Doyle [8] described several different types of sequence dependencies and corresponding dynamic fault tree gates. A brief description of them is given as follows.

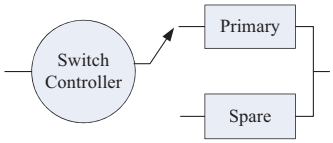


Figure 38.2. A standby sparing system

38.4.2.1 Functional Dependency (FDEP) Gate

A FDEP gate (Figure 38.3) has a single trigger input event and one or more dependent basic events. The trigger event can be either a basic event or the output of another gate in the fault tree. The occurrence of the trigger event forces the dependent basic events to occur. The separate occurrence of any of the dependent basic events has no effect on the trigger event. The FDEP gate has no logical output, thus it is connected to the fault tree through a dashed line.

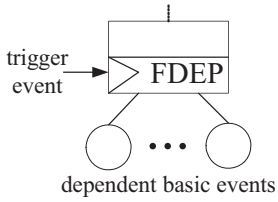


Figure 38.3. Functional dependency gate

For example, the FDEP gate can be used when communication is achieved through a network interface card (NIC), where the failure of the NIC (trigger event) makes the connected components inaccessible.

38.4.2.2 Cold Spare (CSP) Gate

A CSP gate (Figure 38.4) consists of one primary input event and one or more alternate input events. All the input events are basic events. The primary input represents the component that is initially powered on. The alternate inputs represent components that are initially un-powered and serve as replacements for the primary component. The output occurs after all the input events occur, *i.e.,* the primary component and all the spares have failed or become unavailable. As an example, the CSP gate can be used when a spare processor is shared between two active processors. The basic event representing the cold spare processor is the input event to two CSP gates. However, the spare is only available to one of the CSP gates, depending on which of the primary processors fails first.

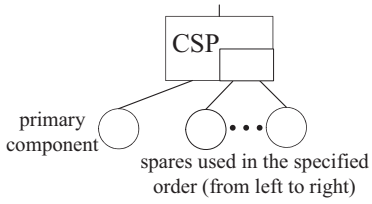


Figure 38.4. Cold spare gate

There are two variations of the CSP gate: hot spare (HSP) gate and warm spare (WSP) gate. The graphical layouts of these two gates are similar to Figure 38.4, only changing CSP to HSP and WSP respectively. In HSP, the spare components have the same failure rate before and after being switched into active use. In WSP, the spare components have reduced failure rate before being switched into active use. Note that the cold, warm, and hot spare gates not only model sparing behavior, but also affect the failure rates of basic events attached to them. As a result, basic events cannot be connected to spare gates of different types, because attenuation of the failure rate would not be defined.

Coppit *et al.* [11] suggest using a generic spare instead of a temperature (cold, warm, or hot) notion for the spare gate. The attenuation of failure rate of an unused, unfailed replica of a basic event

is dictated solely by a dormancy factor of the basic event. This change can provide more orthogonality between spare gates and basic events, and can remove the restriction on sharing of spares among spare gates. This design is implemented in Relex fault tree analysis software [12].

38.4.2.3 Priority-AND Gate

The priority-AND gate (Figure 38.5) is logically equivalent to a normal AND gate, with the extra condition that the input events must occur in a defined order. Specifically, the output occurs if both input events occur and the left input occurs before the right input. In other words, if any of the events has not occurred or if the right input occurs before the left input, the output does not occur.

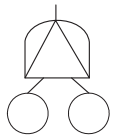


Figure 38.5. Priority-AND gate

As an example, the priority-AND gate can be used to describe one of the failure scenarios for the standby sparing system in Figure 38.2: if the switch controller fails before the primary component, the system fails when the primary component fails. Assume the cold spare is used in this example, and then the fault tree model for the entire system is shown in Figure 38.6.

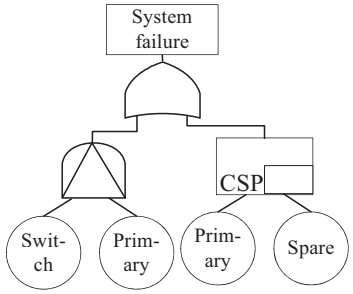


Figure 38.6. DFT of the standby sparing system

38.4.2.4 Sequence Enforcing (SEQ) Gate

The SEQ gate (Figure 38.7) forces all the input events to occur in a defined order: left-to-right order in which they appear under the gate. It is different from the priority-AND gate in that the SEQ gate only allows the events to occur in a specified order whereas the priority-AND gate detects whether the input events occur in a specified order, the events can occur in any order in practice, though.

Figure 38.7. Sequence enforcing gate

38.4.3 Noncoherent Fault Trees

A noncoherent fault tree is characterized by inverse gates besides logic gates used in coherent fault trees. In particular, it may have Exclusive-OR and NOT gates (Figure 38.8). A non-coherent fault tree is used to describe failure behavior of a noncoherent system, which can transit from a failed state to a good state by the failure of a component, or transit from a good state to a failed state by the repair of a component. The structure function of a noncoherent system does not increase monotonically with additional number of functioning components.

(a) NOT gate (b) Exclusive-OR gate

Figure 38.8. Noncoherent fault tree gates

Noncoherent systems are typically prevalent in systems with limited resources, multi-tasking and safety control applications. As an example, consider a *k*-to-*l*-out-of-*n* multiprocessor system where resources such as memory, I/O, and bus are shared among a number of processors [13]. If less than a certain number of processors *k* is being

used, the system will not work to its maximum capacity; on the other hand, if the number of processors being used exceeds *l*, the system efficiency also suffers due to the traffic congestion on a limited bandwidth bus. In FTA, we can consider the system has failed for these two extreme cases. Other examples of noncoherent systems include electrical circuits, traffic light systems, load balancing systems, protective control systems, liquid level control systems, pumping systems, and automatic power control systems [13–18].

In addition, noncoherent systems are often used to accurately analyze disjoint events [19], dependent events [20], and event trees [6]. The wide range of applications of noncoherent systems has gained the attention of reliability engineers working in safety-critical applications. As a result, several commercial reliability software vendors have extended the support of NOT logic from fault trees to reliability block diagrams [12].

38.5 Types of Fault Trees Analysis

Depending on the objectives of the analysis, FTA can be qualitative or quantitative. In the following subsections, possible results and analysis methods for qualitative and quantitative FTA will be discussed in detail.

38.5.1 Qualitative Analysis

Qualitative analysis usually consists of studying minimal cutsets. A cutset in a fault tree is a set of basic events whose occurrence leads to the occurrence of the TOP event. A minimal cutset is a cutset without redundancy. In other words, if any basic event is removed from a minimal cutset, it ceases to be a cutset.

To find the minimal cutsets of a fault tree, a top-down approach is applied. The algorithm starts at the top gate representing the TOP event of the fault tree and constructs the set of cutsets by considering the gates at each lower level. If the gate being considered is an AND gate, then all the inputs must occur to activate the gate. Thus, the AND gate will be replaced at the lower level by a list of all its inputs. If the gate being considered is an OR gate, then the occurrence of any input can activate the gate. Thus, the cutset being built is split into several cutsets, one containing each input to the OR gate.

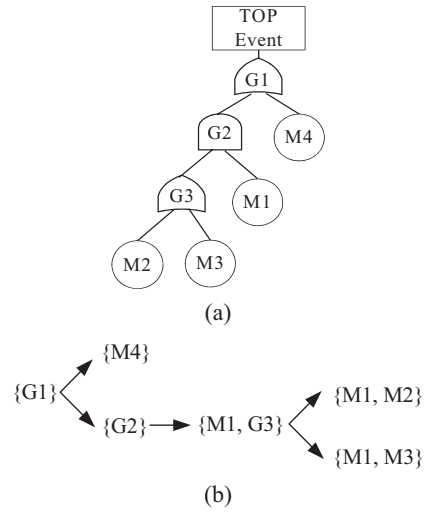


Figure 38.9. An example fault tree and its cutsets. **(a)** Fault tree, **(b)** minimal cutset generation

Consider a fault tree in Figure 38.9(a). Figure 38.9(b) shows its cutset generation. The top-down algorithm starts with the top gate G1. Since G1 is an OR gate, it is split into two sets, one containing each input to G1, that is, {G2} and {M4}. G2 is an AND gate, so it is replaced in the expansion by its two inputs {M1, G3}. Finally, the expansion of G3 splits the cutset {M1, G3} into two, yielding {M1, M2} and {M1, M3}. Therefore, there are three minimal cutsets for this example fault tree: C_1={M1, M2}, C_2={M1, M3}, and C_3={M4}.

Possible results from the qualitative analysis based on minimal cutsets include:

- All the unique combinations of component failures that may result in a critical event (system failure or some unsafe condition) in the system. Each combination is represented by a minimal cutset. For the fault tree in Figure 38.9(a), if both M1 and M2 fail, or both M1 and M3 fail, or M4 fails, the system fails.

- All single-point of failures for the system. A single-point of failure is any component whose failure by itself leads to the system failure. It is identified by a minimal cutset with only a single component. For the fault tree in Figure 38.9(a), M4 is a single-point of failure.
- Vulnerabilities resulting from particular component failures. The vulnerabilities can be identified by considering minimal cutsets that contain the component of interest. For the example system in Figure 38.9(a), once M1 fails, the system is vulnerable to the failure of either M2 or M3.

Those qualitative results can help to identify system hazards that might lead to failure or unsafe states so that proper preventive measures can be taken or reactive measures can be planned.

38.5.2 Quantitative Analysis

Quantitative analysis is used to determine the occurrence probability of the TOP event, given the occurrence probability (estimated or measured) of each basic event. Approaches for quantitative FTA can be broadly classified into three categories: state space oriented methods (see, *e.g.*, [22–26]), combinatorial methods (see, *e.g.*, [27–29]), and a modular solution that combines the previous two methods as appropriate (see, *e.g.*, [30, 31]).

The state space oriented approaches, which are based on Markov chains and/or Petri nets, are flexible and powerful in modeling complex dependencies among system components. However, they suffer from state explosion when modeling large-scale systems. Combinatorial methods can solve large fault trees efficiently. However, a widely held view among researchers is that combinatorial models are not able to model dependencies and thus cannot provide solutions to any dynamic fault tree.

The modular approach combines both combinatorial methods and state space oriented methods. Specifically, in the modular approach, independent subtrees are identified and the decision to use a state space oriented solution or a combinatorial solution is made for a subtree instead of for the fault tree as a whole. These independent subtrees are treated separately and their solutions are integrated to obtain the solution for the entire fault tree. The advantage of the modular approach is that it allows the use of state space oriented approach for those parts of a system that require them and the use of combinatorial methods for the more "well-behaved" parts (static parts) of the system, so that the efficiency of combinatorial solution can be retained where possible. In Section 38.7.2, an example of the modular approach that combines the use of the Markov chain solution for dynamic subtrees and binary decision diagrams based solution for static subtrees will be discussed in detail. The following three sections are devoted to the quantitative analysis techniques for static, dynamic, and noncoherent fault trees, respectively.

38.6 Static FTA Techniques

Quantitative analysis techniques for static fault trees using cutsets or binary decision diagrams will be discussed in this section.

38.6.1 Cutset Based Solutions

In Section 38.5.1, the top-down approach to generate the minimal cutsets from a static fault tree has been described. Each cutset represents a way in which the system can fail. So the system unreliability (denoted by U_{sys}) is simply the probability that all of the basic events in one or more minimal cutsets will occur. Let C_i represent a minimal cutset and there are n minimal cutsets for a system, thus we have:

$$U_{sys} = \Pr(\bigcup_{i=1}^{n} C_i) \cdot \tag{38.1}$$

Because the minimal cutsets are not generally disjoint, the probability of the union in (38.1) is not equal to the sum of the probabilities of the individual cutsets. Actually, for coherent systems, the sum of the individual cutsets gives an upper bound of the system unreliability since the intersection of the events from two minimal cutsets may be counted more than once. Several methods exist for the evaluation of (38.1) [10, 21, 33]. We describe two commonly used ones: inclusion-exclusion and sum of disjoint products.

38.6.1.1 Inclusion–Exclusion (I–E)

The I–E method is a generalization of the rule for computing the probability of the union of two events: $\Pr(A \cup B) = \Pr(A) + \Pr(B) - \Pr(A \cap B)$. It is given by the sum of probabilities of cutsets taken one at a time, minus the sum of probabilities of the intersection of cutsets taken two at a time, plus the sum of probabilities of the intersection of cutsets taken three at a time, and so on, until reaching an term which contains the probability of the intersection of all the cutsets [8]. The equation for representing the above procedure is:

$$U_{sys} = \Pr\{\bigcup_{i=1}^{n} C_i\} = \sum_{i=1}^{n} \Pr(C_i) - \sum_{i<j} \Pr(C_i \cap C_j) + \sum_{i<j<k} \Pr(C_i \cap C_j \cap C_k) \mp \ldots \pm \Pr(\bigcap_{j=1}^{n} C_j) \tag{38.2}$$

Consider the example system in Figure 38.9, there are three minimal cutsets: C_1={M1, M2}, C_2={M1, M3}, and C_3={M4}. The system unreliability can be calculated as:

$$U_{sys} = \Pr\{C_1 \cup C_2 \cup C_3) = \sum_{i=1}^{3} \Pr(C_i) - \Pr(C_1 \cap C_2) - \Pr(C_1 \cap C_3) - \Pr(C_2 \cap C_3) + \Pr(C_1 \cap C_2 \cap C_3)$$

The evaluation of (38.2) gives the exact system unreliability. As each successive summation term is calculated and included into the sum, the result alternatively overestimates (if the term is added) or underestimates (if the term is subtracted) the desired system unreliability. Hence, lower and upper bounds on the system unreliability can be determined by using only a portion of the terms in (38.2).

38.6.1.2 Sum of Disjoint Products (SDP)

The basic idea of the SDP method is to take each minimal cutset and make it disjoint with each preceding cutset using Boolean algebra, as shown in (38.3):

$$\bigcup_{i=1}^{n} C_i = C_1 \cup (\overline{C_1} C_2) \cup (\overline{C_1}\,\overline{C_2} C_3) \cup \ldots \cup (\overline{C_1}\,\overline{C_2}\,\overline{C_3} \ldots \overline{C_{n-1}} C_n) \tag{38.3}$$

$\overline{C_i}$ represents the negation of the set C_i. Because the terms in the right-hand side of (38.3) are disjoint, the sum of probabilities of these individual terms gives the exact system unreliability, that is,

$$U_{sys} = \Pr(\bigcup_{i=1}^{n} C_i) = \Pr(C_1) + \Pr(\overline{C_1} C_2) + \ldots + \Pr(\overline{C_1}\,\overline{C_2} \ldots \overline{C_{n-1}} C_n) \tag{38.4}$$

Consider the example system in Figure 38.9, the system unreliability using the SDP method will be calculated as: $U_{sys} = \Pr(C_1) + \Pr(\overline{C_1} C_2) + \Pr(\overline{C_1}\,\overline{C_2} C_3)$. Similar to the I–E method, lower and upper bounds on the system unreliability can be obtained by using a portion of the terms in (38.4) [8].

38.6.2 Binary Decision Diagrams

Binary decision diagrams (BDD) were, at first, used in the circuit design and verification as an efficient method to manipulate Boolean expressions [34, 35]. It has recently been adapted to solve a static fault tree model for the system reliability analysis. It has been shown by many studies [36–42] that in most cases, the BDD based method requires less memory and computational time than other methods. Thus, it provides an efficient way to analyze large fault trees.

A BDD is a directed acyclic graph (DAG) based on Shannon decomposition. Let f be a Boolean expression on a set of Boolean variables X and x be a variable of X, then the Shannon decomposition and its if-then-else (*ite*) format is:

$$f = x \cdot f_{x=1} + \overline{x} \cdot f_{x=0} = x \cdot F_1 + \overline{x} \cdot F_2 = ite(x, F_1, F_2)$$

The BDD has two sink nodes, each labeled by a distinct logic value 0, 1, representing the system being operational or failed, respectively. Each non-sink node is associated with a Boolean variable x and has two outgoing edges called *then*-edge (or 1-edge) and *else*-edge (or 0-edge), respectively. The two edges represent the two corresponding expressions in the Shannon decomposition as shown in Figure 38.10. In other words, each non-sink node in the BDD encodes a Boolean expression, or an *ite* format. One of the key

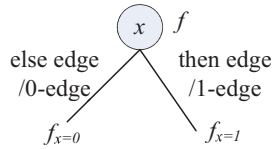


Figure 38.10. A non-sink node in BDD

characteristics of the BDD is the disjointness of $x \cdot f_{x=1}$ and $\bar{x} \cdot f_{x=0}$.

An ordered BDD (OBDD) is defined as a BDD with the constraint that variables are ordered and every source to sink path in the OBDD visits the variables in an ascending order. Further, a reduced OBDD (ROBDD) is an OBDD where each node represents a distinct Boolean expression. Two reduction rules will be introduced in Section 38.6.2.2 to obtain an ROBDD from an OBDD.

To perform a quantitative analysis of a static fault tree using the BDD method, we convert the fault tree to the BDD first, and then evaluate the resulted BDD to yield the system unreliability. In the following, we discuss the conversion and evaluation processes in detail.

38.6.2.1 Converting Fault Trees to BDDs

To construct an OBDD from a fault tree, the ordering of variables/components has to be selected first. The ordering strategy is very important for the OBDD generation, because the size of the OBDD will heavily depend on the order of input variables. A poor ordering can significantly affect the size of BDD, thus the reliability analysis solution time for large systems. Currently there is no exact procedure for determining the best way of ordering variables for a given fault tree structure. Fortunately, heuristics can usually be used to find a reasonable variable ordering [43].

After each variable is assigned a different order or index, a depth-first traversal of the fault tree is performed and the OBDD model is constructed in a bottom-up manner [44]. Specifically, the OBDDs are created for basic events first. Then these basic event OBDDs will be combined based on the logic operation of the current gate traversed. The resulted sub-OBDDs are further combined based on the logic operation of the traversed gate. The mathematical representation of the logic operation on two sub-OBDDs is described as follows.

Let $\Diamond$ represent any logic operation (AND/OR). Let the *ite* format for Boolean expressions G and H, representing two sub-OBDDs, be: $G = ite(x, G_{x=1}, G_{x=0}) = ite(x, G_1, G_2)$ and $H = ite(y, H_{x=1}, H_{x=0}) = ite(y, H_1, H_2)$.

Then:

$$G \Diamond H = ite(x, G_1, G_2) \Diamond ite(y, H_1, H_2) = \begin{cases} ite(x, G_1 \Diamond H_1, G_2 \Diamond H_2) & index(x) = index(y) \\ ite(x, G_1 \Diamond H, G_2 \Diamond H) & index(x) < index(y) \\ ite(y, G \Diamond H_1, G \Diamond H_2) & index(x) > index(y) \end{cases} \quad (38.5)$$

The same rules can be used for logic operation between sub-expressions until one of them becomes a constant expression '0' or '1'. Note that Boolean algebra ($1+x=1$, $0+x=x$, $1 \cdot x=x$, $0 \cdot x=0$) is applied to simplify the representation when one of the sub-OBDDs is a constant expression '0' or '1'.

To illustrate the fault tree to BDD conversion process, we present the construction of the OBDD from the fault tree in Figure 38.9 (a). Assume the variable ordering is M1<M2<M3<M4. Consider the subtree rooted at the OR gate G3; the first path traversed leads to the basic event M2. This means that the OR gate G3 will be applied once OBDDs are built for all the inputs of G3, that is, M2 and M3. Figure 38.11 shows the initial OBDDs for the two basic events M2 and M3 as well as the OBDD resulting from the application of the logic OR gate G3. M2 is the root of the resulted OBDD since it has a lower index than M3.

Figure 38.12 shows the OBDD resulting from the application of the logic AND gate G2 on the OBDD of Figure 38.11 and the OBDD for the basic event M1. M1 is the root of the resulted OBDD since it has a lower index than M2.

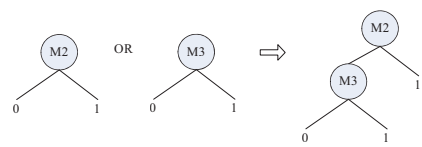


Figure 38.11. OBDD construction up to G3

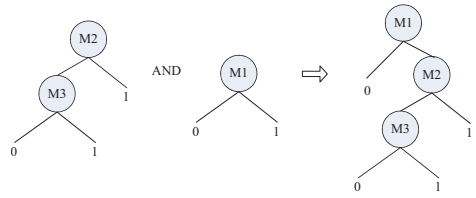


Figure 38.12. OBDD construction up to G2

Figure 38.13 shows the OBDD resulting from the application of OR gate G1 on the OBDDs which represent the inputs of G1, *i.e.,* the OBDD generated in Figure 38.12 and the OBDD for the basic event M4. Since G1 is the top gate of the fault tree, the OBDD in Figure 38.13 gives the full OBDD representing the entire fault tree of Figure 38.9 (a). This graph demonstrates that if both M1 and M2 fail; or if M1 fails, M2 does not fail, and M3 fails; or if M1 fails, M2 and M3 do not fail, and M4 fails; or if M1 does not fail and M4 fails, the entire system fails.

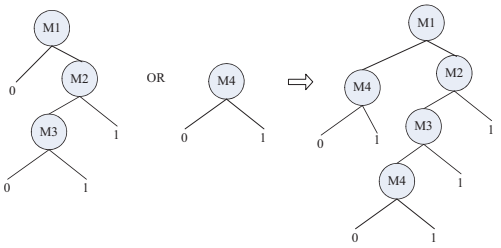


Figure 38.13. OBDD construction up to G1

38.6.2.2 Generating a Reduced OBDD (ROBDD)

As the OBDD is built, the following two reduction rules can be applied to ensure that the OBDD that results is minimal for the chosen ordering:

- Rule#1: isomorphic subtrees are merged since two isomorphic subtrees encode the same Boolean expression. Thus at least one is superfluous and the isomorphic sub-OBDDs can be merged as one sub-OBDD (Figure 38.14). For example, the two sub-BDDs rooted at node M4 in Figure 38.13 are isomorphic and can be merged. Figure 38.15 shows the ROBDD for the fault tree of Figure 38.9 (a) after applying this reduction rule to the OBDD in Figure 38.13.

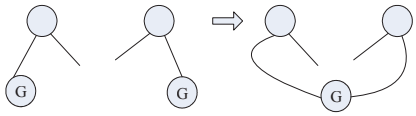


Figure 38.14. Rule#1: merging isomorphic sub-OBDDs

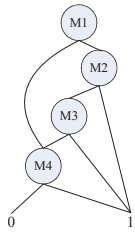


Figure 38.15. An example ROBDD

- Rule#2: deletion of useless nodes. A node encoding a function of form $(x \wedge G) \vee (\bar{x} \wedge G)$ is superfluous and thus can be deleted from the model because the function is simply equivalent to *G* (Figure 38.16).

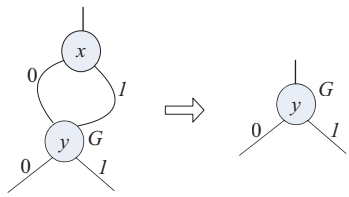


Figure 38.16. Rule#2: deleting useless nodes

38.6.2.3 Calculating System Unreliability

The final BDD model must be evaluated to obtain the system unreliability. Observing the BDD (Figure 38.15) generated for the fault tree in Figure 38.9(a), it is easy to find that each non-sink node in the BDD represents a component that can fail, and each path from the root to a leaf/sink node represents a disjoint combination of component failures and non-failures. If a path leads from a node to its then-edge (or right branch), then the failure of the component should be considered for that path. If a path leads from a node to its else-edge (or left branch), then the non-failure of the component should be considered for that path. If the sink node for a path is labeled with a "1", then the path leads to system failure; if the sink is labeled with a "0" then the path represents the

system being functioning. The probabilities associated with the then-edges on each path are the failure probabilities of corresponding components; the probabilities associated with the else-edges on each path are the operational probabilities of the corresponding components. Because all the paths are disjoint, the system unreliability is given by the sum of the probabilities for all the paths from the root to a sink node labeled "1", or the system reliability is given by the sum of the probabilities for all the paths from the root to a sink node labeled "0".

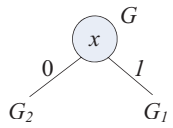


Figure 38.17. An ROBDD branch

The recursive algorithm for evaluating the ROBDD is described as follows. Consider a ROBDD branch G rooted at node x in Figure 38.17. The 1-edge of node x is associated with the failure probability of the component $q(x)$. The 0-edge is associated with the operational probability of the component $1\text{-}q(x)$. The unreliability concerning the sub-BDD G is calculated as: $U(G) = q(x)U(G_1)+[1\text{-}q(x)]U(G_2)$. When x is the rood node of the entire system BDD, $U(G)$ gives the entire system unreliability. The exit condition of this recursive algorithm is: if $G = 0$, then $U(G) = 0$; if $G = 1$, then $U(G) = 1$.

38.6.2.4 Variations of BDDs

Recently the BDD model has been combined with the multistate concept to analyze the reliability of systems subject to imperfect coverage behaviour [45–47], where an uncovered component fault can lead to extensive damage to the entire system despite the presence of fault-tolerant mechanisms [8]. There are three states for a system with imperfect coverage and its components: operation, covered failure and uncovered failure [8]. Readers may refer to Chapter 22 for detailed discussion on imperfect fault coverage. In the multistate BDD based method, each state of the component is represented using a Boolean variable indicating whether the component is in that particular state and the system BDD is generated using these Boolean variables. Because statistical-dependence exists among variables representing different states of the same component, special treatments are needed to address the dependence when applying the traditional Boolean algebra for BDD evaluation [46, 47]. In [42, 48] a similar similar idea was applied to the analysis of general multistate systems in which both the system and its components may exhibit three or more than three performance levels (or states) varying from perfect operation to complete failure. However, the disadvantage of the BDD-based method is that many Boolean variables must be dealt with and dependence among variables representing different states of the same component must be addressed.

To decrease the number of variables involved in the generation and evaluation of the system model, Xing and Dugan first adapted multiple-valued decision diagrams (MDD) [49] for the reliability analysis of fault tolerant systems with imperfect coverage [50, 51]. In their work, a MDD is a directed acyclic graph with three sink nodes each labeled by a distinct logic value 0, 1, 2, representing the system being in the operation, covered failure, and uncovered failure state, respectively. Each non-sink node representing a three-state component is labelled by a ternary-valued variable and has three outgoing edges; one corresponding to each logic value or component state. According to the special characteristic of an uncovered failure, *i.e.*, it leads to the entire system failure [8], a set of special *ternary-valued algebra* rules was developed for performing the logic AND/OR operation on the two basic events. Xing and Dugan showed that the MDD-based method provides smaller models and a much neater and simpler evaluation algorithm for analyzing systems subject to imperfect coverage than the BDD-based method. However, the MDD and rules developed in [50, 51] apply only to systems subject to imperfect coverage, in which both the system and its components have the same set of three states (operation, covered failure, and uncovered failure), and once a component is in the uncovered failure state, the entire system is in that state too. They cannot apply to the general multistate systems in

which the component states may not be consistent with the system states, and characteristics of each state can be nondeterministic.

Recently, a new modelling approach called multistate multivalued decision diagrams (MMDD) has been proposed, which provides an efficient and effective means for analyzing general large-scale multistate systems [52]. Different from the MDD model used in [50, 51], which can have more than two sink nodes representing the system being in each of the multiple states, a MMDD model can have two and only two sink nodes representing the system being or not being in a specific state. Results of case studies in [52] show that the MMDD based method provides smaller models in terms of the number of nodes and much neater and simpler generation and evaluation processes than the BDD-based approach proposed in [42]. Moreover, similar to the BDD-based method, the MMDD model can implicitly represent the sum of disjoint products, each of which indicates a disjoint combination of component states that cause the system to be in a specific state.

38.7 Dynamic FTA Techniques

38.7.1 Markov Chains

Dynamic fault trees (DFT) extend traditional FTA to include dynamic system behavior such as sequence dependence and shared pool of resources. The DFT model includes special purpose gates (dynamic gates described in Section 38.4.2) to incorporate the dynamic behavior into Markov chains, which are used for the solution to the system unreliability analysis.

The two main concepts in the Markov model are system states and state transitions. The state of a system represents a specific combination of system parameters that describe the system at any given instant of time. For representing the system reliability, each state of the Markov model generally represents a distinct combination of faulty and fault free components. The state transitions govern the changes of a state that occur within a system. As time passes and failures occur, the system goes from one state to another until one of the absorbing states (usually the system failure states) is reached. The state transitions are characterized by parameters such as failure rates, fault coverage factors, and repair rates [53].

Solving a Markov model consists of solving a set of differential equations: $\boldsymbol{AP}(t) = \boldsymbol{P}'(t)$. The specific form is:

$$\begin{bmatrix} -\alpha_{11} & \alpha_{21} & \alpha_{31} & \dots & \alpha_{n1} \\ \alpha_{12} & -\alpha_{22} & \alpha_{32} & \dots & \alpha_{n2} \\ \alpha_{13} & \alpha_{23} & -\alpha_{33} & \dots & \alpha_{n3} \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_{1n} & \alpha_{2n} & \alpha_{3n} & \dots & -\alpha_{nn} \end{bmatrix} \bullet \begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ \dots \\ P_n(t) \end{bmatrix} = \begin{bmatrix} P_1'(t) \\ P_2'(t) \\ P_3'(t) \\ \dots \\ P_n'(t) \end{bmatrix}$$

where $\alpha_{jk}, j \neq k$ is the transition rate from state j to state k. The diagonal element α_{jj} in the matrix $\boldsymbol{A}$ is the sum of departure rates from state j, that is, $\alpha_{jj} = \sum_{k=1,k\neq j}^{n} \alpha_{jk}$. Thus, the sum of each column of $\boldsymbol{A}$ is 0. $P_i(t)$ is the probability of system being in state i at time t, and n represents the number of states presented in the Markov model.

To solve the differential equations, Laplace transform is typically applied [4]. The solution includes the probability of the system being in each state. The system unreliability can be calculated by adding the probability of being each failure state: $\sum_{\forall F} P_{F_i}(t)$, where $P_{F_i}(t)$ is the probability of system being in the failure state F_i at time t.

Markov model has more power as a solution method than the combinatorial methods in that it can solve system with dynamic and dependent behaviors. However, Markov model has the significant disadvantage that its size grows exponentially as the size of the system increases. This rapid growth of the number of states may lead to intractable models. Therefore, many researchers made efforts to the approximate bounding methods where only a portion of the state space of Markov chain is generated [54, 55]. In addition, Markov model assumes *exponential* time-to-failure distribution, whereas, combinatorial methods can be applied to any arbitrary failure distribution. Since Markov and combinatorial approaches both have their *pros* and *cons*, a dynamic fault tree modular approach has been proposed to combine both solutions in the system reliability analysis (refer to the following section for details).

38.7.2 The Modular Approach

Gulati and Dugan [30] presented an exciting hybrid approach, called the modular approach, for the efficient analysis of both static and dynamic fault trees. It provides a combination of BDD solution for static subtrees and Markov chain solution for dynamic subtrees coupled with the detection of independent subtrees. The modular approach allows the use of Markov models for dynamic parts of a system that require them, and use of combinatorial methods for static parts of the system to retain the efficiency of combinatorial solutions where possible.

Specifically, in the modular approach, the fault tree is divided into independent subtrees (subtrees that share no input events) using a fast and efficient algorithm [56]. These independent subtrees are further identified as static or dynamic depending on the relationships between the input events. Static subtree gates express the failure criteria in terms of combinations of events. Dynamic subtree gates express the failure criteria in terms of both combinations of events and order of occurrence of input events.

As an example, the modular approach is applied to the fault tree in Figure 38.18 [57]. The fault tree is divided into four independent subtrees: two static subtrees and two dynamic subtrees, as indicated in Figure 38.18. The static subtrees can be solved using the combinatorial BDD-based method. The dynamic subtrees can be solved using the Markov chain based method.

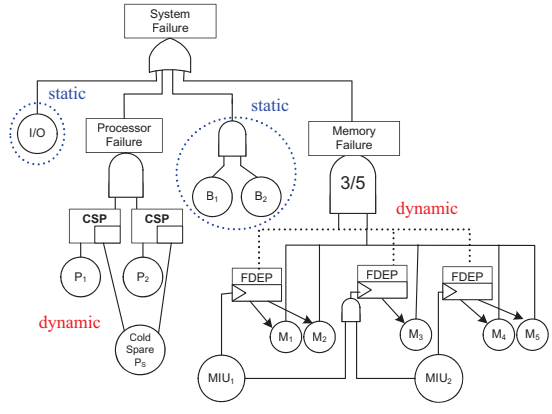


Figure 38.18. The modular approach [57]

Note that modularization is a recursive process as subtrees might themselves contain independent subtrees [30]. Solutions of various independent subtrees are integrated using a relatively straightforward and recursive algorithm to obtain the solution to the entire system.

38.8 Noncoherent FTA Techniques

38.8.1 Prime Implicants

The traditional approach to analyzing a non-coherent system is using prime implicants in the place of minimal cutsets [58]. A prime implicant in a fault tree is a minimal set of basic events whose occurrence or non-occurrence leads to the occurrence of the TOP event (system being unavailable). Similar to the FTA using cutsets, either I–E or SDP method can be applied to obtain the system unavailability based on prime implicants. We use two examples to illustrate the prime implicant based method for the analysis of noncoherent fault trees.

In the first example, we consider a noncoherent fault tree containing an Exclusive OR gate with two inputs: x and y. There are two prime implicants: $I_1 = \{x, \bar{y}\}$ and $I_2 = \{\bar{x}, y\}$. Applying the I-E method, we obtain the expression of system unavailability as:

$$\begin{aligned} \Pr(I_1 \cup I_2) &= \Pr(I_1) + \Pr(I_2) - \Pr(I_1 I_2) \\ &= \Pr(x\bar{y}) + \Pr(\bar{x}y) - \Pr(x\bar{y}\bar{x}y) \\ &= \Pr(x)\Pr(\bar{y}) + \Pr(\bar{x})\Pr(y) - 0 \\ &= \Pr(x)(1-\Pr(\bar{y})) + (1-\Pr(\bar{x}))\Pr(y) \end{aligned} \tag{38.6}$$

Note that $\Pr(I_1 I_2)$ is zero since $I_1 I_2$ contains disjoint events: x and $\bar{x}$; y and $\bar{y}$.

In the second example, we consider the traffic light system used at the crossing of two mono-directional roads (Figure 38.19) [14, 59]. Assume the light functions properly and is RED for road 1 and GREEN for road 2. We define three basic events: event a –car A fails to stop; event b – car B fails to stop; and event c – car C fails to continue. The system has three prime implicants:

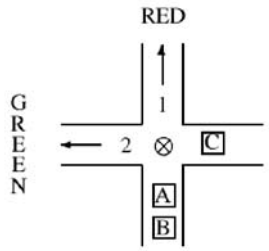


Figure 38.19. Traffic light system

- $I_1 = \{a, \bar{c}\}$: the accident occurs when car *A* fails to stop (*a*) and car *C* moving towards road 2 is crossing ($\bar{c}$);
- $I_2 = \{\bar{a}, b\}$: the accident occurs when car *A* acts properly and stops ($\bar{a}$) and car *B* fails to stop (*b*);
- $I_3 = \{b, \bar{c}\}$: the accident occurs when car *B* fails to stop (*b*) and car *C* continues through the light ($\bar{c}$), no matter what car *A* does.

Define the probability of an event *a* occurring as q_a, and not occurring as p_a. Applying the I–E method, the expression for computing the occurrence probability of an accident is:

$$\begin{aligned}
&\Pr(I_1 \cup I_2 \cup I_3) \\
&= \Pr(I_1) + \Pr(I_2) + \Pr(I_3) - \Pr(I_1 I_2) - \Pr(I_1 I_3) \\
&\quad - \Pr(I_2 I_3) + \Pr(I_1 I_2 I_3) \\
&= \Pr(a\bar{c}) + \Pr(\bar{a}b) + \Pr(b\bar{c}) - 0 - \Pr(a\bar{c}b\bar{c}) \\
&\quad - \Pr(\bar{a}bb\bar{c}) + 0 \\
&= q_a p_c + p_a q_b + q_b p_c - q_a q_b p_c - p_a q_b p_c
\end{aligned} \tag{38.7}$$

38.8.2 Importance Measures

Considerable research efforts have been expended in the component importance analysis for coherent systems and many different importance measures have been proposed for coherent system analysis [4, 60, 61]. However, these measures cannot be directly applied to the analysis of noncoherent systems. In [62, 63] it was proposed to extend four commonly used importance measures for noncoherent systems: 1) Birnbaum's measure [64], 2) component criticality measure [4], 3) Fussell–Vesely measure [65], and 4) initiator and enabler measure [66]. Because Birnbaum's measure is central to the other three importance measures, we discuss it in detail in this section. Readers may refer to [63] for details on the definitions and applications of the other three measures.

Birnbaum's measure of component importance is defined as the probability that a component is critical to system failure, or the probability that the system is residing in a critical state for a component such that its failure causes the system failure [64]. Define:

- $B_i(\underline{q}) \equiv$ Birnbaum's measure of component *i*.
- $q_i(t) \equiv$ the probability that a component *i* is not working at time *t*, it can be either unreliability for a non-repairable system or unavailability for a repairable system.
- $p_i(t) \equiv$ the probability that a component *i* is working at time *t*, *i.e.*, $1 - q_i(t)$.
- $\underline{q} \equiv$ a vector of component unavailability or unreliability for all other components except *i*.
- $Q_{sys}(1_i, \underline{q}) \equiv$ the probability that the system fails with component *i* failed.
- $Q_{sys}(0_i, \underline{q}) \equiv$ the probability that the system fails with component *i* functioning.
- $Q_{sys}(t) \equiv$ the probability that the system fails at time *t*.

The Birnbaum's measure can be expressed as:

$$B_i(\underline{q}) = Q_{sys}(1_i, \underline{q}(t)) - Q_{sys}(0_i, \underline{q}(t)) = \frac{\partial Q_{sys}(t)}{\partial q_i(t)} \tag{38.8}$$

When dealing with a coherent system, the system failure can only be caused by component failures. Therefore, a component in a coherent system can only be *failure-critical*. However, when dealing with a noncoherent system, the system failure can be caused, not only by the failure of a component (referred to as an event *i*), but also by the repair of the component (referred to as event $\bar{i}$). Thus, a component in a noncoherent system can be *failure-critical* or *repair-critical*. These two criticalities must be considered separately because a component can exist in only one state at any time.

Birnbaum's measure for a noncoherent system is given by:

$$B_i(\underline{q}) = B_i^F(\underline{q}) + B_i^R(\underline{q}) \tag{38.9}$$

where $B_i^F(\underline{q})$ represents the component *failure-criticality*, specifically, the probability that the system is in a working state such that the failure of component *i* would cause the system failure; $B_i^R(\underline{q})$ represents the component *repair-criticality*, specifically, the probability that the system is in a working state such that the repair of component *i* would cause the system failure. It has been shown that the failure and repair criticalities can be calculated separately by differentiating $Q_{sys}(t)$ with respect to q_i and p_i, respectively [62]:

$$B_i^F(\underline{q}) = \frac{\partial Q_{sys}(t)}{\partial q_i(t)}, \quad B_i^R(\underline{q}) = \frac{\partial Q_{sys}(t)}{\partial p_i(t)} \tag{38.10}$$

For example, consider the traffic light system in Section 38.8.1. The system unavailability is given in (38.7): $Q_{sys}(t) = q_a p_c + p_a q_b + q_b p_c - q_a q_b p_c - p_a q_b p_c$. According to (38.10), the failure criticality and repair criticality for event *a* are:

$$B_a^F(\underline{q}) = \frac{\partial Q_{sys}(t)}{\partial q_a(t)} = p_c - q_b p_c = p_c(1-q_b) = p_c p_b$$

$$B_a^R(\underline{q}) = \frac{\partial Q_{sys}(t)}{\partial p_a(t)} = q_b - q_b p_c = q_b(1-p_c) = q_b q_c$$

According to (38.9), the Birnbaum's measure of event *a* is: $B_a(\underline{q}) = B_a^F(\underline{q}) + B_a^R(\underline{q}) = p_b p_c + q_b q_c$.

38.8.3 Failure Frequency

Perhaps, the first paper on frequency calculations of noncoherent systems is by Inagaki and Henley [58]. Their method is similar to the method proposed by Vesely for coherent system analysis [67]. For noncoherent systems, prime implicants will be used in the place of minimal cut sets for the failure frequency calculation. According to the method proposed in [58], the expected number of failures within $[t, t + \Delta t]$ is:

$$N(t,t+\Delta t) = \Pr\left\{\bigcup_{i=1}^{p}\theta_i\right\} - \Pr\left\{B\bigcup_{i=1}^{p}\theta_i\right\} \tag{38.11}$$

$$\text{where } B \equiv \bigcup_{i=1}^{p} d_i \text{ and } B\bigcup_{i=1}^{p}\theta_i \equiv B\bigcap\left(\bigcup_{i=1}^{p}\theta_i\right)$$

If Δt is small and is equivalent to the time unit, $N(t,t+\Delta t)$ is equivalent to the failure frequency denoted by $\omega(t)$. It should be noted that $\omega \equiv \omega(t) = \lim_{\Delta t \to 0} \frac{N(t,t+\Delta t)}{\Delta t}$.

Although the method proposed in [58] produces correct results for noncoherent systems, it is unnecessarily complex. The evaluation of (38.11) involves an *NP* problem within each step of another *NP* problem. Therefore, even for the simple example problem considered in [58], a complex procedure is required to solve it. In this section, we describe a simple rule-based method proposed in [59]. The method converts the expression for system unavailability *U* obtained using the calculation procedure of [58] into an expression for ω. The general form of the expression for *U* is the sum of products form: $U = \sum_{i=1}^{m} c_i T_i$, where *m* is the number of product terms, T_i is the product of component availabilities and unavailabilities, and c_i is an integer coefficient that can be negative or positive. For example, in (38.7), the terms are:

i	1	2	3	4	5
c_i	1	1	1	-1	-1
T_i	$q_a p_c$	$p_a q_b$	$q_b p_c$	$q_a q_b p_c$	$p_a q_b p_c$

Each term T_i is in the form of $q_j q_k \ldots p_m p_n$. The general form of T_i is: $T_i = \prod_{j \in F_i} q_j \prod_{k \in S_i} p_k$, where F_i and S_i are the set of component indices corresponding to the unavailability and availability terms in T_i, respectively.

The rule for converting *U* into ω is to multiply every term $c_i T_i$ with the effective rate term $R_i = \sum_{j \in F_i} \alpha_j + \sum_{k \in S_i} \beta_k$, where $\alpha_i = \frac{\omega_i}{q_i} = \frac{p_i \lambda_i}{q_i}$ and $\beta_i = \frac{\nu_i}{p_i} = \frac{q_i \mu_i}{p_i}$. If the system is in the steady-state, then $\alpha_i = \mu_i$ and $\beta_i = \lambda_i$. Refer to [59] for the proof. In simple terms, if T_i is in the form of $q_j q_k \ldots p_m p_n$, then multiply that term with $(\alpha_j + \alpha_k + \ldots + \beta_m + \beta_n)$. Hence, we have: $\omega = c_i T_i R_i$. For example, the R_i terms for (38.7) are:

i	c_i	T_i	R_i
1	1	$q_a p_c$	$\alpha_a + \beta_c$
2	1	$p_a q_b$	$\beta_a + \alpha_b$
3	1	$q_b p_c$	$\alpha_b + \beta_c$
4	-1	$q_a q_b p_c$	$\alpha_a + \alpha_b + \beta_c$
5	-1	$p_a q_b p_c$	$\beta_a + \alpha_b + \beta_c$

Therefore, the failure frequency of the traffic light system (Figure 38.19) is:

$$\omega = q_a p_c(\alpha_a + \beta_c) + p_a q_b(\beta_a + \alpha_b) + q_b p_c(\alpha_b + \beta_c) - q_a q_b p_c(\alpha_a + \alpha_b + \beta_c) - p_a q_b p_c(\beta_a + \alpha_b + \beta_c)$$

38.9 Advanced Topics

38.9.1 Component Importance Analysis

Results from fault tree reliability analysis have been key contributors to system design and tuning activities. However, reliability analysis tells only part of the story; in particular, reliability analysis gives very little information about each individual component's contribution to the entire system failure. Follow-up questions such as "How does a change in one component's reliability affect the entire system reliability?", "How can the entire system reliability be best improved given limited resources?" have to be answered. These and similar questions can be best answered using results of component importance analysis (also called sensitivity analysis) [68].

The importance analysis helps the designer to identify which components contribute most to the system reliability and thus these components would be good candidates for efforts leading to improving the entire system reliability. From the maintenance point of view, the analysis would, by means of a list, tell the repairperson in which order to check the components that may have caused the system failure. Ideally speaking, the maintenance-oriented importance analysis [61] will rank the component whose repair will hasten the system recovery the most, the highest. Section 38.8.2 presents the component importance analysis for noncoherent systems. Xing [72] considers the importance analysis of components in a generalized phased-mission system subject to modular imperfect coverage. Here, we discuss the component importance analysis in the general term.

Two classes of component importance measures have been proposed for the case where the support model is a fault tree: structural-importance (SI) measures and reliability-importance (RI) measures. The SI measures assess the importance of a component to the system operation or reliability by virtue of its position in the fault tree structure, without considering the reliability of the component [70]. Thus, they can be used even if the component reliability is unknown or subject to changes. However, the SI measures cannot distinguish between components that occupy similar structural positions but have drastically different component reliabilities. On the other hand, the RI measures consider both the position of the component in the system and the reliability of the component in question. Thus, the RI measures can generally provide more useful information for generating the ranked list than the SI measures.

Xing [61] studied seven different RI measures, including conditional probability (CP) [71], risk achievement worth (RAW) [60], risk reduction worth (RRW) [60, 70], diagnostic importance factor (DIF), Birnbaum's measure (BM) [4], the criticality importance factor (CIF) [4], and the improvement potential (IP). Refer to [61] for their mathematical definitions as well as physical interpretations. The study in [61] compared the performance of these measures in assisting the system design and maintenance activities. Results of the study show that CP, RAW, and BM may induce misleading conclusions in terms of guiding the system maintenance, though some of these measures serve a good indicator for selecting components that are the best candidates for efforts leading to improving the entire system reliability. RRW, CIF, and IP generally induce reasonable conclusions. However, they give the same importance result for all components in a parallel structure irrespective of the (drastic) difference among the component reliabilities. In addition, the CIF and IP measures become impractical for large dynamic systems because they must be solved using Markov approaches which suffer from the

well-known state explosion problem. Furthermore, the computation of both CIF and IP measures involves the assessment of BM measure that involves simultaneously solving a set of differential equations (the number of equations is the same as the number of states present in the Markov model) for the state occupation probabilities and a much larger set of partial differential equations for the component importance analysis [73]. The solutions to those equations are computationally intensive.

Based on the experimental results obtained in [61], the DIF measure is the most informative and appropriate measure for the maintenance-oriented importance analysis among the nine measures. The DIF measure generally produces the ranking that is consistent with those produced by using the RRW, CIF, and IP measures; it accounts for the effects of exceptionally unreliable component; it can always distinguish components that occupy similar structural positions (for both series and parallel structures) but have different reliabilities.

38.9.2 Common Cause Failures

Common cause failures (CCF) are multiple dependent component failures within a system that are a direct result of a shared root cause or common cause (CC), such as sabotage, flood, earthquake, lightening, power outage, sudden changes in environment, design weaknesses, or human errors. According to [74], CCF are defined as "A subset of dependent events in which two or more component fault states exist at the same time, or in a short time interval, and are direct results of a shared cause." CCF typically occur in systems designed with redundancy techniques, which are characterized by the use of *s*-identical components [75]. It is critical to consider CCF in the system reliability analysis because failure to consider CCF can lead to overestimated system reliability [76, 77].

Considerable research efforts have been expended in the study of CCF for the system reliability modeling and analysis. However, most of these CCF models suffer from various limitations, such as being concerned with a specific system structure [78, 79]; applicable only to systems with exponential time-to-failure distributions [80–82]; being subject to combinatorial explosion as the redundancy level of the system increases [83, 84]; limiting analysis to components being affected by at most a single common-cause [75, 77]; having a single CC that affects all components of a system [79, 85]; or defining CC as being *s*-independent or mutually exclusive [86]. Xing [39] proposed a generic CCF model that addressed these restrictions of the existing CCF models in the reliability analysis of computer network systems by allowing for multiple CC that can affect different subsets of system components, and which can occur *s*-dependently.

Xing [87] utilized the generalized CCF model of [39] and incorporated this CCF model into dynamic fault trees using a new dynamic gate, called CCF gate, for the reliability analysis of hierarchical systems subject to CCF. Moreover, an efficient decomposition and aggregation (EDA) approach was proposed for incorporating CCF into the reliability analysis of hierarchical systems. The basic idea of the EDA approach is to decompose an original reliability problem into a number of reduced reliability problems according to the total probability theorem. The effects of CCF are factored out through the reduction. The reduced problems are represented in a dynamic fault tree model by the CCF gate, which is modeled after the FDEP gate [8]. These reduced problems can be solved using any reliability evaluation approaches that ignore CCF; for example, an efficient one is the BDD based method (Section 38.6.2). The final reliability measure is obtained by aggregating the results of each reduced problem.

Specifically, the EDA approach can be applied in the following three steps:

Step 1: Building common-cause event (CCE) space. Assume the system is subject to *m* common-causes (CC). The *m* CC partition the event space into the 2^m disjoint subsets, each called a CCE:

$$CCE_1 = \overline{CC_1} \cap \overline{CC_2} \cap \ldots \cap \overline{CC_m},$$
$$CCE_2 = CC_1 \cap \overline{CC_2} \cap \ldots \cap \overline{CC_m},$$
$$\ldots\ldots,$$
$$CCE_{2^m} = CC_1 \cap CC_2 \cap \ldots \cap CC_m.$$

A space called "CCE space" (denoted by Ω_{CCE}) is built over this set of collectively exhaustive and mutually exclusive CCE that can occur in the system, *i.e.*, $\Omega_{CCE} = \{CCE_1, CCE_2, ..., CCE_{2^m}\}$. If $\Pr(CCE_j)$ denotes the occurrence probability of CCE_j, then we have $\sum_{j=1}^{2^m} \Pr(CCE_j) = 1$ and $CCE_i \cap CCE_j = \phi$ for any $i \neq j$. Define a common-cause group (CCG) as a set of components that are cause to fail due to the same elementary CC. Let S_{CCE_i} denote the set of components affected by CCE_i, then S_{CCE_i} is simply the union of CCG whose corresponding CC occur. For example, define $CCE_i = \overline{CC}_1 \cap \overline{CC}_2 \cap CC_3$ as a CCE in a system with three elementary CC; S_{CCE_i} is then equal to CCG_3 because CC_3 is the only active elementary CC. For another example, consider $CCE_j = \overline{CC}_1 \cap CC_2 \cap CC_3$, S_{CCE_i} is then equal to $CCG_2 \cup CCG_3$ because both CC_2 and CC_3 are active elementary CC.

Step 2: Generating and solving reduced problems. Based on the CCE space built in step 1 and the total probability theorem, the system unreliability can be calculated as:

$$U_{sys} = \sum_{i=1}^{2^m} [\Pr(\text{system fails} \mid CCE_i) \bullet \Pr(CCE_i)] = \sum_{i=1}^{2^m} [U_i \bullet \Pr(CCE_i)] \quad (38.12)$$

As defined in (38.12), U_i is a conditional probability that the system fails conditioned on the occurrence of CCE_i. The evaluation of U_i is actually a reduced reliability evaluation problem in which the set of components affected by CCE_i do not appear. Specifically, in the system DFT model, each basic event (the failure of a component) that appears in S_{CCE_i} will be replaced by a constant logic value "1" (*true*). After the replacement, a Boolean reduction can be applied to the system DFT to generate a simpler DFT in which all the components of S_{CCE_i} do not appear. Most importantly, the evaluation of the reduced DFT can proceed without further consideration of CCF. The studies in [87] showed that most of DFT after reduction become trivial to solve. In addition, given the fact that systems are usually subject to a small number (m) of root common causes, and considering the parallel processing capability of modern computing systems, even though there are 2^m reduced problems involved in the EDA approach, the overall solution complexity is still low.

Step 3: Integrating for the final result. After obtaining the results for all the reduced problems in (38.12), we integrate them with the occurrence probabilities of CCE, *i.e.*, $\Pr(CCE_i)$ to obtain the final unreliability of the system subject to CCF.

Advantages offered by the EDA approach include: 1) it enables the analysis of multiple CC that can affect different subsets of components within the system, and which may occur *s*-dependently; 2) it allows reliability engineers to use their favorite software package that ignores CCF for computing reliability, and adjust the input and output of the program slightly to produce the system reliability considering CCF. Due to the separation of CCF from the solution combinatorics, the EDA approach has higher computational efficiency and is easier to implement than other potential methods such as Markov methods, which can accommodate CCF by expanding the state space and number of transitions, worsening the state explosion problem [30].

38.9.3 Dependent Failures

In FTA, a common assumption made is that all system components fail independently. However, this is not necessarily true in practical systems. CCF and failure dependence described in the FDEP gate are two examples of dependent failures.

In general, there are two types of dependencies: *positive dependence* and *negative dependence* [4]. *Positive dependence* occurs if the failure of one component leads to an increased tendency for another component to fail. For example, when several components share a common load, the failure of one component may lead to an increased load on the remaining components and thus may

lead to an increased likelihood of failure. N*egative dependence* occurs if the failure of a component leads to a reduced tendency for another component to fail. For example, if an electrical fuse fails open such that downstream circuit is disconnected, the load on the electrical devices in this circuit is removed and thus their likelihood of failure is reduced.

In probability theory, we say that two events E1 and E2 are independent if $Pr(E1 \cap E2) = Pr(E1) \cdot Pr(E2)$ or $Pr(E1|E2) = Pr(E1)$ and $Pr(E2|E1) = Pr(E2)$, meaning that the occurrence of one event has no influence on the occurrence of the other event. A component has a positive dependence when $Pr(E1|E2) > Pr(E1)$ and $Pr(E2|E1) > Pr(E2)$, such that $Pr(E1 \cap E2) > Pr(E1) \cdot Pr(E2)$. A component has a negative dependence when $Pr(E1|E2) < Pr(E1)$ and $Pr(E2|E1) < Pr(E2)$, such that $Pr(E1 \cap E2) < Pr(E1) \cdot Pr(E2)$.

Besides CCF discussed in Section 38.9.2 and functional dependence discussed in Section 38.4.2.1, another type of dependent failure we would like to briefly mention here is cascading failures, also called propagating failures. According to [4], cascading failures are "multiple failures initiated by the failure of one component in the system that results in a chain reaction or domino effect." Cascading failures are common in power grids when one of the elements fails (completely or partially) and shifts its load to nearby elements in the system. Those nearby elements are then pushed beyond their capacity so they become compromised and shift their load onto other elements [88]. Cascading failures may be modeled and analyzed by event trees and fault trees.

38.9.4 Disjoint Events

Disjoint events, also referred to as mutually exclusive events, are events that cannot occur at the same time. For example, two failure modes of a relay: "stuck-open" and "stuck-closed" cannot occur simultaneously. This event dependence can be easily modeled using Markov chains. However, due to the well-known state explosion problem, the Markov chain solution is only practical for small systems. Another alternative is to approximate the mutually exclusive events in a fault tree by stochastically independent events. Thus cutsets containing more than one of mutually exclusive events can occur, leading to incorrect quantitative reliability evaluation, although the errors are usually insignificant. Twigg *et al*. [19] proposed an accurate method to model the mutually exclusive events by converting each of the mutually exclusive events to a subtree that is constructed from ordinary and stochastically independent events as well as logic AND, OR, and NOT gates. Next, we review the basics of the approach through an example fault tree with two disjoint events from [19].

Consider the fault tree in Figure 38.20. Events D1 and D2 are two disjoint events representing two disjoint failure modes of a component D. B and C represent two independent component failure events. Figure 38.20 actually models the two disjoint failure events as independent events, which means that the two failure events D1 and D2 may occur at the same time, leading to errors in reliability calculation. This can also be seen from the cutsets generation.

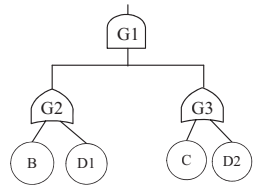


Figure 38.20. Fault tree without modeling disjoint

Apply the top-down approach described in Section 38.5.1, we obtain the minimal cutsets for this fault tree as: {D1, C}, {D2, B}, {B,C}, and {D1, D2}. The minimal cutset {D1, D2} representing the simultaneous occurrence of the two disjoint failure events appears because the dependence between those two events has not been modeled in the fault tree analysis. In the solution of [19], each disjoint event in the original fault tree will be replaced with a disjoint subtree as shown in Figure 38.21.

Specifically, the basic event D1 is replaced with a subtree encoding the Boolean expression of $D1=A \cap A1$, and D2 is replaced with a subtree encoding the Boolean expression of $D2=A \cap \overline{A1}$, where A and A1 are independent arbitrary events

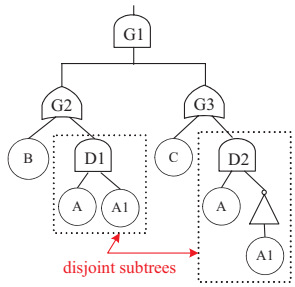


Figure 38.21. Fault tree with modeling of disjoint dependence using disjoint subtrees

and $A = D1 \cup D2$. The minimal cutsets, more accurately, the prime implicants, generated from the new fault tree (Figure 38.21): {B, C}, {A, A1, C}, {A, $\overline{A1}$, B} will be used in the system reliability calculation. Note that the set {A, A1, $\overline{A1}$} was also generated from the top-down approach, but since both A1 and $\overline{A1}$ occur in this set, this set can be automatically removed in the cutset generation.

In general, give a set of *n* mutually exclusive events {D_1, D_2, …, D_n}, each event D_i with probability of π_i. To construct *n* disjoint subtrees with the equivalent occurrence probability π_i, we introduce *n* stochastically independent events: {A, A_1, …, A_{n-1}}, where $A = \bigcup_{i=1}^{n} D_i$, and {$A_1$, …, A_{n-1}} are arbitrary events. The disjoint sets {D_1, D_2, …, D_n} are constructed by subdividing A using A_1, …, A_{n-1} consecutively:

$$
\begin{aligned}
&D_1 = A \cap A_1,\\
&D_2 = A \cap \overline{A_1} \cap A_2,\\
&\ldots\ldots,\\
&D_{n-1} = A \cap \overline{A_1} \cap \ldots \cap \overline{A_{n-2}} \cap A_{n-1},\\
&D_n = A \cap \overline{A_1} \cap \ldots \cap \overline{A_{n-2}} \cap \overline{A_{n-1}}.
\end{aligned}
$$

In particular, the value of *n* is 2 for the example fault tree in Figure 38.20. In general, each disjoint event D_k is converted to a subtree encoding the Boolean function of $D_k = A \cap \overline{A_1} \cap \ldots \cap \overline{A_{k-1}} \cap A_k$. Apparently, the subtree requires one AND gate and (*k*-1) NOT gates. To decrease the number of gates, Morgan's law is applied to D_k:

$$
\begin{aligned}
D_k &= A \cap (\overline{A_1} \cap \ldots \cap \overline{A_{k-1}}) \cap A_k\\
&= A \cap \overline{(A_1 \cup A_2 \cup \ldots \cup A_{k-1})} \cap A_k
\end{aligned}
$$

which requires only three gates: one AND gate, one OR gate, and one NOT gate.

To ensure the subtrees have the same occurrence probabilities as the corresponding disjoint events, Twigg *et al.* [19] derived the probabilities of each independent event in the set {A, A_1, …, A_{n-1}} as:

$$\alpha = \Pr(A) = \Pr(\bigcup_{i=1}^{n} D_i) = \sum_{i=1}^{n} \Pr(D_i) = \sum_{i=1}^{n} \pi_i,$$

$$p_1 = \Pr(A_1) = \frac{\pi_1}{\alpha},$$

$$p_2 = \Pr(A_2) = \frac{\pi_2}{\alpha(1-p_1)} = \frac{\pi_2}{1-\pi_1},$$

……

$$p_k = \Pr(A_k) = \frac{\pi_k}{\pi_{k-1}}\left\{\frac{p_{k-1}}{1-p_{k-1}}\right\} = \frac{\pi_k}{\alpha - \sum_{j=1}^{k-1}\pi_j}.$$

These probabilities are used in the quantitative evaluation of the system unreliability using prime implicants method (Section 38.8.1).

38.9.5 Multistate Systems

A multistate system is a system in which both the system and its components may exhibit multiple performance levels (or states) varying from perfect operation to complete failure [89]. Examples abound in real applications such as communication networks, computer systems, circuits, power systems, and fluid transmission systems [36, 42, 90, 91]. Analyzing the probability of the system being in each state, and thus the reliability of a multistate system is essential to the design and tuning of dependable multistate systems. The difficulty and challenge in analysis arise from the non-binary state property of the system and its components.

Due to the wide use of fault tree in the analysis of systems in other applications, the traditional fault trees have been adapted to model and analyze multistate systems. And the adapted fault trees are called multistate fault trees (MFT) [42]. Similar to the traditional fault tree, a MFT provides a mathematical and graphical representation of the

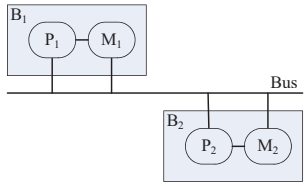


Figure 38.22. An example multistate system

combination of events that can cause the system to occupy a specific state. The quantitative analysis of MFT will be used to determine the probability of system being in that specific state, given the occurrence probabilities of basic events. Each basic event in the MFT represents a component being in a specific state. Also, each MFT consists of a top event representing the system being in a state S_j. The top event is resolved into a combination of events that can cause the occurrence of S_j by means of AND, OR, and *K*-out-of-*N* logic gates.

As an example, consider a multistate computer system that consists of two boards B_1 and B_2 (Figure 38.22) [42]. Each board has a processor and a memory. The two memories (M_1 and M_2) can be shared by both processors (P_1 and P_2) through a common bus. Each board can be considered as a single component with four mutually exclusive and complete states: $B_{i,4}$ (both P and M are functional), $B_{i,3}$ (M is functional, but P is down), $B_{i,2}$ (P is functional but M is down), and $B_{i,1}$ (both P and M are down). Note that $B_{i,j}$ represent the board B_i being in state j, where $i = 1, 2$ and $j = 1, 2, 3, 4$. The entire computer system has three states, which are defined as: S_3 (at least one processor and both memories are functional), S_2 (at least one processor and exactly one memory are functional), and S_1 (no processor or no memory is functional). For illustration purpose, Figure 38.23 shows the MFT for the computer system being in state S_3. Clearly, the system is in state S_3 if the board B_1 is in state 4 and the board B_2 is in state 3 or state 4; or if the board B_1 is in state 3 and the board B_2 is in state 4.

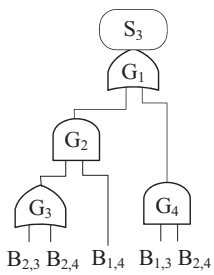


Figure 38.23. MFT of the example system in S_3

Various approaches have been proposed for the analysis of multistate systems; examples include universal moment generating function based methods [91], BDD based methods [38, 42, 92], and MDD based methods [50–52]. Note that among the work, the methods proposed in [38, 50, 51, 92] can only apply to the analysis of multistate systems with multiple failure modes along with a single operational mode, for example, systems subject to imperfect coverage. They cannot directly apply to the general multistate systems, which may contain the states of perfect operation and complete failure, as well as multiple degraded performance levels between those two states. The details of all those approaches for multistate system analysis are outside the scope of this chapter. Readers may refer to the references indicated above for more details.

38.9.6 Phased-mission Systems

A phased-mission system (PMS) is a system used in the mission characterized by multiple, consecutive, and non-overlapping operational phases [38]. During each mission phase, the system has to accomplish a specified task. Since the tasks may differ from phase to phase, the system may be subject to different stresses as well as different reliability requirements. Thus, system configuration, success/failure criteria, and component failure parameters may also change from phase to phase. In the fault tree analysis, the representation of structure functions of a PMS usually requires multiple different fault trees, one for each phase. Further complicating analysis are the statistical dependencies that exist across the phases for a given component

Extensive research has been conducted in the reliability analysis of PMS [38, 41, 46, 51, 72, 92]. Similar to the fault tree analysis methods for non-PMS (Section 38.5.2), the PMS analysis approaches can be classified into three groups: state space oriented approaches based on Markov

chains and/or Petri nets, combinatorial methods, and a modular approach. Readers may refer to Chapter 23 for a state-of-the-art review of these various phased-mission analysis techniques.

38.10 FTA Software Tools

Various software tools have been developed based on the fault trees models. NUREG-0492 [2] summarized available computer software for fault tree analysis and categorized them into five groups. Most of the software codes described in NUREG-0492 were developed in 1970s. In this section, we introduce two software tools that are commonly used by industries and academic research: Galileo dynamic fault tree analysis tool [93] and Relex fault tree analysis software [12]. For details on other available software packages, refer to [94].

Galileo is a dynamic fault tree modeling and analysis tool developed at the University of Virginia [93, 95]. Galileo combines the innovative dynamic fault tree analysis methodology, *i.e.,* the modular approach (Section 38.7.2) with a rich user interface built using package-oriented programming. The important modeling and analysis features of Galileo include: 1) automatic modularization of fault trees and independent solution of modules: efficient BDD based method for static subtrees and Markov chains for dynamic subtrees; 2) multiple time-to-failure distributions (fixed probability, exponential, lognormal, Weibull); 3) imperfect fault coverage modeling in both static and dynamic subtrees; 4) phased mission modeling and analysis; and 5) component importance analysis, *i.e.* sensitivity analysis.

Relex fault tree analysis software [12] supports both quantitative and qualitative analyses, providing computation flexibility based on users' requirements. Relex fault tree analysis tool can compute system unreliability, unavailability, failure frequency, and the number of failures. In addition, it incorporates a minimal cutset (MCS) engine that can quickly determine the minimal cutsets and support interactive, on-screen cutset highlighting. It is the only commercial software package that supports the exact analysis of dynamic fault trees. Relex fault tree analysis tool also supports Lambda-Tau calculations, various importance measures, and noncoherent fault trees.

References

[1] Watson HA. Launch control safety study. Bell Telephone Laboratories, Murray Hill, NJ, USA, 1961.

[2] Vesely WE, Goldberg FF, Roberts NH, Haasl DF. Fault tree handbook. U.S. Nuclear Regulatory Commission, Washington DC, 1981.

[3] Auda DJ, Nuwer K. Effective failure mode effects analysis facilitation. Tutorial Notes of the Annual Reliability and Maintainability Symposium, Alexandria, VA.; Jan. 24–27, 2005.

[4] Rausand M, Hoyland A. system reliability theory: models, statistical methods, and applications (2nd Edition). Wiley Inter-Science, New York, 2003.

[5] Bowles JB, Bonnell RD. Failure modes, effects, and criticality analysis. Tutorial Notes of the Annual Reliability and Maintainability Symposium 1997.

[6] Andrews JD, Dunnett SJ. Event-tree analysis using binary decision diagrams. IEEE Transactions on Reliability 2000; 49(2): 230–238.

[7] IEC61078, Analysis techniques for dependability – Reliability block diagram method. International Electrotechnical Commission, Geneva, 1991.

[8] Dugan JB, Doyle SA. New results in fault-tree analysis. Tutorial Notes of the Annual Reliability and Maintainability Symposium 1997.

[9] NASA, Fault tree handbook with aerospace applications, NASA Office of Safety and Mission Assurance, Washington DC, 2002.

[10] Henley EJ, Kumamoto H. Probabilistic risk assessment. IEEE Press, New York, 1992.

[11] Coppit D, Sullivan KJ, Dugan JB. Formal semantics of models for computational engineering: A case study on dynamic fault trees. Proceedings of the International Symposium on Software Reliability Engineering 2000; 270–282.

[12] Relex software, www.relex.com

[13] Pham H. Optimal design of a class of noncoherent systems. IEEE Transactions on Reliability 1991; 40(3): 361–363.

[14] Amendola A, Contini S. About the definition of coherency in binary system reliability analysis. In: Apostolakis G, Garribba S, Volta G, Editors. Synthesis and analysis methods for safety and reliability studies. Plenum Press, New York, 1978; 79–84.

[15] Jackson PS. Comment on probabilistic evaluation of prime implicants and top-events for non-coherent systems. IEEE Transactions on Reliability 1982; R-31: 172–173.
[16] Jackson PS. On the s-importance of elements and implicants of non-coherent systems. IEEE Transactions on Reliability 1983; R-32: 21–25.
[17] Johnson BD, Matthews RH. Non-coherent structure theory: a review and its role in fault tree analysis. UKAAE, SRD R245, 1983; October.
[18] Wolfram S. Mathematica – A system for doing mathematics by computer. Addison-Wesley, Reading, MA, 1991.
[19] Twigg DW, Ramesh AV, Sandadi UR, Sharma TC. Modeling mutually exclusive events in fault trees. Proceedings of the Annual Reliability and Maintainability Symposium 2000; 8–13.
[20] Twigg DW, Ramesh AV, Sharma TC. Modeling event dependencies using disjoint sets in fault trees. Proceedings of the 18th International System Safety Conference 2000; 275–279.
[21] Misra KB. Reliability analysis and prediction: a methodology oriented treatment. Elsevier, Amsterdam, 1992.
[22] Bobbio A, Franceschinis G, Gaeta R, Portinale L. Exploiting Petri nets to support fault tree based dependability analysis. Proceedings of the 8th International Workshop on Petri Nets and Performance Models 1999; 146 – 155.
[23] Dugan JB, Trivedi KS, Sometherman MK, Geist RM. The hybrid automated reliability predictor. AIAA Journal of Guidance, Control and Dynamics 1991; 9(3): 554–563.
[24] Dugan JB, Bavuso SJ, Boyd MA. Fault trees and Markov models for reliability analysis of fault tolerant systems. Reliability Engineering and System Safety 1993; 39: 291–307.
[25] Hura GS, Atwood JW. The use of Petri nets to analyze coherent fault trees. IEEE Transactions on Reliability 1988; R-37: 469–474.
[26] Malhotra M, Trivedi KS. Dependability modeling using Petri nets. IEEE Transactions on Reliability 1995; R-44: 428–440.
[27] Coudert O, Madre JC. Fault tree analysis: 10^{20} prime implicants and beyond. Proceedings of the Annual Reliability and Maintainability Symposium 1993; 240–245.
[28] Doyle SA, Dugan JB. Analyzing fault tolerance using DREDD. Proceedings of the 10th Computing in Aerospace Conference 1995.
[29] Sinnamon R, Andrews JD. Fault tree analysis and binary decision diagrams. Proceedings of the Annual Reliability and Maintainability Symposium 1996; 215–222.
[30] Gulati R, Dugan JB. A modular approach for analyzing static and dynamic fault trees. Proceedings of the Annual Reliability and Maintainability Symposium 1997.
[31] Sahner R, Trivedi KS, Puliafito A. Performance and reliability analysis of computer systems: an example-based approach using the SHARPE software package. Kluwer, Dordrecht, 1996.
[32] Misra KB. New trends in system reliability evaluation. Elsevier, 1993.
[33] Shooman ML. Probabilistic reliability: an engineering approach (2nd Edition). McGraw-Hill, New York, 1990.
[34] Brace K, Rudell R, Bryant R. Efficient implementation of a BDD package. Proceedings of the 27th ACM/IEEE Design Automation Conference 1990; 40–45.
[35] Bryant R. Graph based algorithm for boolean function manipulation. IEEE Transactions on Computers 1986; 35: 677–691.
[36] Chang YR, Amari SV, Kuo SY. OBDD-based evaluation of reliability and importance measures for multistate systems subject to imperfect fault coverage. IEEE Transactions Dependable and Secure Computing 2005; 2(4): 336–347.
[37] Kuo S, Lu S, Yeh F. Determining terminal-pair reliability based on edge expansion diagrams using OBDD. IEEE Transactions on Reliability 1999; 48(3): 234–246.
[38] Xing L, Dugan JB. Analysis of generalized phased-mission systems reliability, performance and sensitivity. IEEE Transactions on Reliability 2002; 51(2): 199–211.
[39] Xing L. Fault-tolerant network reliability and importance analysis using binary decision diagrams. Proceedings of the 50th Annual Reliability and Maintainability Symposium, Los Angeles, CA, 2004.
[40] Yeh F, Lu S, Kuo S. OBDD-based evaluation of k-terminal network reliability. IEEE Transactions on Reliability 2002; 51(4): 443–451.
[41] Zang X, Sun H, Trivedi KS. A BDD-based algorithm for reliability analysis of phased-mission systems. IEEE Transactions on Reliability 1999; 48(1): 50–60.
[42] Zang X, Wang D, Sun H, Trivedi KS. A bdd-based algorithm for analysis of multistate systems with multistate components. IEEE Transactions on Computers 2003; 52(12): 1608–1618.
[43] Bouissou M, Bruyere F, Rauzy A. BDD based fault-tree processing: a comparison of variable ordering heuristics. Proceedings of ESREL Conference 1997.

[44] Coudert O, Madre JC. Metaprime, an interactive fault-tree analyzer. IEEE Transactions on Reliability 1994; 43(1): 121–127.
[45] Xing L. Dependability modeling and analysis of hierarchical computer-based systems. Ph.D. Dissertation, Electrical and Computer Engineering, University of Virginia, 2002; May.
[46] Xing L, Dugan JB. Generalized imperfect coverage phased-mission analysis. Proceedings of the Annual Reliability and Maintainability Symposium, Seattle, WA, 2002; 112–119,
[47] Zang X., Sun H., and Trivedi KS. Dependability analysis of distributed computer systems with imperfect coverage. Proceedings of the 29th Annual International Symposium on Fault-Tolerant Computing 1999; 330–337.
[48] Caldarola L. Coherent systems with multistate components. Nuclear Engineering and Design 1980; 58: 127–139.
[49] Miller DM, Drechsler R. Implementing a multiple-valued decision diagram package. Proceedings of the 28th International Symposium on Multiple-valued Logic 1998.
[50] Xing L. Dugan JB. Dependability analysis using multiple-valued decision diagrams. Proceedings of the 6th International Probabilistic Safety Assessment and Management, Puerto Rico 2002.
[51] Xing L, Dugan JB. A separable TDD-based analysis of generalized phased-mission reliability. IEEE Transactions on Reliability 2004; 53(2): 174–184.
[52] Xing L. Efficient analysis of systems with multiple states. Proceedings of the IEEE 21st International Conference on Advanced Information Networking and Applications, Niagara Falls, Canada 2007; 666–672.
[53] Gulati R. A modular approach to static and dynamic fault tree analysis. M. S. Thesis, Electrical Engineering, University of Virginia, August 1996.
[54] Sune V, Carrasco JA. A method for the computation of reliability bounds for non-repairable fault-tolerant systems. Proceedings of the 5th IEEE International Symposium on Modeling, Analysis, and Simulation of Computers and Telecommunication System 1997; 221–228.
[55] Sune V, Carrasco JA. A failure-distance based method to bound the reliability of non-repairable fault-tolerant systems without the knowledge of minimal cutsets. IEEE Transactions on Reliability 2001; 50(1): 60–74.
[56] Dutuit Y, Rauzy A. A linear time algorithm to find modules of fault trees. IEEE Transactions on Reliability 1996; 45(3): 422–425.
[57] Manian R, Dugan JB, Coppit D, Sullivan KJ. Combining various solution techniques for dynamic fault tree analysis of computer systems. Proceedings of the 3rd IEEE International High-Assurance Systems Engineering Symposium 1998; 21–28.
[58] Inagaki T, Henley EJ. Probabilistic evaluation of prime implicants and top-events for non-coherent systems. IEEE Transactions on Reliability 1980; 29(5): 361–367.
[59] Amari SV. Computing failure frequency of noncoherent systems. International Journal of Performability Engineering 2006; 2(2): 123–133.
[60] Dutuit Y, Rauzy A. Efficient algorithm to assess component and gate importance in fault tree analysis. Reliability Engineering and System Safety 2001; 72: 213–222.
[61] Xing L. Maintenance-oriented fault tree analysis of component importance. Proceedings of the 50th Annual Reliability and Maintainability Symposium, Los Angeles, CA, USA. 2004; 534–539,
[62] Andrews JD, Beeson S. Birnbaum's measure of component importance for noncoherent systems. IEEE Transactions on Reliability 2003; 52(2): 213–219.
[63] Beeson S, Andrews JD. Importance measures for non-coherent-system analysis. IEEE Transactions on Reliability 2003; 52(3): 301–310.
[64] Birnbaum ZW. On the importance of different components in a multicomponent system. In: Krishnaiah P, Editor. Multivariate analysis. Academic Press, New York, 1969.
[65] Fussell J. How to hand calculate system reliability characteristics. IEEE Transactions on Reliability 1975; R-24: 169–174.
[66] Barlow RE, Proschan F. Importance of system components and fault tree events. Stochastic Processes and Their Applications 1975; 3: 153–173.
[67] Vesely WE. A time dependent methodology for fault tree evaluation. Nuclear Engineering and Design 1970; 13: 337–360.
[68] Andrews JD, Moss TR. Reliability and risk assessment. Longman Scientific and Technical, Essex, 1993.
[69] Anne A. Implementation of sensitivity measures for static and dynamic subtrees in DIFtree. M.S. Thesis, University of Virginia, 1997.
[70] Chang Y, Amari SV, Kuo S. Computing system failure frequencies and reliability importance measures using OBDD. IEEE Transactions on Computers 2004; 53(1): 54–68.

[71] Papoulis A. Probability, random variables, and stochastic processes (3rd Edition). McGraw-Hill Series in Electrical Engineering, McGraw-Hill, New York, 1991.

[72] Xing L. Reliability importance analysis of generalized phased-mission systems. International Journal of Performability Engineering 2007; 3(3): 303–318.

[73] Frank PM. Introduction to system sensitivity. Academic Press, New York, 1978.

[74] NUREG/CR-4780, Procedure for treating common-cause failures in safety and reliability studies. U.S. Nuclear Regulatory Commission, Washington DC, 1988; Vols. I and II.

[75] Tang Z, Dugan JB. An integrated method for incorporating common cause failures in system analysis. Proceedings of the 50th Annual Reliability and Maintainability Symposium, 610–614, Los Angeles, CA, 2004.

[76] Mitra S, Saxena NR, McCluskey EJ. Common-mode failures in redundant VLSI systems: a survey. IEEE Transactions on Reliability 2000; 49(3): 285–295.

[77] Vaurio JK. An implicit method for incorporating common-cause failures in system analysis. IEEE Transactions on Reliability 1998; 47(2): 173–180.

[78] Bai DS, Yun WY, Chung SW. Redundancy optimization of *k*-out-of-*n* systems with common-cause failures. IEEE Transactions on Reliability 1991; 40(1): 56–59.

[79] Pham H. Optimal cost-effective design of triple-modular-redundancy-with-spares systems. IEEE Transactions on Reliability 1993; 42(3): 369–374.

[80] Anderson PM, Agarwal SK. An improved model for protective-system reliability. IEEE Transactions on Reliability 1992; 41(3): 422–426.

[81] Chae KC, Clark GM. System reliability in the presence of common-cause failures. IEEE Transactions on Reliability 1986; R-35: 32–35.

[82] Fleming KN, Mosleh N, Deremer RK. A systematic procedure for incorporation of common cause events into risk and reliability models. Nuclear Engineering and Design 1986; 93: 245–273.

[83] Dai YS, Xie M, Poh KL, Ng SH. A model for correlated failures in *n*-version programming. IIE Transactions 2004; 36(12): 1183–1192.

[84] Fleming KN, Mosleh A. Common-cause data analysis and implications in system modeling. Proceedings of the International Topical Meeting on Probabilistic Safety Methods and Applications 1985; 1: 3/1–3/12, EPRI NP-3912-SR.

[85] Amari SV, Dugan JB, Misra RB. Optimal reliability of systems subject to imperfect fault-coverage. IEEE Transactions on Reliability 1999; 48 (3): 275–284.

[86] Vaurio JK. Common cause failure probabilities in standby safety system fault tree analysis with testing – scheme and timing dependencies. Reliability Engineering and System Safety 2003; 79(1): 43–57.

[87] Xing L. Reliability modeling and analysis of complex hierarchical systems. International Journal of Reliability, Quality and Safety Engineering 2005; 12(6): 477–492.

[88] Dobson I., Carreras BA, Newman DE. A loading-dependent model of probabilistic cascading failure. Probability in the Engineering and Informational Sciences 2005; 19(1): 15–32.

[89] Huang J, Zuo M. Dominant multi-state systems. IEEE Transactions on Reliability 2004; 53(3): 362–368.

[90] Li W, Pham H. Reliability modeling of multi-state degraded systems with multi-competing failures and random shocks. IEEE Transactions on Reliability 2005; 54(2): 297–303.

[91] Levitin G, Dai YS, Xie M, Poh KL. Optimizing survivability of multi-state systems with multi-level protection by multi-processor genetic algorithm. Reliability Engineering and System Safety 2003; 82(1): 93–104.

[92] Tang Z, Dugan JB. BDD-based reliability analysis of phased-mission systems with multimode failures. IEEE Transactions on Reliability 2006; 55(2): 350–360.

[93] Galileo Dynamic Fault Tree Analysis Tool, http://www.cs.virginia.edu/~ftree/.

[94] Fault Tree Analysis Software, http://www.fault-tree.net/software.html.

[95] Sullivan KJ, Coppit D, Dugan JB. The Galileo fault tree analysis tool. Proceedings of the 29th International Conference on Fault-Tolerant Computing, Madison, Wisconsin, June 15–18, 1999: 232–235.

39

Common Cause Failure Modeling: Status and Trends

Per Hokstad[1] and Marvin Rausand[2]

[1] SINTEF, Technology and Society, NO 7465 Trondheim, Norway
[2] Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway

Abstract: This chapter presents a status of common cause failure (CCF) modeling. The well known beta-factor model is still the most commonly used CCF model. The strengths and limitations of this model are therefore outlined together with approaches to establish plant specific beta-factors. Several more advanced CCF models are also described with a special focus on the new multiple beta-factor model. Problems relating to data availability and estimation of the unknown parameters of the various models are discussed, and ideas for further research are suggested.

39.1 Introduction

Reliability modeling of common cause failures (CCF) was introduced in the nuclear power industry more than 30 years ago [1]. This industry has had a continuous focus on CCF, and has been in the forefront regarding development of CCF models, and on collection and analysis of data related to CCF. The aviation industry has also given these failures close attention. The Norwegian offshore industry has for some 20 years focused on CCF related to reliability assessment of safety instrumented systems (SIS) [2].

More recently, the IEC 61508 [3] standard points at the need to control CCF in order to maintain the safety integrity level (SIL) of safety functions. The standard suggests a method to calculate the probability of failure on demand (PFD) where the contribution of CCF is modeled by the well known beta-factor model.

The objective of this chapter is to present the current status concerning modeling and analysis of CCFs in risk and reliability analyses.

The chapter is structured as follows. In Section 39.1 we give an introduction to CCF and define CCF and related concepts. In Section 39.2 we present and discuss various ways of classifying CCFs and introduce the concepts of root causes and coupling factors. Section 39.3 presents the status related to modeling of CCF with a main focus of the beta-factor model together with challenges and extensions of this model. Various approaches to determine a plant specific beta-factor are outlined. A new extension of the beta-factor model, the multiple beta-factor model, is introduced and discussed. In Section 39.4 we present data sources and methods for estimating the parameters of the models presented in Section 39.3. Concluding remarks and suggestions for further research are presented in Section 39.5.

39.1.1 Common Cause Failures

When components of a system fail, the failures cannot always be considered as independent events. We may distinguish between two main types of dependence: *positive* and *negative*. If a failure of one component leads to an increased tendency for another component to fail, the dependence is said to be positive. If, on the other hand, the failure of one component leads to a reduced tendency for another component to fail, the dependence is called negative.

In reliability applications, positive dependence is usually the most relevant type of dependence. Negative dependence may, however, occur in practice. Consider, for example, two components that influence each other by producing vibrations or heat. When one component is "down" for repair, the other component will have an improved operating environment, and its likelihood of failure is reduced.

Consider a system of two components, 1 and 2. Let A_i denote the event that component i is in a failed state $(i = 1, 2)$. One way of formulating dependence stems from the idea that the components are susceptible to some common stress that causes simultaneous failures. When this common stress occurs, the event "A_1 and A_2" is referred to as a CCF event. The CCF event may be due to several types of dependencies, for example:

- Physical dependencies
- Functional dependencies
- Location/environmental dependencies
- Plant configuration related dependencies
- Human dependencies

There is no generally accepted definition of CCF. This implies that people in different industry sectors may have different opinions of what a CCF event is. Smith and Watson [4] review nine different definitions of CCF and suggest that a definition of CCF must encompass the following six attributes:

1. The components affected are unable to perform as required.
2. Multiple failures exist within (but not limited to) redundant configurations.
3. The failures are "first in line" type of failures and not the result of cascading failures.
4. The failures occur within a defined critical time period (*e.g.*, the time a plane is in the air during a flight).
5. The failures are due to a single underlying defect or a physical phenomenon (the common cause of failures).
6. The effect of failures must lead to some major disabling of the system's ability to perform as required.

In the nuclear power industry a CCF event is defined as "a dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause" [5].

In the space industry a CCF event is defined as "the failure (or unavailable state) of more than one component due to a shared cause during the system mission" [6].

39.1.2 Explanation

The term CCF implies the existence of a cause-effect relationship that links the CCF event to some cause. Such a relationship is not, however, reflected in most of the CCF models that are presented later in this chapter [7].

A crucial question when using the definitions of CCF is how to interpret the term *simultaneous*. It is obvious that there can be a strong dependence even if the failures do not occur at the same time. In the NASA definition [6], a multiple failure is classified as a CCF event if the failures occur during the same mission. Such a mission may last a long period of time. In the aviation industry the term CCF is used for multiple failures during the same flight. For safety instrumented systems [3] the main functional failures are often *hidden* and can only be detected during periodic function tests. In this case, it seems natural to classify a multiple failure as a CCF if failures of redundant components occur within the same test interval. The test interval may be several months and even years. When multiple failures are detected during a test, it is not straightforward to decide whether the

failures have occurred due to the same cause, or whether they have occurred at the same time. Consider, for example, a number of fire detectors that are installed in the same room. The detectors are sensitive to humidity and will tend to fail if the humidity in the room increases above a certain level. If the humidity becomes too high, the detectors will deteriorate and fail, but *not* necessarily at the same time. The failures may be spread out over a rather long period of time. When the detectors are checked in the periodic test, the problem will likely be detected and both the failed and the deteriorated detectors will be replaced.

Whether or not the multiple failures that are detected in the test represent a true CCF event must be decided on the basis of a thorough investigation of the causes of the component failures.

Due to lack of information it may be difficult to decide whether or not the failures had the same cause. In practice, the term CCF is therefore often used synonymously with *multiple* failure.

However, a single failure can actually be seen as a CCF. The common cause may, for example, be erroneous maintenance or environmental stresses (*e.g.,* vibration, high temperature or high humidity). These causes may lead to failures of different multiplicities. Following this argument, a common cause may lead to just one component failing, thus a CCF of multiplicity one is also possible.

Often, it is most simple to use the term CCF synonymously with multiple failures that occur close in time. We should, avoid classifying a multiple failure due to joint occurrence of independent failures as a CCF. The classification should be based on the cause of the failures.

39.2 Causes of CCF

Many authors find it useful to split CCF causes into *root causes* and *coupling factors* [8, 9]. A root cause is a basic cause of a component failure (*e.g.*, a corrosive environment), while a coupling factor explains why several components are affected by the same root cause (*e.g.*, inadequate material selection for several valves).

39.2.1 Root Causes

A *root cause* of a failure is the most basic cause that, if corrected, would prevent recurrence of this and similar failures. There is often a series of causes that can be identified, one leading to another. This series of causes should be pursued until the fundamental, *correctable* cause has been identified [10]. The concept of root cause is tied to that of *defense*, because there are, in many cases, several possible corrective actions *(i.e.*, defenses) that can be taken to prevent recurrence. Knowledge about root causes allows system designers to incorporate countermeasures for reducing the susceptibility to both single failures and CCFs.

A number of studies have investigated the root causes of CCF events, and several classification schemes have been proposed and used to categorize these events. Tables 39.1–39.3 (adapted from [9]) show root causes of CCF events arranged in a hierarchy. Thus, the hierarchy starts with those causes that are introduced during the design phase and proceeds through the manufacturing, construction, installation, and commissioning phases. Root causes introduced during plant operation, maintenance or due to the environment are given in Tables 39.1 and 39.2. Several other taxonomies of root causes have also been proposed, (*e.g.*, see [5, 10, 11]). Several studies of CCFs in complex systems have shown that the majority of the root causes are related to human actions and procedural deficiencies. A study of centrifugal pumps in nuclear power plants indicates that the root causes of about 70% of all CCFs are of this category [12].

In practice, root causes of component failures can seldom be determined from failure cause descriptions. CCF root causes have to be identified through root cause analyses, supported by check-lists of generic root causes [10]. The description of a CCF in terms of a single root cause is in many cases too simplistic [8]. Cooper *et al.* [13] advocate using the concept of common failure mechanism instead of root cause to cater for multiple root causes.

Table 39.1. Root causes of CCF events (design, manufacturing, construction, installation and commissioning)

Cause type	Examples of specific cause
Design requirements and specifications inadequacy	Designer failure to predict an accident
	Designer failure to recognize what protective action is needed
Design error or inadequacy in design realization	Inadequate facilities for operation, maintenance, testing or calibration
	Inadequate components
	Inadequate quality assurance
Design limitations	Financial
	Spatial
Manufacturing error or inadequacy	Failure to follow instructions
	Inadequate manufacturing control
	Inadeqaute inspection
	Inadequate testing
Construction/installation/commissioning	Failure to follow instructions
	Inadequate construction control
	Inadequate inspection
	Inadequate testing

39.2.2 Coupling Factors

A *coupling factor* is a property that makes multiple components susceptible to failure from a single shared cause. Such properties include:

- Same design
- Same hardware
- Same software
- Same installation staff
- Same maintenance or operation staff
- Same procedures
- Same environment
- Same location

Table 39.2. Root causes of CCF events (operation)

Cause type	Examples of specific cause
Lack of procedures	Lack of repair procedures
	Lack of test or calibration procedures
Defective procedures	Defective repair procedures
	Defective test or calibration procedures
Failure to follow procedures	Failure to follow repair procedures
	Failure to follow test or calibration procedures
Supervision inadequacy	Inadequate supervisory procedures
	Inadequate action or supervisory communication
Communication problems	Communication among maintenance staff
Training inadequacy	Operator training in handling emergency situations

Table 39.3. Root causes of CCF events (environmental)

Cause type	Examples of specific cause
Stresses	Chemical reactions (corrosion)
	Electrical failure
	Electromagnetic interference
	Materials interaction (erosion)
	Moisture
	Pressure
	Radiation
	Temperature
	Vibration
Energetic	Earthquake
	Fire
	Flood
	Impact loads

A more detailed taxonomy of coupling factors is given in [5, 14, 15]. Studies of CCFs in nuclear power plants indicate that the majority of coupling factors contributing to CCFs are related to operational aspects [12].

To save money and ease operation and maintenance, the technical solutions in many industries become more and more standardized. This applies both to hardware and software and increases the presence of coupling factors. Sintef, a Norwegian research organization, has recently carried out several studies of the impacts of this type of standardization on Norwegian offshore oil and gas installations, where new operational concepts and reduced manning levels are feeding this trend [16].

Two different approaches can be applied to the modeling of CCFs, an *explicit* method and an *implicit* method. Assume that a specific cause of CCF can be identified and defined. By the explicit method, this cause of dependency is included into the system logic models, for example as a basic event in the fault tree model, or as a functional block in a reliability block diagram [17, 18]. Explicit causes may also be included in event trees. Examples of causes that may be modeled explicitly are:

- Human errors
- Utility failures (*e.g.,* electricity, cooling, heating)
- Environmental events (*e.g.,* earthquakes, lightning)

Some causes of dependencies are difficult or even impossible to identify and model explicitly. These are called *residual* causes and are catered for in a so-called implicit model. The residual causes cover many different root causes and coupling factors, such as common manufacturer, common environment, and maintenance errors. There are so many causes that an explicit representation of all of them in a fault tree or an event tree would be unmanageable.

When establishing the implicit model, it is important to remember which causes were covered in the explicit model, so that they are not counted twice. For small system modules it may be possible to use Markov techniques to model both explicit and implicit causes. This is not pursued further in this chapter. See, for example, chapter 8 of [18] for a further treatment of this topic.

Modeling and analysis of CCF as part of a risk or reliability study should, in general, comprise at least the following steps (see also [11, 19]):

1. *Development of system logic models*: This activity comprises system familiarization, system functional failure analysis, and establishment of system logic models (*e.g.*, fault trees, reliability block diagrams, and event trees).
2. *Identification of common cause component groups*: The groups of components for which the independence assumption is suspected not to be correct are identified.
3. *Identification of root causes and coupling factors:* The root causes and coupling factors are identified and described for each common cause component group. Suitable tools are checklists and root cause analysis.
4. *Assessment of component defenses:* The common cause component groups are evaluated with respect to their defenses against the root causes that were identified in the previous step.
5. *Explicit modeling*: Explicit CCF causes are identified for each common cause component group and included into the system logic model.
6. *Implicit modeling*: Residual CCF causes that were not covered in the previous step are included in an implicit model as discussed later in this section. The parameters of this model have to be estimated based on checklists (*e.g.*, IEC 61508 [3] part 6) or from available data.
7. *Quantification and interpretation of results*: The results from the previous steps are merged into an overall assessment of the system. The step will also cover importance, uncertainty, and sensitivity analyses – and reporting of results.

In most cases, we will not be able to find high quality input data for the explicitly modeled CCF causes. However, even with low-quality input data, or guesstimates, the result will usually be more accurate than by including the explicit causes into a general (implicit) CCF model.

The CCF models that are discussed in the rest of this section are limited to cover implicit causes of CCF.

39.2.3 The Beta-factor Model and its Generalizations

The *beta-factor model* was introduced by Fleming [20] in 1975 and is still the most popular CCF model. The beta-factor model may be explained by the following simple example: Consider a system of n identical components each with a constant total failure rate λ. In the following these identical components are referred to as *channels*. Given that a specific channel has failed, this failure will, with probability β, cause all the n channels to fail, and with probability $1-\beta$, just involve the given channel. The system will then have a CCF rate $\lambda_C = \beta\lambda$, where all n channels fail. In addition, each channel has a rate of independent failures, $\lambda_I = (1-\beta)\lambda$. The total failure rate of a channel may be written as $\lambda = \lambda_I + \lambda_C$.

The beta-factor model may also be regarded as a *shock model* where shocks occur randomly according to a homogeneous Poisson process with rate λ_C. Each time a shock occurs, all the channels of the system fail, irrespective of the status of the channels. Each channel may hence fail due to two independent causes; shocks and channel specific (individual) causes. The rate λ_I is sometimes called the rate of *individual* failures.

The parameter β can be interpreted as the mean fraction of all failures of a channel that also affect all the other channels of the system.

When a failure occurs, the *multiplicity* of the failure event is either one or n. Intermediate values of the multiplicity are not possible when assuming the beta-factor model. This is illustrated in Figure 39.1 for a system of three identical channels, where A_i denotes failure of channel i,

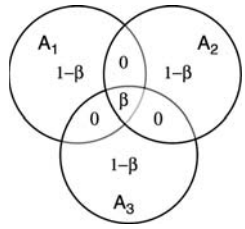


Figure 39.1. Fractions of different multiplicities of failures for a system with three identical channels when using the beta-factor model

for $i = 1, 2, 3$. Due to its simplicity, the beta-factor model is often preferred in practical applications of CCF modeling. IEC 61508 [3] recommends using the beta-factor model to quantify the probability of failure on demand (PFD) of safety instrumented systems. A single "plant specific" β can be determined for each of the channel groups of the safety instrumented system by using the checklist in IEC 61508 [3], part 6.

This approach is briefly introduced later in this section. It does, however, determine a β that is more or less independent of the system configuration.[1] For system configurations with voting 1oo2 (1-out-of-2), 1oo3 (1-out-of-3), 2oo3 (2-out-of-3), and so on, the system unavailability will be dominated by the CCF event, and we will get approximately the same unavailability for all configurations. This makes a comparison between different configurations and voting logics rather meaningless. The main advantage of the beta-factor model is its simplicity, requiring only one extra parameter, β.

The original beta-factor was defined for identical channels with the same constant failure rate λ. Many systems are, however, diversified with channels that are not identical. In this case it is more difficult to define and interpret the beta-factor. An approach that is sometimes used is to define β as a percentage of the geometric average of the failure rates of the various channels of the system.

1) A system has a *k*-out-of-*n* configuration (or reliability structure) when it is functioning if and only if at least *k* of the *n* (redundant) components, or channels, are functioning. In analyzes of safety systems this is often referred to as a *koon* voting

The parameter β is easy to interpret and also rather easy to estimate when data are available. Note that several data sources, like OREDA [21], present estimates for the total failure rate, λ. In many analyses this failure rate is accepted and taken as being constant. This approach implies that the rate λ_I of individual (single) failures will be *reduced* when we increase the value of β. Other data sources, like MIL-HDBK 217F [22], present only the individual failure rate, λ_I, and the rate of CCFs must therefore be added to give the total failure rate.

C-factor model:

The C-factor model was introduced by Evans *et al*. [23], and is essentially the same model as the beta-factor model, but defines the fraction of CCFs in another way. In the C-factor model, the CCF rate is defined as $\lambda_C = C \cdot \lambda_I$, that is, as a fraction of the *individual* failure rate λ_I. The total failure rate may then be written as $\lambda = \lambda_I + C \cdot \lambda_I$. In this model, the individual failure rate λ_I is kept constant and the CCF rate is added to this rate to give the total failure rate.

39.2.4 Plant Specific Beta-factors

The defenses against CCF events that are implemented in a plant will affect the fraction β of CCF events. Estimates of β based on generic data are therefore of limited value.

There are several suggestions on how to choose a more "correct" β, based the actual system's vulnerability to possible causes of CCF events. Some of the methods that are designed to determine "plant specific" (application specific) β's are briefly reviewed in this section.

Humphreys' method

One of the first methods to determine a plant specific β was suggested by Humphreys [24]. He identifies eight factors that are considered to be important for the actual value of β (grouped in *design*, *operation* and *environment*). The various factors are weighted based on expert judgment and discussions amongst reliability engineers as shown in Table 39.4. Some other potential factors are not included because they were found to be too difficult to quantify.

Each of the chosen eight factors is described in the Appendix of [24] and classified into five categories from a (= worst) to e (= best). For a specific application, the eight sub-factors are classified into categories a-e, and given weights (score) according to Table 39.4. A simple procedure is next used to produce an application specific β estimate:

Table 39.4. Factors and weights in Humphreys' (1987) method

Factor	***Sub-factor***	***Weights***				
		a	**b**	**c**	**d**	**e**
Design	Separation	2400	580	140	35	8
	Similarity	1750	425	100	25	6
	Complexity	1750	425	100	25	6
	Analysis	1750	425	100	25	6
Operation	Procedures	3000	720	175	40	10
	Training	1500	360	90	20	5
Environment	Control	1750	425	100	25	6
	Tests	1200	290	70	15	4

Table 39.5. The partial beta-factor method [19]

Defenses	Reference values
Design control	0.6
Design review	0.8
Functional diversity	0.2
Equipment diversity	0.25
Fail-safe design	1.0
Operational interfaces	0.8
Protection and segregation	0.8
Redundancy and voting	0.9
Proven design and standardization	0.9
Derating and simplicity	0.9
Construction control	0.8
Testing and commissioning	0.7
Inspection	0.9
Construction standards	0.9
Operational control	0.6
Reliability monitoring	0.8
Maintenance	0.7
Proof test	0.7
Operations	0.8
	$\prod_{i=1}^{19}\beta_i = 0.001$

1. The sum of column "a" representing the worst possible case should correspond to $\beta = 0.3$, a value that is considered to be a realistic worst case scenario [24].
2. The sum of column "e" representing the best possible case should correspond to $\beta = 0.001$ (*i.e.,* it is not realistic to attain any lower value of β).
3. To allow the convenience of whole numbers a divisor of 50000 was chosen, in which case the sum of column "a" should be 15000, and the sum of column "e" should be 50.

The application specific β is determined by adding the weights for the chosen categories and dividing by 50000. Consider, for example, a system of identical channels. This system will be a worst case (*i.e.*, category "a") with respect to the sub-factor "similarity", and get the weight 1750 for this factor. If all the other factors are of the best category "e", the total weight will be 1795, and the estimated value of β is hence 0.036. This means that the lowest possible β-value for a system of identical channels is 3.6% when we are using the method of Humphreys [24].

Partial Beta-factor Method

Johnston [19] suggested the partial beta-factor method. Also this method requires a qualitative analysis in order to assess a plant specific β. In the partial beta-factor method, the plant specific β is determined as a product of a number of partial betas that are derived from judgments of the system defenses. 19 different defenses are defined and reference values are allocated to each defense, as shown in Table 39.5.

When all 19 factors are assigned their reference value, we multiply them and end up with the estimate of β. However, the qualitative analysis may result in alternative (higher) values being used. Johnston [19] also discusses a generalization where this approach is applied separately for different CCF causes.

IEC Model for Determining the Beta-factor

IEC 61508 [3], part 6, Annex D suggests an approach that is based on an idea similar to the one suggested by Humphreys [24]. The IEC approach is adapted to safety instrumented systems (SIS). A SIS generally consists of one or more input elements (*e.g.,* sensors, transmitters), one or more logic solvers (*e.g.,* programmable logic controllers [PLC], relay logic systems), and one or more final elements (*e.g.,* safety valves, circuit breakers). Application specific β-values must be calculated for input elements, logic solvers, and final elements separately. To estimate β, about 40 specific questions have to be evaluated/answered

concerning the following factors for each type of elements of the safety system [3, 25]:

- Degree of physical *separation/ segregation*
- *Diversity/redundancy*, (*e.g.,* different technology, design; different maintenance personnel)
- *Complexity/maturity of design/experience*
- Use of *assessments/analyzes and feedback data*
- *Procedures/human interface* (*e.g.,* maintenance/testing)
- *Competence/training/safety culture*
- *Environmental control* (*e.g.,* temperature, humidity; personnel access)
- *Environmental testing*

The system elements are then assigned X_i and Y_i scores related to question no. i, where X_i is selected if diagnostic testing will lead to improvement and Y_i is selected if not. The ratio X_i / Y_i presents the benefit of diagnostic testing as a defense against CCF related to question no. i. Total scores are next calculated using simple formulas, and compared with predefined values in Table D.4 in part 6 of IEC 61508 [3], to give the estimate of β. The result of this procedure is one out of five possible β-values; 0.5% (applies to logic only); 1%, 2%, 5%, and 10% (input and final elements only). The highest possible β-value for input and final elements is therefore 10%, which is a low value compared to Humphreys' method [24]. The main reason for this is that most SIS channels are subject to frequent diagnostic testing and that failures thereby can be removed and CCFs can be avoided.

There are two scores X and Y, since the IEC standard gives different β's for detected failures and undetected failures, and hence also incorporates the diagnostic coverage (DC) into the calculation of β.

Unified Partial Model

The unified partial method (UPM) was developed for the British nuclear power industry [26] and is based on the beta-factor model. In the UPM framework, the defenses against CCFs are broken down to eight factors:

1. Environmental control
2. Environmental tests
3. Analysis
4. Safety culture
5. Separation
6. Redundancy and diversity
7. Understanding
8. Operator interaction

The actual system is assigned one out of five possible levels $x_{i,j}$ for $i = 1, 2, \ldots, 5$, across each defense, $j = 1, 2, \ldots, 8$, and scores $s_j(x_{i,j})$ are given accordingly from generic tables that have been deduced from past research. The overall beta-factor is obtained as a scaled sum of these scores. The UPM model has been discussed in [27, 28] where a novel approach based on influence diagrams is suggested for assessment of the plant specific beta-factor.

39.2.5 Multiplicity of Failures

Let Z denote the number of failed channels when a CCF occurs in a system with n channels. When using the beta-factor model, Z can only take the values 0 and n. Various generalizations are suggested. Either we could assume some parametric distribution of Z, say a binomial distribution, or we could allow Z to have a completely general distribution, but could introduce various ways to parameterize the distribution.

Considering a system with n channels, we note that the following symmetry assumptions apply for most parametric CCF models:

- There is a complete symmetry in the n channels, and the components of each channel have the same constant failure rate (*i.e.,* independent of time). Further, all specific combinations where k channels are failing and $n-k$ channels are not failing have the same probability to occur.
- Removing j of the n channels will have no effect on the probabilities of failure of the remaining $n-j$ channels.

These assumptions imply that we do not have to specify completely new parameters for each n. The parameters defined to handle CCF for $n = 2$ are retained for $n = 3$, and so on.

Remark: Beckman [29] claims that the susceptibility to CCF is architecture sensitive and postulates that triple redundant architectures are three times more sensitive to CCF than dual architectures. He does not, however, give any formal justification for his assertions.

In the remaining part of this section we first consider the main example of Z having a parametric model. Next we look at the general cases, in particular the so-called multiple Greek letter model. Finally we present the multiple beta-factor (MBF) model and a special case of this model.

39.2.6 The Binomial Failure Rate Model and Its Extensions

The binomial failure rate (BFR) model was introduced by Vesely [30] and is a special case of the Marshall-Olkin's multivariate exponential model [31]. The situation under study is the following: A system is composed of n identical channels. Each channel can fail at a random time, independent of each other, and they are all supposed to have the same individual (independent) failure rate λ_I.

The BFR is based on the premise that CCFs result from shocks to the system [23]. The shocks occur randomly according a homogeneous Poisson process with rate ν. Whenever a shock occurs, each of the individual channels is assumed to fail with probability p, independent of the states of the other channels. The number Z of channels failing as a consequence of the shock is thus binomially distributed (n, p). The probability that the multiplicity, Z, of failures due to a shock is equal to z is

$$\Pr(Z = z) = \binom{n}{z} p^z (1-p)^{n-z},$$

for $z = 0, 1, \ldots, n$.

The mean number of channels that fail in one shock is $E(Z) = n \cdot p$. The following two conditions are assumed:

- Shocks and independent failures occur independently of each other.
- All failures are immediately discovered and repaired, with the repair time being negligible.

As a consequence, the time between independent failures of a channel, in the absence of shocks, is exponentially distributed with failure rate λ_I, and the time between shocks is exponentially distributed with rate ν. The number of independent failures in any time period of length t_0 is therefore Poisson distributed $\lambda_i \cdot t_0$, and the number of shocks in any time period of length t_0 is Poisson distributed $\nu \cdot t_0$.

The channel failure rate caused by shocks thus equals $p \cdot \nu$, and the total failure rate of one channel equals

$$\lambda = \lambda_I + p \cdot \nu$$

By using this model, we have to estimate the independent failure rate λ_I and the two parameters ν and p. The parameter ν relates to the degree of "stress" on the system, while p is a function of the built-in channel protection against external shocks. Note that the BFR model is identical to the beta-factor model when the system has only two channels.

This is Vesely's original BFR model. The statistical analysis of such models is discussed by Atwood [32]. Several aspects of the situation must be clarified to make the analysis possible. It may, for example, happen that ν cannot be estimated in a direct way from failure data, because shocks may occur unnoticed when no channel fails.

Several extensions of Vesely's BFR model have been studied. It may, for example, happen that p varies from one shock to another. One way of modeling this is to assume p to be beta distributed, that is, it has a beta distribution with parameters r and s. Such an approach is discussed, for example, by Hokstad [33]. He introduces a re-parameterization of the beta

distribution. Instead of r and s, the model can be expressed by the shock rate and a measure of dependence between the failure of two channels. The model reduces to the beta-factor model and the BFR model, respectively, for specific choices of model parameters.

The assumption that the channels will fail independently of each other, given that a shock has occurred, represents a rather serious limitation, and this assumption is often not satisfied in practice. The problem can, to some extent, be remedied by defining one fraction of the shocks as being "lethal" shocks, that is, shocks that automatically cause all the channels to fail $p = 1$. If all the shocks are "lethal," one is back to the beta-factor model. Observe that this case $p = 1$ corresponds to the situation that there is no built-in protection against these shocks.

Situations where independent failures may occur together with non-lethal as well as lethal shocks are often realistic. Such models are, however, rather complicated, even if the non-lethal and the lethal shocks occur independently of each other.

39.2.7 The Multiple Greek Letter Model

A large number of further extensions of the beta-factor model have been suggested, for example, by Apostolakis and Moieni [34]. Some models allow a completely general multiplicity distribution. However, different parameterizations give rise to different models. Three of the most well known models are

- The basic parameter (BP) model [35]
- The alpha factor model [36, 37]
- The multiple Greek letter (MGL) model [38]

The MGL model was introduced by Fleming *et al*. [38] and is briefly discussed below. A more recent model, the multiple beta-factor (MBF) model is presented in the next section.

In the MGL model various conditional probabilities are introduced, and for a system with $n = 3$ channels (say, A_1, A_2, and A_3) we define:

$\beta =$ the conditional probability that the cause of a failure of a specific channel will be shared by at least one additional channel.

$\gamma =$ the conditional probability that a channel failure known to be shared by at least one additional channel will be shared by at least two additional channels. Additional Greek letters are introduced for systems of higher order n. Here, β is the probability that, given one channel (A_1) has failed, at least one of the other $n-1$ will also fail (either A_2 or A_3 or both for a system of three channels). We note that the beta-factor model is a special case of the MGL model when $n = 2$, and also when all the parameters of the MGL model, except for β, are equal to 1.

In a system of three channels, this model implies that the channel failure probability, Q, can be split as follows:

Pr(channel has a single failure) $= 1 - \beta \cdot Q$.
Pr(channel has a double failure) $= \beta(1-\gamma) \cdot Q$.
Pr(channel has a triple failure) $= \beta\gamma \cdot Q$.

Here, $\beta(1-\gamma)$ is the probability that, given one channel (A_1) has failed, also exactly one additional channel (either A_2 or A_3) has failed. Similarly, $\beta\gamma$ is the probability that given one channel (A_1) has failed, then both A_2 and A_3 have also failed. In this way we can for any n give the probability of failure of any multiplicity expressed by conditional probabilities (Greek letters).

39.2.8 The Multiple Beta-factor Model

The multiple beta-factor (MBF) model [39] is, like the MGL, completely general, since any multiplicity distribution can be adapted. However, in the MBF model the rate of CCF causing system failure for a *koon* configuration is given as $\lambda_{koon} = C_{koon} \cdot \beta\lambda$. Here λ is the channel failure rate, β is the beta-factor (of two channels), and C_{koon} is a *configuration factor* taking into account the reliability structure of the *koon* system. The same β is used for all configurations. Further, the MBF model uses $C_{1oo2} = 1$, and the β used in MBF will for $n = 2$ channels have the same interpretation as in the beta-factor model.

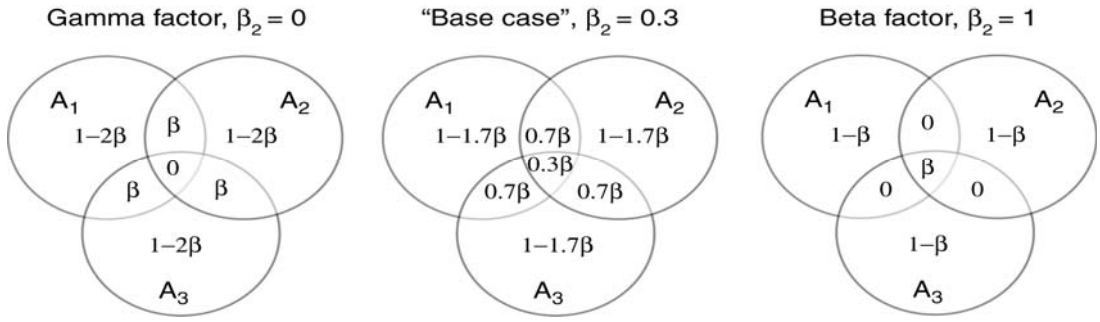


Figure 39.2. Illustration of the multiple beta-factor (MBF) model for a triplicated system $(n=3)$. Three different choices of the parameter β_2

Analogously, if Q is the probability of a channel being in the failed state, the probability of a *koon* configuration being in the failed state due to a CCF equals $Q_{koon} = C_{koon} \cdot \beta \cdot Q$. This factorization of the system failure probability Q_{koon} into the single channel failure probability (Q), the double channel failure probability (β), and the multiple channel failure probability (C_{koon}) is the key feature of the modeling. For Q and β there should be data available for estimation, and a "plant specific" β could be estimated, for example, using the approach in IEC 61508 [3].

As there is often rather limited information available to carry out a formal estimation of the C_{koon} factors, we may as a starting point apply a set of *generic* values that can be applied in quick and simple analyses when limited information on the multiplicity of CCF is available. This will then represents a modeling of intermediate complexity, in between the very simple beta-factor model and the rather detailed modeling (as multiple Greek letter model) used by some analysts for instance in the nuclear industry. If some consensus can be reached on generic C_{koon} values, then more realistic input, and better decision support is obtained than by just applying $C_{koon} = 1$ for all configurations, as suggested by the beta-factor model.

In order to give explicit formulas for C_{koon}, we introduce the probability, β_j that channel $j+1$ fails, given that channels $1, 2, \ldots, j$ have just failed in a CCF.

Note that $\beta_1 = \beta$. In order to analyze a system with three channels, we also need to specify β_2, and so on. Figure 39.2 illustrates the case for $n=3$.

The probability $f_{k,n}$ that exactly k of the n channels are failed can now be expressed by these β values [39] and the probability of system failure due to a CCF is given as

$$Q_{koon} = \Pr(\text{at least } n-k+1 \text{ channels fail in CCF}) = \sum_{j=n-k+1}^{n} f_{j,n}$$

We can write $Q_{koon} = C_{koon} \cdot \beta \cdot Q$, where C_{koon} is independent of β and Q. The configuration factors C_{koon} are given explicitly as a function of β_k, for $k = 2, 3, \ldots, n-1$.

Example (Special Case $n=3$)

This parameterization easily gives the multiplicity results for a system of $n=3$ channels (see Figure 39.2).

By direct probabilistic arguments, it follows that the probability of the system having k $(=1,2,3)$ channels failed equals

$$f_{1,3} = 3[1-(2-\beta_2)\beta]Q$$
$$f_{2,3} = 3(1-\beta_2)\beta Q$$
$$f_{3,3} = \beta_2\beta Q$$

For a 1oo3 configuration, system failure occurs if all three channels fail, and thus the probability of system failure due to CCFs is $Q_{1oo3} = f_{3,3} = \beta_2\beta Q$. This directly gives $C_{1oo3} = \beta_2$. For a 2oo3 configuration, the system fails if at least two channels fail, and the probability of system failure equals $Q_{2oo3} = f_{2,3} + f_{3,3} = (3-2\beta_2)\beta Q$, directly giving $C_{2oo3} = 3-2\beta_2$.

The parameter β_2 can take any value in the interval [0, 1]. Choosing the value $\beta_2 = 1$, we get the ordinary beta-factor model. The other extreme, $\beta_2 = 0$, is here referred to as the *gamma factor model* (see Figure 39.2). Note that the value $\beta_2 = 0.3$ is introduced as a *base case*. This gives $C_{1oo3} = 0.3$, $C_{2oo3} = 2.4$, being factors that are easily recognized in Figure 39.2 (as $C_{2oo3} = 0.7 + 0.7 + 0.7 + 0.3$).

Since the explicit expressions for the configuration factors, C_{koon}, are rather complex for large n, and since there is often few data available to perform separate estimation of all $\beta-$ s, some simplification of the model is appropriate. One special case is that $\beta_j = \beta_p$, for all $j \geq p$. Here we select $p = 3$.

Special Case: $\beta_j = \beta_3$ for $j \geq 3$.

It follows that [39]

$$C_{koon} = \beta_2 \sum_{j=n-k+1}^{n} \binom{n}{j} \beta_3^{j-3}(1-\beta_3)^{n-j}$$

for $k = 1, 2, \ldots, n-2$.

$$C_{(n-1)oon} = \binom{n}{2}(1-\beta_2/\beta_3) + \beta_2 \sum_{j=2}^{n} \binom{n}{2} \beta_3^{j-3}(1-\beta_3)^{n-j}$$

The choice of β_2 has indeed a dominant effect on the configuration factors. The two extremes, $\beta_2 = 0$ and $\beta_2 = 1.0$, usually give quite unrealistic models. However, the knowledge about the "true" β_2 is in many cases very limited. So it is useful to define a generic value as a *base case*, applicable when little information is available. If we strictly remove common channels as cause of the CCF, and if we are rather restrictive with the meaning of *simultaneous* failure, it is believed that the typical β_2 value is usually closer to 0 than 1, and somewhat arbitrarily the value $\beta_2 = 0.3$ is suggested (based on some previous expert judgment for failure multiplicity distributions of safety systems). Also $\beta_2 = 0.5$ could be a reasonable choice when little information is available. For $k \geq 3$ the value $\beta_k = 0.5$ is suggested unless more information is available. Table 39.6 presents some numerical results (sensitivities) for C_{koon}. The following examples are given

- *Sensitivity 1*: $\beta_k = 0.3$ for all $k \geq 2$;
- *Base case*: $\beta_2 = 0.3$; $\beta_k = 0.5$ for all $k \geq 3$;
- *Sensitivity 2*: $\beta_k = 0.5$ for all $k \geq 2$.

Note that there are two real extreme (most often unrealistic) cases:

Table 39.6. Numerical values of configuration factors (Note: $C_{1oo2} = 1$)

Parameter choice	Configuration factor C_{koon}				
	1oo3	**2oo3**	**1oo4**	**2oo4**	**3oo4**
$\beta_j = 0.3$ $(j \geq 2)$	0.3	2.4	0.09	0.93	3.9
Base case	0.3	2.4	0.15	0.75	4.0
$\beta_j = 0.5$ $(j \geq 2)$ β_k	0.5	2.0	0.25	1.25	2.8

- The "gamma factor model" ($\beta_k = 0$ for all $k \geq 2$) gives $C_{(n-1)oon} = \binom{n}{2}$ and $C_{koon} = 0$ for $k < n-1$
- The beta-factor model ($\beta_j = 1$ for all $j \geq 2$) gives $C_{koon} = 1$ for all $k < n$.

Such a table can also be used for sensitivity considerations, for example, regarding the ranking of configurations. As expected 1oo4 is ranked the best of these configurations, and 3oo4 is the worst with respect to CCF. However, it may be hard to distinguish 2oo4 from 1oo2, unless more explicit data are available.

39.3 Data Collection and Analysis

This section reviews recent data sources for CCF and discusses some questions related to parameter estimation and to the collection and analysis of data that are used as input to CCF model estimation.

Today, CCF must be considered rare events, and the individual plants present limited experience. Thus, global industry experience is needed to make statistical inferences. Then there can be need for "data mapping." This is used when we have data from systems with different degree of multiplicity/redundancy. However, if data from different plants are used, it must be kept in mind that there could be a significant variability amongst the plants.

39.3.1 Some Data Sources

Rather few data sources on CCF are available. To a large extend they are from the nuclear industry.

Some data are rather old, and a few sources are listed in Hokstad [40]. Here we restrict to discuss the ICDE data base and SKI data.

The ICDE data base:

The best recent source of CCF data is probably the International Common Cause Failure Data Exchange (ICDE) project [41].

The ICDE project was initiated in 1994 and collects and analyzes CCF event data from the nuclear industry in nine OECD countries. Since April 1998, the project has been operated by the Nuclear Energy Agency (NEA). The objectives of the ICDE project are to:

1) Collect and analyze CCF events over the long term so as to better understand such events, their causes, and their prevention.
2) Generate qualitative insights into the root causes of CCF events which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences.
3) Establish a mechanism for the efficient feedback of experience gained in connection with CCF phenomena, including the development of defences against their occurrence, such as indicators for risk based inspections.
4) Generate quantitative insights and record event attributes to facilitate quantification of CCF frequencies in member countries.
5) Use the ICDE data to estimate CCF parameters.

Various summary reports are available on the internet also for non-members. Examples of available ICDE project reports are (see http://www.-eskonsult.se/icde/):

- Collection and analysis of common-cause failure of safety and relief valves.
- Collection and analysis of common-cause failure of check valves.
- Proceedings of the ICDE workshop on qualitative and quantitative use of ICDE data.

ICDE also gives general recommendations regarding classification of CCF data, for example regarding

- Coupling factors
- Root causes

- Corrective actions
- Detection methods

The project has published papers on "lessons learned" and general insight and results from the CCF data collection [42–44]; all papers appearing at the PSAM/ESREL conference in 2004.

SKI data reports:

SKI (Statens Kärnkraft Inspektion/Swedish Nuclear Power Inspectorate) has through several reports investigated CCFs in boiling water reactors (BWR). In particular, [45] gives actual data on safety/relief valves (SRV), and the number of SRVs usually varies from 12 to 16 in these systems. The analysis is based on data from different BWR generators, located in Forsmark, Oskarshamn, Barsebäck, and Ringhals. The database contains about 200 events, and failures are classified according to severity, failure mode, detection method, and which part of the channel that failed. Failure cause is given, and the multiple events are classified as "actual CCFs", "potential CCFs" or "recurring faults". A couple of other relevant reports from SKI are [46, 47], where [47] covers events that potentially lead to CCF. Such events, named "common cause initiators," are not just causing a disturbance in plant operation, but can also degrade or even disable the function of a safety system that is needed to cope with the disturbances.

The SKI project undertakes the following tasks:

- SRV data analysis: data being collected from Finnish and Swedish BWR plants.
- Specification of reference application: Detailed study on one plant in order to test analysis methods.
- Application and comparison of CCF models: A number of different CCF models are employed, and their applicability in high redundancy systems is discussed.
- Conclusions and recommendations: Give qualitative insights from the CCF mechanisms and possible defenses.

39.3.2 Parameter Estimation

The standard estimators for the parameters of main CCF models are given in Mosleh [35], and are referred, for example, in [40]. Here we restrict ourselves to discuss the estimation of beta-factors, referring to the MBF model and the standard beta-factor model. We let

$X_{k,n} =$ the number of observed failure events resulting in exactly k channels failing of a system with n channels (*i.e.*, the number of failures of multiplicity k).

$\hat{\beta}_{k,n} =$ estimator for β_k (see the MBF model), based on data from a system with n channels.

It is of some interest to compare the estimator of β_1 in the MBF model with the estimator of β in the standard beta-factor model. Considering now a system with n channels, Hokstad *et al*. [48] give the following estimator for $\beta = \beta_1$

$$\hat{\beta}_{1,n} = \frac{\sum_{j=2}^{n} j \cdot \frac{j-1}{N-1} X_{j,n}}{\sum_{j=1}^{n} j \cdot X_{j,n}} .$$

The beta-factor model is a special case of the MBF model, by letting $\beta_j = 1$ for all $j \geq 2$. However, the definition of $\beta_1 = \beta$ is not identical in the two models. The "ordinary" β is the probability that *all* other channels are affected, given the failure of a specific channel, and the β_1 of the MBF model is the probability that a specific other channel is affected. So the interpretation of the two β's coincide only for $n = 2$.

For a n-channels system a commonly suggested estimator for β is (*e.g.,* see [35, 48]):

$$\beta^* = \frac{\sum_{j=2}^{n} j \cdot X_{j,n}}{\sum_{j=1}^{n} j \cdot X_{j,n}}$$

and, as expected, for $n = 2$, the two estimators coincide. However, for $n > 2$, the beta-factor model has a problem with the estimation. The model does not allow for CCFs of multiplicities less than n. However, the estimator of β includes failures of all multiplicities. Since these failures of multiplicity $< n$ actually do occur, (and thus should be accounted for), there will necessarily

become some sort of discrepancy between the theoretical model and the estimator. Irrespective of how these $X_{j,n}$ for $j < n$, are taken into account, it will imply an interpretation of β^* that differs from that of the actual β in the beta-factor model.

The above estimator β^* seems related to the definition of β in the multiple Greek letter (MGL) model. Here the beta-factor is defined as the conditional probability that the cause of a failure of a specific channel will be shared by *at least one* additional channel; (*i.e.*, given one channel has failed, at least one of the other $n-1$ will also fail).

To highlight this interpretation, we compare $\hat{\beta}_{1,3}$ and β^* for the case $n = 3$. Then

$$\beta^* = \frac{2X_2/3 + X_3}{X_1/3 + 2X_2/3 + X_3}$$

$$\hat{\beta}_{1,3} = \frac{X_2/3 + X_3}{X_1/3 + 2X_2/3 + X_3}$$

Here the numerator of $\hat{\beta}_{1,3}$ is the number of failure events involving two specific channels, (say A_1 and A_2), and the numerator of β^* is the number of failures involving one channel (say A_1) and *at least* one additional channel (*i.e.*, either A_2 or A_3). Obviously, $\hat{\beta}_{1,3} \le \beta^*$. Actually, from the formula for β^* and $\hat{\beta}_{1,n}$ it is seen that $\hat{\beta}_{1,n}$ is always smaller than β^* when $n > 2$ (as also follows from the definition of β^* and β_1).

It is concluded that the estimator of β in the standard beta-factor model is somewhat inconsistent, (and actually *has to* be inconsistent, due to the definition of β). This is another argument for applying more general CCF models.

39.3.3 Impact Vector and Mapping of Data

For each failure event of a system with n channels exposed to CCF we may define an impact vector [37]. This vector has $n+1$ elements, one for each value for number of failures. The vector can be written $(I_0, I_1, \ldots, I_n)$, where $I_k = 1$ if the outcome is that exactly k of the n channels fail, and 0 otherwise.

The following two main problems are encountered in the use of CCF data:

- The CCF events are often not well defined, giving rise to various hypotheses regarding how many (which) channels have failed; (*i.e.*, the I_k are random variables rather than indicator variables).
- Scarcity of data will imply that it is needed to apply data from various plants to assess CCF probabilities/rates; (or we have the situation that the data comes from a *source* plant with operational experience, but are going to be applied on a *target* plant). Then it is required to investigate differences between the plants with respect to environment, operations, *etc*. If, in addition, the various plants have different n values, it is also required to *map* the data before they can be used on the target plant.

The use of a stochastic impact vector is discussed by Knochenhauer *et al.* [49] who give an example for diesel generators, and includes uncertainty estimation of CCF parameters (Bayesian approach). Another estimation approach is given by Xie [50]. He uses a "knowledge-based multi-dimension discrete" (KBMD) CCF to assess probabilities of the various failure multiplicities. Here various environment load-channel strength relationships are embodied implicitly. The approach can be used to estimate high redundancy system CCF based on low multiplicity failure event data of the system. The results of the KMBD model regarding multiplicity distribution are also compared with other models.

We have the general problem that failure events observed at one or few plants are often not sufficient to estimate the parameters of the CCF model. So, assimilating experience from other plants may be essential. However, the plants may have different lay-out, design and channel separation principles. So there is a need to assess similarity/applicability, to assess applicability/-modification factors.

When source and target plant have different numbers of channels (n-values, different degree of

redundancy), we need to use data mapping [37, 51]. In particular, the impact vector of the source plant is mapped up/down to the impact vector of the target plant, and thus derives the expected failure probabilities of various failure multiplicities in a "corresponding" failure event with the n-value of the target plant. Also Hokstad *et al.* [48] use data mapping in the estimation of the parameters of MBF model, assuming data coming from plants with different n-values.

Vaurio [52] has recently given a comprehensive discussion on the topic of mapping, related to estimation in CCF models. He refers to two kinds of generic mapping-down rules, based on two different CCF mechanisms and assumptions:

- The first set of mapping down rules can be obtained assuming *externally caused* CCFs, and assuming that the plants with $n-1$ channels are similar to the plants with n channels with one channel removed. "Similarity" here means that all cause events occur with the same frequency and have equal consequences, *i.e.*, the cause events fail existing channels equally likely at both families of plants.
- The second set of mapping down rules has been developed for cascading failures or *channel-caused* CCFs, meaning that a single channel failure causes other channels to fail with certain probabilities. Furthermore, it is assumed that plants with $n-1$ channels have the same single failure rates and the same failure propagation probabilities as the plant with n channels.

Both kinds of events can occur in reality, and both sets of rules assume identical design, separation, operations and maintenance principles in plants with different sizes n. Such mapping rules are purely mathematical, based on combinatorial arguments. Further references are found in [52], who also presents mapping-*up* rules suggested in the literature.

It can be shown that the mapping down equations for the weights of the impact vectors are based on the ideal case of *externally caused* CCF as defined above [53].

39.4 Concluding Remarks and Ideas for Further Research

The beta-factor model is by far the most commonly used CCF model, and its use is also supported by standards like IEC 61508 [3]. A main challenge related to using the beta-factor model is to estimate/choose an appropriate, plant specific value of β. A range of "tools" [3, 19, 24, 26] have been proposed for this purpose. Several of these "tools" have been developed based on experience without any structured basis. Zitrou *et al.* [28] propose to use a more structured approach based on influence diagrams. This is a promising approach that should be subject to further research.

CCFs are especially important for safety instrumented systems (SIS). A SIS has two main failure modes [18]: Fail to function on demand (FTF) and spurious operation (SO). The method in IEC 61508 [3] part 6 is applicable for FTF failures. In most practical analyses, however, analysts tend to use the same estimate for β both for FTF and SO failures. This is an erroneous approach since the mechanisms leading to the two failure modes are totally different. More research should be devoted to estimating β for common cause SO failures. SO failures can in some cases be safety critical, and even more critical than FTF failures. Consider, for example, the airbag system in a car. If the airbag does not function as intended in a crash, we have an FTF failure. If the airbag blows up spuriously, we have a SO failure. The consequences of the SO failure will depend on the situation in which it occurs. It is easy to imagine a situation where an SO failure of the airbag will give fatal consequences.

The approach described in IEC 61508 [3] part 6 for estimating a plant specific β results in one out of a few distinct values for β. This implies that we have to make rather significant improvements to the system, environment or operational procedures to see any effect on the value of β. In situations where a contractor is obliged to follow the IEC 61508 procedure, he may be de-motivated in his efforts to make improvements, because it does not show any effects on the calculated PFD. The procedure in IEC 61508 should therefore be

replaced by a new procedure that is more sensitive to improvements.

Another issue is related to the understanding of how various types of diagnostic testing may influence the occurrence of CCFs, and how to take account of the diagnostic testing when estimating β. More research is also needed to fully understand how the practical inspection and testing procedures – and human errors, influence on the occurrence of CCFs.

When we establish models for systems exposed to CCFs, it is important to start by identifying the significant causes for CCFs and to include these causes explicitly into the model. More research should be devoted to developing checklists and other tools that can support the explicit modeling of CCFs. Such tools need to be based on a thorough understanding of the physical mechanisms that may lead to CCF.

It is further observed that all current implicit models are based on the exponential failure model. The occurrence of CCF in models with deterioration (*e.g.,* Weibull models) should be further investigated.

Above we observed that the mapping down equations for the weights of the impact vectors are based on the ideal case of *externally caused* CCF, as defined above. This generally seems to be the case in the current literature, and could be a topic for development to further investigate alternative, or more general models to this CCF mechanism.

A final topic for further research related to CCFs is to apply fuzzy logic in the collection and utilization of input data to determine the specific CCF parameters. See, for example, Maisseu and Xingquan [54] for a recent reference.

References

[1] NUREG-75/014. Reactor safety: An assessment of accident risk in U.S. commercial nuclear power plants, WASH-1400. U.S. Nuclear Regulatory Commission, Washington, D,. 1975.

[2] Hauge S, Hokstad P, Langseth H. Øien K. Reliability prediction method for safety instrumented systems. PDS method handbook, edition. Report STF50 A06031, Sintef, Trondheim, Norway. 2006.

[3] IEC 61508. Functional safety of electrical/ electronic/programmable electronic safety-related systems. Parts 1–7. International Electrotechnical Commission, Geneva 1997.

[4] Smith AM, Watson IA. Common cause failures – a dilemma in perspective. Reliability Engineering 1980; 1(2):127–142.

[5] NEA. International common-cause failure data exchange. ICDE general coding guidelines. Technical note NEA/CSNI/ R(2004)4. Nuclear Energy Agency, 2004.

[6] NASA. Probabilistic risk assessment procedures guide for NASA managers and practitioners. NASA Office of Safety and Mission Assurance. Washington. DC, 2002.

[7] Littlewood B. The impact of diversity upon common mode failures. Reliability Engineering and System Safety 1996; 51:101–113.

[8] Parry GW. Common cause failure analysis: A critique and some suggestions. Reliability Engineering and System Safety1991; 34:309–320.

[9] Paula HM, Campbell DJ, Rasmuson DM. Qualitative cause-defense matrices: Engineering tools to support the analysis and prevention of common cause failures. Reliability Engineering and System Safety 1991; 34:389–415.

[10] DOE. Root cause analysis guidance document. Report no. DOE-NE-STD-1004-92. U.S. Department of Energy, Washington, DC, 1992.

[11] Rasmuson DM. Some practical considerations in treating dependencies in PRAs. Reliability Engineering and System Safety 1991; 34:327–343.

[12] Miller AG, Kaufer B, Carlson L. Activities on component reliability under the OECD nuclear energy agency. Nuclear Engineering and Design 2000; 198:325–334.

[13] Cooper SE, Lofgren EV, Samanta PK, Wong S-M. Dependent failure analysis of NPP data bases. Nuclear Engineering and Design 1993; 142:137–153.

[14] Mosleh A, Rasmuson DM, Marshall FM. Guidelines on modeling common-cause failures in probabilistic risk assessment. U.S. Nuclear Regulatory Commission, Washington, DC, NUREG/CR-5485, 1998.

[15] Childs JA, Mosleh A. A modified FMEA tool for use in identifying and assessing common cause failure risk in industry. Proceedings Annual Reliability and Maintainability Symposium, Washington D.C.; Jan. 18–21, 1999; 19–24.

[16] Hauge S, Onshus T, Øien K, Grøtan TO, Holmstrøm S, Lundteigen MA. Independence of

safety systems on offshore oil and gas installations – Status and challenges (in Norwegian). Report STF50 A06011, Sintef, Trondheim, Norway, 2006.
[17] NASA. Fault tree handbook with aerospace applications. NASA Office of Safety and Mission Assurance, Washington. DC, 2002.
[18] Rausand M, Høyland A. System reliability theory; models, statistical methods, and applications, 2nd edition. Wiley, New York. 2004.
[19] Johnston BD. A structured procedure for dependent failure analysis (DFA). Reliability Engineering 1987; 19:125–136.
[20] Fleming KN. A reliability model for common mode failures in redundant safety systems. Report GA-A13284, General Atomic Company, San Diego, CA, 1975.
[21] OREDA. Offshore reliability data, 4th ed. Available from: Det Norske Veritas, NO 1322 Høvik, Norway, 2002.
[22] MIL-HDBK 217F. Reliability prediction of electronic equipment. U.S. Department of Defense, Washington, DC, 1991.
[23] Evans MGK, Parry GW, Wreathall J. On the treatment of common-cause failures in system analysis. Reliability Engineering 1984; 9:107–115.
[24] Humpreys RA. Assigning a numerical value to the beta factor common cause evaluation. Reliability '87. Proceedings paper 2C; 1987.
[25] Smith DJ, Simpson KGL. Functional safety – A straightforward guide to applying the IEC 61508 and related standards. Elsevier, Burlington, UK, 2005.
[26] Brand PV. A pragmatic approach to dependent failures assessment for standard systems. AEA Technology plc.1996.
[27] Zitrou A, Bedford T. Foundations of the UPM common cause model. In: Bedford T, Gelder PH. van, eds. Safety and Reliability. Balkema, ESREL 2003; 1769–1775.
[28] Zitrou A, Bedford T, Walls L. Developing soft factors inputs to common cause failure models. In: Spitzer C, Schmocker U, Dang VN, eds. Probabilistic safety assessment and management. Springer, Berlin, 2004; 825–830.
[29] Beckman LV. Match redundant system architectures with safety requirements. Chemical Engineering Progress 1995; December: 54–61.
[30] Vesely WE. Estimating common.cause failure probabilities in reliability and risk analyses: Marshall-Olkin specializations. In: Assessment J, Fussell B, Burdick GR, eds. Nuclear systems reliability engineering and risk. SIAM, Philadelphia, 1977; 314–341.
[31] Marshall AW, Olkin I. A multivariate exponential distribution. Journal of the American Statistical Association 1967; 62:30–44.
[32] Atwood CL. The binomial failure rate common-cause model. Technometrics1986; 28(2):139–148.
[33] Hokstad P. A shock model for common-cause failures. Reliability Engineering and System Safety 1988; 23:127–145.
[34] Apostolakis G, Moieni P. The foundations of models of dependence in probabilistic safety assessment. Reliability Engineering 1987; 18(3):177–195.
[35] Mosleh A. Common cause failures: An analysis methodology and example. Reliability Engineering and System Safety 1991; 34:249–292.
[36] Mosleh A, Siu NO. A multi-parameter common cause failure model. 9th International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, Aug. 17–21, 1987; 147–152.
[37] Mosleh A, Fleming KN, Parry GW, Paula HM, Worledge DH, Rasmuson DM. Procedures for treating common cause failures in safety and reliability studies. Analytical Background and Techniques. (EPRI NP 5613). U.S. Nuclear Regulatory Commission, Washington, DC, NUREG/CR-4780 1989; 2.
[38] Fleming KN, Mosleh A, Deremer RK A systematic procedure for the incorporation of common cause events into risk and reliability models. Nuclear Engineering and Design 1985; 93:245–279.
[39] Hokstad P, Corneliussen K. Loss of safety assessment and the IEC 61508 standard. Reliability Engineering and System Safety 2004; 83:111–120.
[40] Hokstad P. Common cause and dependent failure modeling. In: Misra KB, editor. New Trends in system reliability evaluation. Chapter 11, Elsevier, Amsterdam, 1993; 411–444.
[41] ICDE. International Common Cause Failure Data Exchange Project. http://www.nea.fr/html/jointproj/icde.html
[42] Baranowsky P, Rasmuson D, Johanson G, Kreuser A, Pyy P, Werner W. General insights from the international common cause failure data exchange (ICDE) project. In Proceedings PSAM 7 ESREL Berlin; June 14–18, 2004:70–75.
[43] Tirira J, Werner W. Lessons learnt from data collected in the ICDE project. In Proceedings PSAM 7, ESREL, Berlin; June 14–18, 2004:82–87.
[44] Johanson G, Jonsson E, Jãnkãlã K, Pesonen J, and Werner W. Insights and results from the analyses

of common-cause failure data collected in the ICDE Project for Safety and Relief Valves. In Proceedings PSAM 7, ESREL, Berlin; June 14-18, 2004: 88–93.

[45] SKI, CCF analysis of high redundancy systems, safety/relief valve data analysis and reference BWR application. SKI Technical Report 91:6, Stockholm. http://www.ski.se/extra/document/?instance=1&action_show_document.122.=1 1992.

[46] SKI, Analysis of CCF for hydraulic scram and control rod systems in BWRs. http://www.ski.se/dynamaster/file_archive/030117/f6fefeb66a3209faccd6387d4f804bf2/96%2d77.pdf 1996.

[47] SKI, Investigates events that (potentially) lead to CCF. SKI Technical Report 98:09. http://www.ski.se/dynamaster/file_archive/010803/97837624857/98%2d9.pdf ; 1998.

[48] Hokstad P, Maria A, Tomis P. Estimation of common cause factors from systems with different numbers of channels. IEEE Transactions on Reliability 2006; 55(1):18–25.

[49] Knochenhauer M, Mankamo T, Pörn K. Analysis and modelling of dependent failures. In Proceedings from PSAM 7, ESREL, Berlin; June 14-18, 2004; 831–836.

[50] Xie L. A knowledge-based multi-dimension discrete common cause failure model. Nuclear Engineering and Design 1998; 183:107–116.

[51] Kvam PH, Miller JG. Common cause failure prediction using data mapping. Reliability Engineering and System Safety 2002; 76:273–278.

[52] Vaurio JK. Consistent mapping of common cause failure rates and alpha factors. Reliability Engineering and System Safety 2007; 92:628–645.

[53] Mosleh A, Fleming KN, Parry GW, Paula HM, Worledge DH, Rasmuson DM. Procedures for treating common cause failures in safety and reliability studies. Procedural framework and examples. (EPRI NP 5613). U.S. Nuclear Regulatory Commission, Washington, DC, NUREG/CR-4780 1988; 1.

[54] Massieu A, Xingquan W. Fuzzy parametrization of Bulgaria's nuclear policy decision. Journal of Performability Engineering 2005; 1(2):167–178.

40

A Methodology for Promoting Reliable Human–System Interaction

Joseph Sharit

Department of Industrial Engineering,
University of Miami, Coral Gables, Florida, 33124-0623, USA

Abstract: A qualitative methodology is proposed that can help both designers and managers anticipate problems, which are often manifest as human errors, that people will have in interacting with various products and systems. The methodology adapts a number of well-known hazard evaluation techniques so that they can be applied to human performance, and combines them in a way that increases the analytical team's ability to predict the possibility for human performance failures and their consequences. A basis is also provided for examining explanations for these failures, and for providing categorical severity and likelihood assessments of these consequences. The importance of assessing the impact of barriers on adverse consequences is also discussed.

40.1 Introduction

Despite enormous technological advances in products, services, and industrial work processes, the human remains and will likely remain an integral system component. In some cases, particular operations or system functions either cannot be automated or cannot be done so with sufficient reliability, thus requiring the human's presence. In other cases, human-system interaction is necessary if only for enabling the human to acquire an adequate account of ongoing system information, which provides the opportunity for adapting the system to changing events and for implementing interventions that can lead to system improvement. Designers, managers, and supervisors of these systems are faced with a challenging goal: how does one ensure that the human's presence does not lead to adverse outcomes such as injuries, poor system performance, and economic losses, while at the same time allow the human the flexibility to engage in the kinds of activities that can promote a better understanding of system operations, and ultimately improved system performance?

This broad objective is often stated in terms of the seemingly simpler goal of minimizing human "errors" and violations that could undermine joint human-system performance. Human reliability, which in its most literal sense represents the analogue of mechanical component reliability, has been defined as the probability of successful completion of an activity or task within some prescribed or implied time period. If we identify an activity or cluster of activities dedicated to meeting some task objective, and consider the criteria that denote successful performance of that activity or task, then strictly speaking failure to meet these

criteria represents human failure. In human reliability analysis (HRA), human failures are represented by human errors in task performance. Quantitative perspectives to HRA focus on obtaining quantitative estimates of these errors, and there exist a variety of methods intended for meeting this goal [1, 2, 3]. The importance of quantitative HRA derives from the need, either mandated or governed by management policy, to supply analysts with quantitative estimates of human reliability in order to more accurately account for the risks associated with systems that encompass human, equipment, and environmental aspects.

With technology evolving at very rapid rates, forcing continual modifications to existing systems and possibly even to the organizational structures that are responsible for managing them, many designers and managers face more fundamental issues. Specifically, they would like to know: (1) how the designs or operations that they are responsible for might lead to human error or violations; (2) what the potential consequences of these human behaviors are; and (3) what barriers or safeguards can prevent or mitigate the potentially negative consequences of these behaviors while, at the same time, not introduce new opportunities for human errors and violations. This set of challenges represents a qualitative perspective to HRA. Quantitative perspectives often require sufficient resolution of qualitative considerations in order to address the goal of quantitative human error estimation. Obviously, if potentially erroneous actions are not identified, then their quantification cannot be considered and the risks to the system are underestimated.

The most common tools for incorporating estimates of human error into quantitative system risk assessments are fault tree (FT) analysis and event tree (ET) analysis [2]. FTs use Boolean AND and OR operations to determine deductively the combinations of events that are capable of causing some unwanted top event. ETs use an initiating event as a starting point and, through inductive reasoning, infer different accident scenarios that can be propagated depending on whether various barriers or mitigating actions are successfully applied. In either case human actions may need to be considered. FTs and ETs are often used in combination, where FTs serve to determine the possibilities of success for each mitigative or barrier function represented along the path of accident propagation within the ET. Both FTs and ETs can be used qualitatively by deriving cut sets. A cut set is a set of one or more events which, if all occur, can result in the occurrence of the top event in a FT or in the designated accident scenario in an ET. It is when human actions need to be considered and quantitative risk analysis studies are required that risk analysts will be compelled to obtain quantitative estimates of human errors.

The earlier approaches to HRA, whether relatively resource efficient such as TESEO (*tecnica empirica stima errori operati*) [4], or very resource intensive such as THERP (technique for human error rate prediction) [5], generally suffered from an inability to adequately account for human involvement that is of a more cognitive nature and for the complexity of the various contexts in which the human performs. The "second-generation" approach to HRA, referred to as CREAM (cognitive reliability and error analysis method) [3], in its qualitative form, does overcome some of these limitations, especially in its ability to create elaborate linkages between various work conditions in order to predict events. However, once the method shifts the objective to human quantitative performance prediction it, like all such approaches, must resort to some type of decomposition-aggregation scheme whereby factors characterizing the work context are decomposed and, according to some rule or scheme, aggregated to provide a quantitative estimate.

Although the decomposition-aggregation cycles inherent to these approaches can be very revealing of issues and factors that can undermine system reliability, the conceptual understanding that is needed for promoting organizational learning will often be masked by the emphasis given to generating quantitative estimates of human error. Thus the goal of quantitative approaches to human reliability assessment can be disruptive. A more reasonable approach would be to identify the ways in which human activities or required behaviors could be erroneous in the sense of potentially

creating hazards or putting some aspect of the system at risk. A risk category—that is, a level of likelihood and severity—could then be associated with the possible consequences of these actions or behaviors; this risk category would be based in part on the explanations that can be considered for failed behaviors. This approach is consistent with the view [6] that encourages "a move away from the search for objective probabilities via standard probabilistic risk assessment tools…toward an exploratory or descriptive approach" (p. 82).

Motivating this approach is the assumption that what designers and managers require, especially when implementing new technologies or managing systems with complex interactions, are the *possibilities* of exposure to risk. Strict quantification of human error generally imposes constraints on analysis due to the need for employing some type of formalization to ensure that a quantitative figure can be arrived at. Although loosening the constraints compelled by strict quantification will necessarily expand the space of possibilities of human behaviors that can cause adverse consequences, it could provide insights that would otherwise be ignored or handled awkwardly if they were to be funneled into a quantitative estimate. The option always exists, however, for extending qualitative perspectives of HRA to quantitative end products [3, 7] if these data are required, for instance, when fault-tree analysts seek human reliability estimates.

To illustrate the need to consider human reliability within a more expanded space of possibilities, consider a designer who is assigned the task of building a computerized physician order system for hospitals. The potential impact of such a system in reducing prescribed medication errors by physicians is enormous. However, there is evidence that such systems can introduce new unforeseen adverse consequences arising from the actions of physicians by virtue of the interplay between the user's information-processing limitations, interface design features, and characteristics of the hospital's organizational structure and policies [8]. Thus a presumed barrier to human error may in fact produce new anticipated "errors" [9], and it has been suggested that it may take many years of organizational learning for these problems to become remedied [10]. Are attempts to provide quantitative estimates of these errors necessary or should we instead attempt to expose them?

As another example, when performing certain work procedures there may be a tendency for workers to invoke short cuts in order to minimize the outlay of effort the procedure calls for or because they feel that the procedure exposes them to unnecessary risks. Do we want to identify work-related factors (such as the existence of opportunities for invoking short-cuts to minimize effort) and organizational factors (such as the inability for designers to be more specific concerning procedural steps and thereby place the burden on the worker to adapt the procedure) that could predict such possibilities, or do we want to quantify these occurrences? Many other examples could be given that present the same dilemma, and that point to the need for a resolution that favors exposing the possibilities for undermining system performance.

The methodology presented below combines a number of very fundamental hazard evaluation (HE) methods within the context of creative brainstorming to predict possible human failures and the possible consequences of these failures. It also provides a template for deriving explanations for these failures in order to provide a logical basis for imposing barriers or safeguards. The HE methods, in particular failure modes and effects analysis (FMEA), and hazard and operability analysis (HAZOP), will be adapted to consider exclusively "human failures." The purpose of this approach is to enable managers and designers to identify *possibilities* for exposure of the system to risk. The "human failure" HAZOP and subsequent What-IF analysis are overlaid iteratively on the human FMEA to open up the analytic process to further brainstorming, for example, to consider how the consequences of one human failure might impact other actions or other aspects of the system. This type of analysis is especially important in systems that are interactively complex [11].

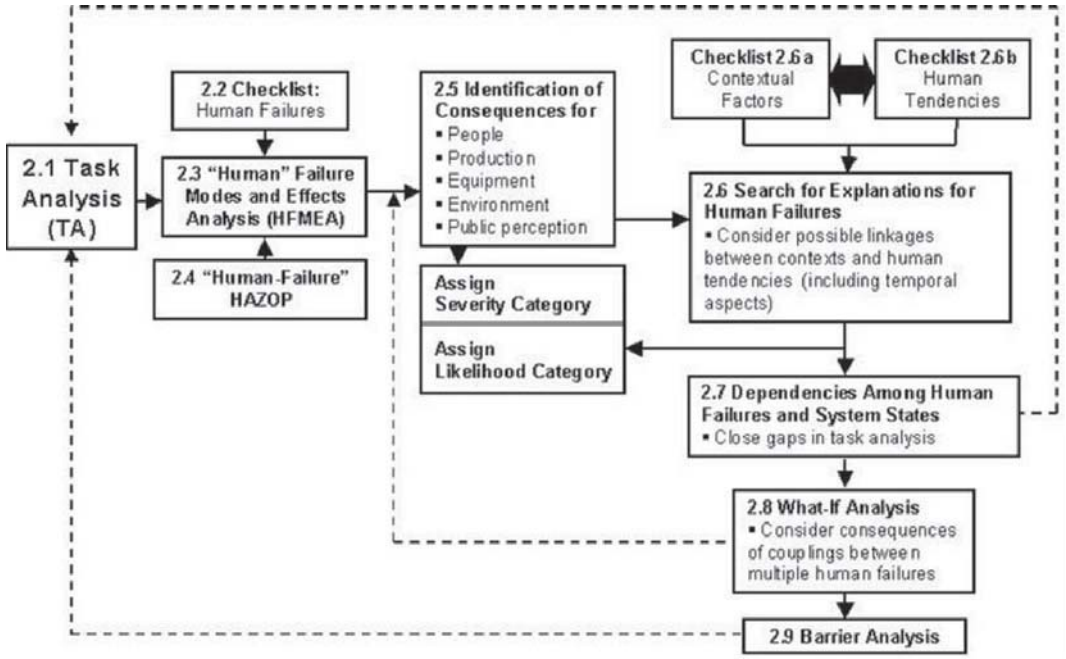


Figure 40.1. Overview of the methodology for exposing human failures and their consequences and causes (the block numbers correspond to the sections in the text where those topics are discussed)

40.2 Methodology

The overall approach to prediction of human failures and their consequences is illustrated in Figure 40.1. In this figure, the various methods or stages comprising the overall methodology are numbered and presented as a flow process with iterative loops. The discussion below corresponds to this numbering scheme.

40.2.1 Task Analysis

The starting point of this methodology, task analysis (TA), is fundamental to the entire endeavor. Many different TA methods exist [12, 13]. TA describes the human's involvement with a system in terms of the goals to be accomplished and all the human's activities, both physical and cognitive, that are necessary to meet these goals. If the operations underlying a goal cannot be usefully described or examined, then the goal can be reexamined in terms of its subordinate goals and their accompanying plans—a process referred to as "redescription" [14] that defines a task analysis methodology referred to as hierarchical task analysis (HTA). The level of detail in the TA will depend on whether it is being applied during the preliminary or later stages of design, or during the operational stages of the product or system.

When examining each of the various human-system interactions that generally encompass TA, the analyst will typically focus on a goal or sub-goal that is capable of being adequately characterized. Analysis of these interactions could be performed using a variety of perspectives and methods. The analyst may resort to simple models of human information processing to determine if the human is receiving sufficiently salient, clear, complete, and interpretable input; has adequate time to respond to the input with respect to being able to mentally code, classify, and resolve the information or in terms of the time the system

allows for executing an action; and whether feedback is available to enable the human to determine whether the action is or was executed correctly and is appropriate for dealing with the goal in question. More complex information processing schemes can also be used. For example, one could determine if working memory—the human's short-term memory store to which a good deal of our conscious effort or attention is dedicated, as when we plan, evaluate, conceptualize, and make decisions—may be overloaded [15], which can result in many different forms of erroneous activities depending on the particular context. The analyst may also question whether the human has available in long-term memory adequate facts, schemas, or mental models that he or she may need to translate inputs into appropriate actions.

If the task element concerns making a decision, various limitations associated with human decision making can be explored, such as tendencies to overweight or underweight critical sources of information, or resort to heuristics that lead to various biases in judgment.

In some situations, the analyst may find it useful to exploit similarities that may exist between operations from different domains by identifying characteristics of a current operation and relating these to other operations the analyst may have encountered or has insights into. Similar task elements (such as the need to recall previous steps in a procedure, working in restricted spaces, the need to scan monitors for information, the need to discriminate between various alarms) arise in different contexts. The analyst may also employ checklists that cover a broad range of ergonomic considerations to determine if the human is being subjected to factors (such as illumination, noise, posture) that can contribute to erroneous actions. These types of checklists can be expanded to include what are often referred to as performance shaping factors that consider task, workplace, interface, and organizational design factors.

Finally, analysts can resort to other types of methods of data collection if they feel there are still important performance issues that need to be resolved. For example, one can use concurrent verbal protocols (where people think aloud as they perform the task), retrospective verbal protocols (where people view their performance on a video or the results of their performance on a computer screen), or prospective verbal protocols (where people verbalize how they plan to perform a task or accomplish some goal or subgoal). Other approaches are also discussed in [14]. With HTA, if exploration of the human-task interaction proves to be too difficult or is not sufficiently revealing of potential points of weakness, the analyst should consider "redescribing" the goal in terms of a set of subordinate goals (*i.e.*, subgoals) and an organizing component called a "plan" that specifies the conditions under which these sub-goals have to be carried out to meet the system goal in question.

40.2.2 Checklist for Identifying Relevant Human Failure Modes

The primary "table" or organizing device driving this methodology is the one typically used with the failure modes and effects analysis (FMEA) hazard evaluation technique. This technique requires specifying the failure modes for each component as well as the consequences and causes of these failure modes. In this case, however, the failures under consideration are human; thus the mapping from the steps of the task analysis to the possible failure modes within the FMEA results in a human FMEA (HFMEA). This procedure typically will require some form of classification system that can provide a wide range of human behaviors that could occur in human-system interaction. The classification system should be sufficiently flexible so that the specific behaviors could be easily adapted to the particular work domain or task under consideration.

One such classification system considers four broad categories of behavior: perceptual processes (searching for and receiving information, and identifying objects, actions, and events); mediational processes (information processing and problem solving/decision making); communication processes; and motor processes. This classification system can be traced to the various stages that can occur in human information processing, specifically, perceptual encoding, central processing, and responding [15]. Table 40.1 represents an

example of such a classification system in the form of a checklist. The categories are not meant to be exhaustive; many more items could conceivably be proposed. Nor are they truly mutually exclusive given that perceptual, communication, and response execution activities are inextricably linked to thought (*i.e.*, mediational) activities.

Thus the distinctions in Table 40.1 are motivated primarily by a leaning towards one or another category based on how dominant that category appears to be for the task analysis step being analyzed.

The proposed methodology for predicting possible adverse consequences resulting, at least in part, from human failures thus begins by an exhaustive consideration of possible failure modes for a particular human activity within some operational context. In this respect, the approach is consistent with traditional FMEA, which also attempts to consider every possible failure mode, although it does so for mechanical components. Because a single analyst can, in principle, perform a TA and, using the checklist, derive possible failure modes for the task step, this approach is relatively efficient. There are, however, other approaches one can adopt. For example, starting with TA, one could use a detailed analysis of the contexts in which the human performs the task, along with knowledge concerning human tendencies and limitations, to predict how human failures may come about. This approach would be more resource intensive, requiring from the outset more group brainstorming. It also shifts the focus almost immediately to work contexts. By initially laying out all possible (*i.e.*, relevant) failure modes, as is done in a traditional FMEA, the process of seeking out the conditions that comprise the contexts in which human performance occurs becomes more simplified.

Note that in traditional FMEA the failure modes of a device or component are explicit, and it is not debatable as to whether these failure modes constitute an external mode of failure or an explanation for the failure. The adaptation of FMEA to human performance, as driven by TA, is not intended to maintain this same distinction. If the true purpose of the method is to establish possible consequences of human failures and ultimately to design barriers to mitigate or prevent these consequences, then a strict application of the concept of external manifestation of human error will necessarily lead to a reduced set of possible consequences. Thus the human failure "uses the wrong rule" clearly is an inferable "error" that, in the strict sense advocated in [3], does not meet the criteria of an externally manifest error. However, within the context surrounding a particular step in a task analysis, it may have severe consequences and thus may be a valid human "error" to consider. Otherwise we become restricted to a sparse set of external error modes of which "action omitted" and "wrong action performed" characterize almost all observable human failures. This lack of specificity would not adequately address the requisite variety of possible consequences, which is what the designer and manager are interested in, and would like to be able to consider without tracing these general error modes through complex sequences or networks of contexts within which the human performs. Although analysis of accidents that have already occurred may require more objectivity in terms of what actually happened, such restrictions should not impede the exploration of what "could happen," which is what this methodology intends to pursue.

While some degree of inference may be required when selecting a number of the items in this checklist, the inclusion criterion used for many of the items was that they should be capable of passing the "fly on the wall" test. In this test, a hidden observer very familiar with the task and the contexts under which it may be performed should be able to be reasonably assured that an item from this checklist applies if that observer can "see" both the human and the context within which the human is performing. In addition, the types of failures comprising these categories should, for the most part, be separable from the explanations that potentially underlie these failure modes.

Table 40.1. Checklist of human failures

Perceptual activities	Communication activities	Mediational activities	Response execution activities
▪ Misses signal/cue or insufficient signals considered ▪ Ignores signal ▪ Confuses signals ▪ Fails to detect changes (*e.g.*, trends) in situations ▪ Fails to detect changes in situations related to deterioration within the system ▪ Fails to verify or correlate unusual information ▪ Only partial information gathered ▪ Gathered information from unreliable sources	▪ Absence of communication ▪ Communication ambiguous (key details omitted) ▪ Communication using a medium that is not likely to be checked on time ▪ Communication is overloading (too much raw data given too quickly) ▪ Communication to wrong individual or team member ▪ Communication lacks necessary context (and thus details can be misleading) ▪ Communication is unintelligible (*e.g.*, due to language barriers or distortion in communication channel) ▪ Communication too aggressive in tone (and thus may not produce adequate questioning) ▪ Communication not understandable (*e.g.*, due to use of inappropriate terms or lack of knowledge by the receiver) ▪ Understanding of communication by receiver not verified	▪ Computation is incorrect (*e.g.*, computing a dosage requirement) ▪ Estimation/anticipation is incorrect (*e.g.*, how many orders will get delayed, how long it will take for temperature to stabilize) ▪ Misinterpretation of information being attended to (*e.g.*, thinks data is in cm and not mm) ▪ Judgment is incorrect (*e.g.*, safety implications of a lab result or display reading) ▪ Assigns too much importance to a source or item of information ▪ Fails to define task goals ▪ Fails to select a plan to meet task goals ▪ Ignores pre-conditions in selecting a plan ▪ Ignores feedback during problem solving or system operations ▪ Misinterprets feedback ▪ Uses the wrong rule ▪ Confuses one rule for another ▪ Fails to invoke a rule that should have been invoked ▪ Performs a routine violation of a procedure ▪ Performs an exceptional violation of a procedure ▪ Failed to consider side effects of actions ▪ Allowed oneself to become distracted during an interdependent sequence of actions ▪ Insufficient consideration of information during problem solving ▪ Incorrect sources of information used during problem solving or for making a decision	▪ Action is too early or too late (*e.g.*, in initiating an order) ▪ Action is insufficient or excessive (*e.g.*, force or movement) ▪ Actions are performed in the wrong sequence(*e.g.*, steps are reversed) ▪ Actions are omitted (*e.g.*, in an assembly operation) ▪ Actions are repeated (*e.g.*, administering a drug twice) ▪ An extraneous action is substituted ▪ A correct action is applied to the wrong object or process ▪ An incorrect action is applied to the right object ▪ A check on an action is omitted ▪ Action is performed too fast or too slow ▪ Actions are in the wrong direction (*e.g.*, when setting a thermostat) ▪ Actions are of the wrong movement type

Thus, although "uses the wrong rule" may be construed as an *explanation* or *cause* for a "wrong action performed," it is also conceivable that an error such as "uses the wrong rule" can be represented within a TA and thus be considered in terms of its consequences, as would be the case for any failure mode—whether human or mechanical component. Furthermore, as causes of failure modes will generally be attributed to an interplay between human tendencies and the contexts in which these tendencies or limitations are embedded, "uses the wrong rule" should, in turn, require an explanation that, as we shall see, will be based on linkages between human tendencies (that essentially define human fallibility) and the contexts within which the human performs. Finally, as will be discussed further on, these failure modes represent a first pass. There will an opportunity to refine or generate new failure modes that are based on a more detailed understanding of the operational context by employing yet another variation of a well known hazard evaluation technique—in this case, a human failure hazard and operability analysis (HAZOP).

40.2.3 Human Failure Modes and Effects Analysis (HFMEA)

As indicated above, the hazard evaluation technique referred to as failure modes and effects analysis (FMEA) is more accurately referred to as a human FMEA (HFMEA) when its focus is on the ways or "modes" in which the human can "fail." An advantage of the FMEA technique is that it lends itself to thoroughness, and is thus often acknowledged for its ability to optimize designs and incorporate protective features into the system design. However, it has disadvantages as well. One problem with it is that there is no method for assessing the degree of thoroughness of the analysis. In adapting FMEA for human failures [1], this drawback is minimized by preceding this analysis with a TA, which provides the template for identifying failure modes—that is, the requirements specified in the TA dictate the possible failure modes that are considered by the HFMEA. What this in effect does is shift the burden to ensuring a thorough TA.

A disadvantage of FMEA that remains as well in the HFMEA relates to the emphasis in the conventional FMEA on single-point failures (*e.g.*, a valve failing open), which increases the likelihood of failing to account for adverse system outcomes deriving from multiple co-existing hazards or failures. As we shall see, FMEA adapted for human failure modes ultimately will need to be combined with other hazard analysis techniques that can serve to incite creative brainstorming about higher-order threats to the system. This exercise should logically follow the HFMEA, and will need to be tailored to the specific system in question.

40.2.4 Human-failure HAZOP

To further refine the failure modes, the analytical team can also consider applying the HAZOP analysis method [16]. This well known hazard evaluation technique uses a very systematic and thorough approach to analyze points of a process or operation, referred to as "study nodes" or "process sections" [17]. In its most fundamental form, this analysis is conducted by applying, at each point of the process being analyzed, "guide words" (such as "no," "more," "high," "reverse," "as well as," and "other than") to parameters (such as "flow," "pressure," "temperature," and "operation") in order to generate deviations (such as "no flow" or "high temperature") that represent departures from the design intention. Analogous to FMEA, HAZOP analysis also includes determining reasons for the deviations, consequences of the deviations, and recommendations in the form of design changes, procedural changes, or areas for further study. The guide words are the key to stimulating the brainstorming process that underlies hazard identification. In fact, HAZOP is distinct from many other hazard analysis techniques in that it depends highly on nature of the team assembled and the team's brainstorming dynamics in terms of the stimulation of creative analyses and the generation of new ideas.

Although HAZOP was initially intended for process industries, as with FMEA there is no reason it cannot be adapted to human failures. However, in the proposed methodology, the

emphasis is on the creative aspect of HAZOP—the application of guide words to parameters. Thus HFMEA remains the core template for organizing the human failure analysis, while other methods feed into it (like TA) or embellish it (like HAZOP). The key is to derive "guide words" and "parameters" that are applicable to the TA. As in traditional HAZOP, where teams often supplement lists of deviations with ad hoc items, the analysts can consider any descriptor relevant to the task or context that can qualify or quantify the human failure. As noted in [1], this "*human-error HAZOP*…can range from a simple biasing of the HAZOP procedure towards the identification of human errors to an actual alteration of the format of the HAZOP procedure itself" (p. 95). For example, this human HAZOP used knowledge of drilling operations and a number of taxonomies of human error to create an additional set of HAZOP guidewords as an aid for identifying human errors in an offshore drilling exercise [18].

40.2.5 Identifying Consequences and Assessing Their Criticality and Likelihood

Conventional FMEAs usually incorporate a cause for each failure mode identified as well as the consequences of these failures. These consequences are sometimes referred to as failure events as it may be necessary in some instances to surmise the consequences from the events (for instance, the implications of a failure event described in terms of a clutch pedal that does not move or a lack of response to the activation of a switch).

It is also possible for each failure event to have adverse consequences for one or more "system targets" such as personnel, production (including quality), equipment, the environment, and the public (including public perception). Depending on the risk assessment approach adopted, a criticality value could also be assigned to each failure-target combination. Qualitative risk assessment perspectives would assign a subjectively designated level of severity and likelihood to the consequences of the failures. Four levels of severity that are often used are negligible, marginal, critical, and catastrophic. Levels of likelihood could include impossible, improbable, remote, occasional, probable, and frequent. Taken together, these levels would determine whether actions are recommended for mitigating the risk [17]. Quantitative approaches would attempt to compute a component criticality number, defined as the number of system failures in a particular class of severity per hour or trial caused by the component across all its failure modes [2].

Unlike the generation of possible failure modes for a given TA step, the complex events that may intercede between human failures and adverse consequences argue for making consequence analysis a dynamic team enterprise. As with traditional FMEA, the analysis of consequences should not be biased by knowledge derived from the analysis of causes of the human failures, implying that the initial emphasis should be on *identification* of consequences and their severity. For example, a causal explanation for the consequences of a human failure that requires many concurrent conditions to be in place and several human limitations acting in concert, while possible, may appear very remote and thus predispose analysts to exclude the consequences from consideration. This works against maintaining independence between likelihood and severity assessments of consequences, which is fundamental to risk assessment [2]. Thus, in addition to the identification of consequences, it should also be possible to assign a level of severity to the failure effect. However, the consideration of the likelihood of the consequences is a different matter; likelihoods of a consequence depend, in part, on the likelihood of the human failures that instigated the consequences. Gauging an appropriate likelihood category for consequences thus requires a consideration of the possible causes or explanations for the human failures, as indicated in Figure 40.1.

One approach to likelihood assessment is to assign "confidence weights" to the different sets of causes or explanations that are being considered for the human failure (as discussed below, a set of causes comprises some combination of contextual factors and their interaction with human tendencies and limitations). The ability to generate several high weights would then imply a possibly high likelihood category for the consequences being considered.

40.2.6 Explanations of Human Failures

Causal analysis from a systems perspective requires an understanding of the context in which the human performs and how human tendencies and limitations can interact with these contexts. Although this analysis can suggest how likely the possibility is for certain human errors, its real benefit lies in its ability to bring about a deeper qualitative understanding of the interactive human-system process. This knowledge is essential for suggesting safeguards or barriers, or other courses of action (*e.g.*, replacing or eliminating parts or entire systems) for the purpose of reducing risks associated with human errors. The generation and use of this knowledge also provides an organization with the ability to learn (*e.g.*, in regards to weaknesses in the system or how common work-related conditions and events can combine to produce adverse consequences).

To aid analysts in identifying important interactions between relevant performance conditions and human tendencies and limitations, two checklists can be used (steps 2.6a and 2.6b in). Table 40.2 presents a number of categories of contextual factors that can impact upon human performance, and Table 40.3 lists a number of human tendencies. Many of the human tendencies reflect human cognitive or physiological limitations and thus represent aspects of human fallibility. The information contained in these checklists derives from a wide variety of sources that include [3, 7, 15], as well as other sources and personal research studies. These checklists can easily be extended or modified to be more applicable to a particular work domain or a specific set of operations of interest to an organization. To the extent that they do not represent a compilation of simple sparse statements, as are typically found in applications of HRA, but provide some logic and inherent guidance as to their potential applicability, then these checklists become aids. In this regard, both tables were constructed with the intent of demonstrating their pedagogical nature, although the extent to which this is done is more illustrative rather than exhaustive.

Using an aid such as Table 40.2, the task is to *assemble* various scenarios than can possibly characterize performance conditions, by identifying relevant contextual factors or categories and then their corresponding attributes (*i.e.*, items). These contextual factors can be depicted in a small graphical network to highlight the ways in which these factors can interact and thus induce a demanding performance environment [9]. These depictions are not intended to constrain the effects of the contextual factors by examining how one factor sequentially impacts upon another, but rather attempt to capture the totality of the context. Temporal attributes in the interactions between these factors can also be considered. For example, feedback that is delayed or in a form that is difficult to access may be missed, and this may impact upon how information becomes documented for use by other people

Following the construction of relevant networks of contexts, the analytical team would need to determine which human tendencies or limitations are relevant to the contexts under examination, and how these tendencies could result in "errors." Note that many of the human tendencies that are listed are not mutually exclusive—some imply the existence of others. Also, many of these tendencies can be thought of as subsumed under a superordinate tendency such as load shedding or minimizing cognitive load [19], which ultimately may be manifest in behaviors that are referred to in [20] as the efficiency-thoroughness tradeoff. As suggested earlier, when possible linkages between human fallibility and contexts are discovered, confidence ratings can be used to assess how likely the analyst feels that the interplay identified represents a credible explanation for the possible human failure.

There will be times when the linkages between context and human tendencies are relatively straightforward. In fact, such linkages are probably good starting points in the analysis. For example, a working environment characterized by spontaneous interruptions and that requires activities involving face-to-face communication can form a context that on its own can be conducive to omissions in communication. By building on this context, for example, by recognizing that cues needed to trigger recall of the required communication are generally absent, the confidence in the generation of this

human error through the interplay of context and human tendencies is increased.

This analytical process discourages the view of the expert [6] or lone analyst in favor of brainstorming. Thus, as with the application of more conventional hazard evaluation techniques, careful attention needs to be given to the makeup of the analytical team [17]. Brainstorming also can expand the scope of the analysis. For example, it can enable better conceptualization of how actions at earlier steps or how different system states can interact with an error, and how different system states that emerge can result in new problems for the human performing the task. It can also encourage suggestions for barriers and discussion concerning the possible implications on the system of these barriers.

40.2.7 Addressing Dependencies

A fundamental disadvantage of the FMEA technique is that it does not address adverse consequences induced by co-existing multiple-element failures within the system. In the case of a HFMEA, the effects of prior human failures on impending human actions or behaviors may be important. In fact, human failures may transform the system in ways that may require rethinking the TA in terms of alternative actions the human may take, both imminently and more distally. For example, consider a person performing maintenance operations involving a series of steps under time constraints, and in a restricted space with poor lighting that makes it difficult to access or consistently refer to written work procedures. An error in this operation (which could take on a number of different forms depending on the nature of the task and other individual factors) could result, at a later time, in an unexpected system state that further disposes the human to error.

This raises a related issue, which concerns whether TA as a technique can capture the fluctuations that may occur in human response to system demands, including those demands that are now imposed due to previous human performance shortcomings. In general, a good TA should account for alternative human actions in the form of contingencies if goals and plans are not accomplished. When a HTA is displayed in a tabular format, it is not uncommon to devote a separate column to considerations such as whether problems associated with a particular step in the TA can impact other steps, or whether the person has opportunities to detect or recover an error that was performed. However, even if the TA is limited in this respect, the consideration of prior human failures on impending human actions at this stage of the overall analysis provides the opportunity to close such gaps in the TA, as illustrated by the feedback loop from step 2.7 to step 2.1 (Figure 40.1). In this sense, the prediction of human failures and their consequences is, like any design procedure, an iterative process that seeks to revisit assumptions and revise the analysis.

40.2.8 What-If Analysis

In addition to consideration of whether human failures can impact upon other (impending) human behaviors, the effects on the system of multiple human failures that may or may not be coupled need to be addressed. This clearly necessitates a brainstorming process, and use of techniques such as What-If analysis [17] is appropriate. In traditional hazard analysis, this technique can, in principle, be used to examine virtually any aspect of a system's design or operation.

40.2.9 Design Interventions and Barriers

Once explanations for the possible human failures have been proposed, barriers that can prevent or mitigate the adverse consequences can be considered. A useful classification system for barriers [20] considers four categories: physical barrier systems (that physically prevent an action from taking place); functional barrier systems (that impede the actions from taking place); symbolic barrier systems (that require interpretation); and incorporeal barrier systems (that depend on the knowledge of the user).

With regard to each of these barrier systems, the barrier can perform its function in various ways. For example, some of the functions of physical barrier systems include containing or preventing (walls, restricted access, containers), restraining or preventing movement (harnesses, cages), maintaining

resilience (rigid consoles, shatterproof glass), and separating and protecting (scrubbers and filters). Functions of functional barrier systems include preventing movement or action (interlocks, passwords, pre-conditions), hindering actions (controls out of reach), attenuating (noise reduction), and dissipating energy (air bags, sprinklers). As noted, symbolic barrier systems require interpretation and include functions such as countering or preventing actions (labels and warnings), regulatory actions (instructions, procedures), indicating system status (traffic signs, warnings, alarms), and communication (air-traffic controller giving clearance, approval by a supervisor to begin work). Finally, incorporeal barrier systems depend upon functions such as complying (social or group pressure, ethical norms) and prescribing (rules, laws).

In addition, systems that are designed to provide feedback that can promote self-detection of errors, and the use of redundant independent checks (*e.g.*, by co-workers or supervisors) can also serve as barriers. The important factor in the consideration of barriers is that these systems can also impact upon the context within which the human performs [9]. Thus the consequences on the system of these barriers also needs to be evaluated (Figure 40.1), consistent with the iterative nature of any design process.

40.3 Summary

This chapter has presented a methodology proposed for the purpose of exposing possible human errors and violations and for analyzing the potential consequences and possible causes of these behaviors. The argument was made that such a qualitative approach to proactively accounting for human failures in human-system interaction can be conducive to organizational learning. The approach is highly dependent on producing a thorough task analysis as its starting point, but then hinges on the application of a combination of hazard evaluation techniques that have been adapted for analysis of human failures. The possible need for iterative analysis and the importance of using a dynamic group process for brainstorming was emphasized.

Table 40.2. Factors governing the contexts under which the human performs

Time available to perform any of the task Activities
• Is there enough time to: perceive the inputs or information; understand what is being perceived; integrate what is being perceived; or interpret what is being perceived? • Is there enough time to respond (*e.g.*, manually) to what is being perceived or cued? • Is there enough time to put together an adequate plan? • Does time allow for effective strategies in time-sharing, for example, in performing some task and intermittently communicating with other people?
Adequacy of Human–Machine Interface or Task Design
• Is the location of displays or other important items consistent with the geographical layout of the environment that needs to be monitored or controlled? • Are displays or controls that serve similar functions grouped together? • Are displays or controls that are frequently used or serve important functions placed in prominent positions? • Are displays and controls appropriately positioned so that there is minimal confusion concerning which controls are associated with which displays? Are displays and controls properly and conspicuously labeled so that there is minimal confusion concerning what one is looking at or listening to or what control is being activated? Are displays and especially controls too crowded so that there is the possibility for confusing displays or controls?

Table 40.2. (continued)

- Is there a hierarchical organization of information available to the human concerning the overall system, from its individual components to representations that capture the general functions and objectives of that system, so that a range of different types of activities, from normal control to diagnosis and decision making can be supported?
- Do actions such as button presses provide adequate feedback (that is salient and that provide redundant cues)?
- Does the human have to invest reasonable effort to acquire information from the device or system, for example, by having to be very precise in physical input actions, by having to negotiate many menu systems on a single display in order to find the needed information, or by excessive scrolling or following activated links?
- Are the displays that the human must monitor or controls that the human must activate organized so that the human must expend reasonable effort to move between displays or controls? If so, the tendency to minimize effort may result in minimizing walking around, possibly leading to omissions or reading errors.
- Is the content of the information complete and unambiguous so that the human can reliably identify and classify needed information, and is the information being provided relevant to the task?
- Are task-related events or information input occurring at a frequency that is possibly beyond the ability for a human to adequately process?
- If the human needs to see historical trends in data or information, can the system interface provide this information, and do so in a form that the human can easily process?
- Can information easily be transitioned between its raw forms (for example, the values of individual variables) and the integration and suitable presentation of this information according to various rules that the human may need to apply?
- If the human needs to assess what-if scenarios can the interface provide such assessments, for example, through predictive displays?
- If the human is interacting with a hand-held device, is it easy to locate the device, get to the desired function, and negotiate its display of information?
- If alarms are present, do they provide sufficient feedback concerning the nature of the problem and possibly even some indication of appropriate actions to take?
- Have alarms been designed to strike a balance between "nondetection" and "overstimulation" (which can result in shutting off alarms)? Can alarms disrupt the processing of other alarms or important speech communication?
- How extensive is the use of synthesized speech? Because listening to synthetic speech may demand more mental resources than listening to natural speech, it may interfere with other ongoing tasks.
- When people need to handle objects, controls, or tools, has redundancy been considered (*e.g.*, by providing "haptic" information regarding the shape of manipulated objects)? This may be critical where protective clothing such as gloves may diminish the ability to correctly identify the object.
- Are controls "isometric" in the sense that they do not move when pressure is applied to them? This lack of feedback could undermine human control activities.
- Are lockouts appropriately designed and labeled so that their operation and status is clear?

Table 40.2. (continued)

• When the person's hands/eyes are busy when multitasking, are voice commands available to perform the additional task or tasks?
Automation and New Technology
• Is the human required to passively monitor displays or automated systems for considerable amounts of time? • If something were to go wrong with the automated system or subsystem, are the deviations presented quickly enough to the human and in a way that would allow the human to be reasonably successful at diagnosing the problem? • Is the reliability of the system sufficiently high to ensure that the human has adequate trust in its performance? If not, is there an understanding of the types of strategies the human may resort to in the face of such unreliable performance? • Is the human given sufficient hands-on experience with the system in order to ensure that control of the automated system can be maintained in the event of automation failures? • As a result of limits in automation, are there tasks the human needs to perform that are fragmented in the sense that they are simply pieces of larger tasks that disrupts or distracts from the larger continuity of the task? • Does the human have an adequate model of the automation so that if distracted the human can quickly assess what the automated system is doing? • Is the system designed in such a way that the human can easily identify the mode in which the automated system is operating in? • Is the system designed in such a way so that the implications of human actions to the automated system are made apparent to the human? • If new technology is introduced, can there be problems confusing previous information or activities with ones that are now required?

Work Procedures
• Are written procedures or procedures in some other form available to guide performance of the task, or is the human expected to know how to perform task activities without resorting to any procedures? • Are procedures integrated with training, so that during training people had the opportunity to reference and test the procedures, or are training and work procedures unlinked? • Were the procedures directed or guided by a task analysis? • Have the procedures been performed by their designers to determine the feasibility or adequacy of the procedures? • Are the procedures written in a clear, unambiguous language, with relatively short sentences (so that the meaning of a sentence is not apparent until a later portion of the sentence is read), and minimal use of negation? • Are the procedures organized and formatted well, so that the persons following them can easily anticipate where other information is and have a good model of the relationships among different sections of the procedure? • Do procedures have good implicit placeholders so that workers can easily find their place following an interruption? • Are the instructions in the procedure congruent in the sense that the order of the words or commands corresponds to the order in which they are to be carried out? • If the procedure is similar to one or more other procedures the worker may perform, for instance, in terms of common sequences of operations or the need to identify similar conditions but which require different responses, are there mechanisms present to ensure that the worker continues to use the correct procedure?

Table 40.2. (continued)

• Are sufficient information, examples, and context provided to allow people to develop sound mental models from the procedures, so that the procedures generate a set of expectancies about how the device or system will behave? • Are the procedures consistent with the expertise of the workers? • Do the procedures expose the people who must perform them to undo risk or hazards? • Are the procedures cumbersome, so that they require a good deal of mental or physical effort, or do they appear unduly time consuming? If so, are short-cuts or easier ways of doing the procedure identifiable by workers? • Do workers have a convenient work area for consulting the procedural documentation? • Are people expected to improvise procedures when there are procedural aspects that lack specificity? If so, are they given any guidelines about how to go about doing this (for example, strategies to use in certain situations or boundary conditions governing when they should or should not attempt certain activities)? • If people improvise on procedures, is this information documented in some way so that the organization can better understand the implications of such improvisation? • Do procedures identify contingencies, backout criteria, indications that an error or abnormal system response has occurred, and potential recovery points to eliminate or reduce the adverse consequences of errors? • Do the conditions under which the task needs to be performed prevent easy reference or access to the procedures?
• Have procedures been revised to take into account changes that have been made to the operations, such as the use of different equipment, communication protocol, and objectives? • Are the people who are to perform the procedures involved in their design? If not, procedural violations are more likely due to incompatibilities between workers and designers or managers in perception of the adequacy of the procedure. • Have procedures taken into account lessons learned by the organization? If not, they may lose their credibility and thus become susceptible to violation. • Do procedures indicate ways in which the person performing the procedure can recover from potential errors or circumstances that can result in losses?
Training
• People will tend to perform tasks that are procedural (*i.e.*, based on the kinds of knowledge that allows us to do tasks, but that is difficult to verbalize) more effectively if training is conducted using actual task performance rather than the presentation of facts, *etc.* • It may be more effective to offer instructions that use pictures and voice since these can be processed in parallel and tend to place less load on the person during training. • In cases where work procedures will be used, does training adequately address the concerns and challenges implied in the procedure? • If certain aspects of a procedure may not apply in particular situations, have rules or boundary conditions been explicitly communicated so that workers can clearly map a procedure's directives to the given situation?

Table 40.2. (continued)

- For situations in which it is essential that a vast array of perceptual cues be accurately identified and integrated with a variety of control responses, has simulation been used as a vehicle for training?
- Is training dominated by the presentation of vast amounts of declarative (facts, rules) information prior to gaining experience with the work activities? If so, much of this information may become "inert" and become useless. Consider more active involvement with task activities, where knowledge is gradually accumulated as experience is gained.
- Are workers trained in developing accurate and useful mental models of aspects of the process or operations in addition to more fundamental information on task operations? If not, the person may be less likely to deal with abnormal or novel situations and more likely to perform actions with adverse consequences.
- Has appropriate performance support (*e.g.*, job aids, troubleshooting support) been considered?
- Does training impart sufficient knowledge for the person to adequately perform the task?
- Is there adequate and sufficiently frequent training for emergency procedures or operations?
- When new technology or automation is introduced, does training address the relevant concerns? For example, if new technology results in different team communication patterns, are these changes anticipated and adequately addressed in training? If automation requires understanding the underlying dynamics of the technology and incorporation of new control strategies, are these issues anticipated and adequately addressed in training?
- Has training considered informing people about the miss/false alarm tradeoff?
- Has training considered the possibility that people may not use a device or system for an extended period of time and may require becoming reacquainted?
- Has training considered how people can detect their mistakes and the mistakes of others?

Task Feedback

- Does the human receive feedback concerning his of her actions?
- How quickly is feedback given? Delayed feedback could be problematic.
- What is the form of the feedback? Is it in a form where it could be easily missed if distracted or not paying attention? Is it in a form that is legible and understandable? Is it in a form that makes it difficult to access?
- Does the human have control over the feedback; that is, can the human request feedback, and manage the form in which that feedback is received?
- Does the control device or system only provide artificial visual feedback (*e.g.*, a red light turning on) to indicate a state change? Such feedback can easily be missed or misinterpreted.

Information Sources and Documentation (Related to Procedures)

- Are there multiple sources from which the person can obtain information from? Does the human have to make a choice concerning which source to consult?
- Is the information in the source legible, unambiguous, accurate, and complete?
- Is it relatively easy to obtain information from the source or does it require reasonable effort?
- Is it relatively easy to embellish or edit the information in the source, for example, adding comments or information, or changing values?

Table 40.2. (continued)

• Does the human have the ability to manage the information in the source by having the information organized and displayed in different formats (for example, requesting that trend information be displayed)? If so, how easily can this be done?
Multiple Objectives
• Are there multiple objectives to satisfy? How many? • Is it clear what these objectives are? • Are these objectives relatively stable or are they changing over time? • Do the objectives have different priorities? Do these priorities shift over time?
Ergonomic Considerations
• Are there high levels of noise? Is there noise in frequency ranges that can mask important communications or alarms? • If communication between people is essential and the individuals are not always in physical proximity, is there a protocol to ensure that all possibly needed communication channels are available in working order? • Do people need to perform activities in restricted spaces? If so, can these workers attend to all relevant stimuli? Can they assume their postures for the time needed to perform the activities without becoming fatigued? Can they maneuver and control tools, protective clothing, and equipment adequately? Can they communicate effectively with other people when necessary? • Are certain jobs difficult to carry out when wearing personal protective equipment such as earplugs, helmets, goggles, gloves, breathing apparatus, full body suits, safety belts, and safety footwear? If so, the risk of injury is increased.
• Are lighting conditions adequate for the work operations? Is their sufficient illumination, appropriate visual contrasts in the person's field of view, a lack of glare or flicker, and an absence of large external viewing areas (*e.g.*, windows) that can be distractive? • Can all visual stimuli, such as labels and icons, be sufficiently discriminated from one another? • Are there conditions of heat, humidity, or cold? If so, workers are likely to become fatigued or accelerate or bypass activities. • Are tools designed appropriately for the tasks they are used to perform? If not, can they induce too much or too little force, excessive variability in movement, or insufficient control? • Are there concerns for poor air quality due to pollutants or other factors? If so, the person's mental functioning may become compromised. • Do controls require excessive force or static forces? If so, these actions may be subject to suboptimal control.
Workload
• Is most of the activity concentrated in relatively small blocks of time? If so, there are concerns that the person is sufficiently alert and ready to confront the demands. • Is the workload excessive, in terms of the rate at which events occur and need to be handled, or in terms of the degree of multitasking required? If so, load shedding through simplification or other approaches may lead to neglecting procedures. • Is the person required to work long shifts so that fatigue is an issue? In the event of shift changes, this may erode the effectiveness of communication to the incoming shift. • Are there sufficient rest pauses for highly mental or physical work activities?

Table 40.2. (continued)

• Are there long or uneventful vigilant periods? If so, the human may be vulnerable to missed information or incorrect processing of events. • Are there demands to perform calculations? These activities often take time and if unsupported (*e.g.*, by computer aids) are error prone and can take time away from other activities.
Organizational and Psychosocial Factors
• If there are highly interrelated tasks that require considerable communication and cooperation among a number of people, is some systematic method of team training on these tasks incorporated by the organization? • For tasks or operations involving teamwork, has the distribution of workload among team members been given adequate consideration? Overloading can result in the inability to address certain ongoing activities for which one is responsible, and underloading can result in a lack of alertness. • Does role ambiguity exist, whereby a person is uncertain about his or her role at work? Has the organization made the work objectives, what coworkers and supervisors are to expect, and the scope of the responsibility clear to the worker? • Is it likely that a worker may skip an activity by assuming that it will be done by someone else at some later time? This usually occurs under time pressure and when clear roles and responsibilities are not defined. • Does role conflict exist? That is, is the person simultaneously subjected to two or more sets of pressures such that complying with one set undermines compliance with another? • If a person is uncertain about how to perform an operation, would it be clear that assistance should be solicited and where such assistance should come from? If not, the person is likely to ignore that operation. • Have clear protocols for communication been established for different task situations? For example, do workers know when and what information needs to be specified to prevent ambiguity and thus the possibility for false assumptions? • Have clear protocols for communication been established so that people know which channels of communication are appropriate for the different situations? For example, during shift changes, face-to-face communication may be needed whereas phone contact may be appropriate for other situations. • Have clear protocols for communication been established to mitigate the potentially detrimental effects of a lack of questioning by passive types who are receiving the communication and intimidation by aggressive types providing information? • Does the organization subcontract workers? If so, is the organization assured that these workers understand the communication protocols and other work-related policies that are in place among the full-time workers, and that would need to be known if these subcontracted workers were to communicate with full-time employees, especially across shifts? • Is there a clear leadership within teams or groups of workers? • Do individual work group cultures exist within the organization? Do these cultures impose pressure on individuals within the group to follow certain practices?

Table 40.2. (continued)

- Has the organization addressed staffing issues so that workers understand that understaffing is not the organization's policy?
- Does the organization embody a culture that emphasizes repeated and independent checks?
- Does the organization provide adequate time and resources for personnel involved in design activities? For example, are designers working under undo time pressure? Are they deprived of the opportunity for adequate testing of their design concepts and iterating their designs?
- Does the organization have a "blame culture" whereby management exonerates itself when incidents or accidents occur and shifts the blame to those who violated procedures or who otherwise were responsible for the final actions that gave rise to the adverse event? Such cultures create distrust between workers and supervisors, a lack of learning and improvement within the organization, and violations of procedures.
- Does the organization possess a good safety culture? Such organizations provide the opportunity for organizational learning from incidents, accidents, and operations in general. They typically have open feedback channels between their workers and management that enables ongoing revisions to procedures, strategies, and designs to be incorporated and evaluated. Such organizations have more "open" climates that view their employees as stakeholders; the employees, in turn, are usually more willing to offer important information on operations and incidents.
- Is there a tendency for the organization to only report deviations from normal operations? If so, workers are likely to interpret the absence of reporting as indications that their performance is appropriate when in fact it may not be.

Perceptual/Memory Tendencies

- People can only attend (*i.e.*, focus on) a limited number of cues (due to memory limitations).
- When information is received over time, the earlier aspects of this information tend be given the greatest weight. Information that occurs later or that changes over time has a greater likelihood of being ignored.
- People are more apt to attend to perceptually salient information, and this information is likely to be given more weight.
- People tend to simplify the processing of information by treating many of the features or aspects of the "message" as if they were about equal in significance and thus tend to overweight unreliable cues.
- People tend to look for information that confirms the selected diagnosis, decision, or idea, and avoid seeking information that could support an alternative theory.
- People tend to "sample" the world where they expect to find information, and attend to channels based on how valuable it is to look or costly to miss.
- People are limited in how many absolute judgments they can make, for instance, in being able to absolutely identify a particular alarm or pressure level. Thus if there are too many alarms that each need to be identified, confusion becomes an issue.

Table 40.3. (continued)

- Accuracy and speed of recognition of features or aspects of information will be greatest when the displayed features are compatible with how those features are represented in long-term memory (LTM).(LTM contains our storehouse of potentially retrievable information; it provides the basis for storing information and retrieving it at a later time.)
- People tend to rely on good articulation of the edges of objects for their recognition.
- As stimulus quality degrades, people tend to rely on increased contextual information as well as redundancy to successfully negotiate the information.
- People tend to perceive negation in sentences poorly because our perceptual system treats the positive meaning of a sentence as the default state of the message.
- The need to select information from a larger array of information sources will tend to be inhibited or reduced in its emphasis if this activity is effortful.

Tendencies Due to Memory Limitations or Resorting to Heuristics

- Working memory (or short-term memory) is a kind of "workbench" of consciousness in which we visualize, plan, compare, evaluate, transform cognitive representations, develop an understanding of information, make decisions, and solve problems. People can only keep a limited number of items in their working memory (short-term memory) and, unless this information is rehearsed, can only do so for a limited time—otherwise this information decays rapidly.
- People tend to have greater difficulty accurately recalling items in WM if the items sound or look similar to other items being entertained.
- People tend to have difficulty comprehending text that requires retention of words whose meaning is not apparent until a later portion of the sentence is read.
- People tend to process instructions better if the order of the words or commands in the instructions corresponds to the order in which they are to be carried out.
- People tend to be better at recalling or reactivating information of a particular type that has been frequently activated in the past (which allows that information to have a stronger trace in LTM).
- People tend to be better at recalling or reactivating information of a particular type that has been recently activated.
- When people receive new information about events or situations, they do not make appropriate adjustments in the likelihoods of those events; typically, their "new" likelihood assessments are too low or too high.
- Different pieces of information that are activated together in WM tend to become associated in our memory and these associations can form the basis for later reactivation from LTM. When processing information that is or can be represented in the form of If-Then rules, as may occur in troubleshooting, the activation (for instance, by virtue of what one perceives or mentally considers) of parts of the If portion of the rule or other representation will tend to increase the likelihood of other associated information becoming activated as well.

Table 40.3. (continued)

- People tend to fail to retrieve information that is stored in their LTM because that information is weak in strength due to there having been a low frequency or lack of recency in its activation, weak or few associations with other information contained in LTM, or interfering associations as might occur when too many associations needed to be acquired in a short period of time.
- The knowledge that people have about many things, topics, or concepts tends to be organized (*i.e.*, associated) in LTM. People often rely on mental models, which is organized knowledge concerning concepts, equipment, or systems that allow people to generate a set of "expectancies" about how the system or equipment will behave.
- Unless people are very well trained and have rehearsed needed information thoroughly, information that is "out of sight" will often be "out of mind" (*i.e.*, not considered), especially in the face of distractions or interruptions, or when there are many activities taking place.
- People tend to have knowledge about their own knowledge and abilities, including the anticipated effort required to gain additional information, and this will factor into their strategies.
- People are often overconfident in the accuracy of their own knowledge (knowledge in the head), and thus may disregard the need to expend effort to gather information (knowledge in the world)
- Powerful interface features or computer aids that require high degrees of cognitive effort to learn may be disregarded unless the costs incurred by their disuse are made sufficiently high. When time-sharing (*i.e.*, performing multiple activities almost concurrently), people will have greater success if one or more of the tasks has become almost automatic to the point of requiring almost no cognitive effort (*i.e.*, attention). For a task to become automatic there must be consistent mapping between its elements—for example between what the person sees and what the response to that stimulus should be.
- People tend to be better at time-sharing when the inputs from the tasks are spread across different modalities (for example, vision and hearing) as opposed to forcing the human to use the visual channel or the auditory channel for processing both tasks.
- There is a better chance of successful time sharing if people know the details regarding the relative importance of the tasks.
- Guesses that people make about what events or situations are occurring or have occurred are usually based on expectations, which, in turn, are based on past experiences that are stored in one's LTM. Expectations for these events or situations will be high if they have been frequently encountered in the past, or if they have associations with other events, cues, or scenarios that have been experienced within the same context.
- People are only able to entertain a limited number of hypotheses or alternative explanations at a time.
- People will retrieve hypotheses most easily that have been considered recently or frequently.

Table 40.3. (continued)

- People tend to judge an event as likely (*e.g.*, that a person should be classified as "suspicious" or that there is a malfunction in a connection between two subsystems) if the event
- "represents" the typical features of the category in question. Thus if a set of symptoms resembles the features for a particular hypothesis, this set will generate that hypothesis as a likely candidate.
- People tend to be overconfident concerning the hypotheses they have decided to consider and are thus less likely to seek out evidence for alternative hypotheses.
- Although people may have in their LTM a number of possible action plans associated with some hypothesis (for example different alternative actions if in fact the problem is insufficient power or is a particular disease or condition), people are limited in the number of such alternatives that they can consider at any one time.
- People tend to consider the most available alternative from their memory (*e.g.*, based on how recently or how frequently those alternatives have been used).
- The likelihoods that people assign to the outcomes of possible alternative or action plans will be distorted to the extent that instances of outcomes are available in one's LTM.
- In situations involving making decisions or judgments, people are susceptible to how the situation is framed; thus, depending on how a situation is cast, an investment in a safety system may seem appropriate or inappropriate.
- Tasks characterized by a relatively large and variable amount of information that is presented simultaneously but briefly, where there are many relationships among the different inputs of information, and where there is a relatively short time period for making decisions, tend to induce an intuitive decision-making process. Hallmarks of this process include low levels of cognitive effort, low conscious awareness, rapid processing, and high confidence in one's answer.

Slips and Lapses

- Are there tasks that are similar in sequence or have operations that are similar? For example, two assembly tasks may have similar sequences so that the operations governing one assembly task is embedded in a sequence of operations normally associated with the other assembly task. A distraction on the less frequently performed assembly task may result in the person resuming the task by performing the operations associated with (*i.e.*, "slipping into") the more frequently performed task.
- Does each step of a task adequately cue the next step? If not, distractions or interruptions may cause the person to believe the task was completed (*i.e.*, lapsing) when in fact it wasn't or result in the person repeating an operation.

Table 40.3. (continued)

Use of Rules
• When people perform activities by resorting to rules such as "If conditions A B C exist then the problem must be X" or "If the problem is X then actions Y and Z are required," they are vulnerable to first exceptions. This may occur, for example, when conditions A B C exist but in a different context, which may now invalidate the rule or require its modification. For example, a wrong diagnosis is made based on discovering 3 features symptomatic of a condition; the critical absence of another feature, which would negate the diagnosis, was not taken into account. • Inadequate knowledge can lead a person to believe that a particular rule is appropriate when it is not. This often occurs if the person's knowledge represents a partial match of the antecedent conditions of the rule; however, because the other antecedent elements have not been verified, that rule may be invalid for that situation.
• A rule that has been used with frequent success will tend to be made to fit a situation; thus, information may be perceived incorrectly, in part because it is similar to antecedent information of a frequently used rule. • When people need to make up time or feel compelled to minimize effort, bad rules are often adopted. These often form the basis for violations of procedures ("If I do it that way, then all the orders should still be processed in time").
Psychomotor Control
• Due the inherent noise within the human's neuromuscular system, the human is limited in the accuracy associated with any given motor movement. • When the input bandwidth is high relative to the system lag, people usually correct too quickly and do not wait until the system output stabilizes before applying another corrective input (*i.e.*, they don't filter out the high-frequency inputs). • In general, bandwidth, gain, and lag can all produce instability in human control actions.
Personality and Risk Taking
• Some personality types tend to heed the advice of group authority figures within work groups or organizations, even if that advice (*e.g.*, what to do if a machine jams or minimizing safety implications in prioritizing objectives) may lead to very adverse outcomes. • People will tend to be more motivated to perform if human-machine interfaces are well designed, ergonomic factors have been given attention, people are given good training and job performance support, people are actively involved in the design of procedures and incident reporting systems, and both vertical and horizontal feedback channels are available to them. • People tend to give more weight to the severity of adverse outcomes as compared to the likelihood of adverse outcomes in their perceptions of risk. • Decreasing danger by increasing barriers or other safety improvements (*e.g.*, in sensors or warnings) may increase a person's risk-taking tendencies. • People are more likely to be at risk of injury or inducing system losses when they step out from under supervision and become more independent and active in their work activities, most likely due to still working with an incomplete mental model.

Table 40.3. (continued)

	Tendencies when Under Stress
• A person's risk taking behavior will, to some extent, be determined by whether they have adequate knowledge concerning whether a hazard exists, what actions are available to cope with the hazard, and what the consequences are of safe behavior versus alternative behaviors (by considering alternative actions based on the risks and values of their outcomes). • Familiarity with a device or hazard tends to decrease the perception of risk. Recent negative experiences with a device or hazard tend to increase a person's perception of that risk. • People with a "locus of control" that is primarily internal, so that they perceive themselves as having control over external events rather than the other way around, are more likely to be successful in coping with external events such as emergencies because they feel their actions can affect what happens to them. People with a "locus of control" that is primarily external may seek the help of colleagues because they assume that the situation is out of their control. However, the external personality may be more cautious during normal task activities in risk taking. • People described as having a type B personality (relaxed, relatively satisfied, not always fighting situations) may be more effective in performing under stress than people having a type A personality (feeling more pressured and preoccupied with success). However, the type A personality may be more motivated to accumulate knowledge and acquire high skill levels. • Risk-taking tends to be increased when people operate in a group, possibly due to the fact that responsibility becomes diffused across team members and the problem appears less unique when it is debated within a group discussion.	• If conditions are dangerous, people may rely on others to make a decision. • People tend to focus on explaining past facts, which may no longer be important for the problem on hand (but provides a sense of control). • People do not delegate responsibility well. • The information overload that typically accompanies stress can lead to short-term paralysis in processing available information, possibly due to the sudden transition from a relatively low information-processing state to an overloaded state. • Confirmation bias is more likely, where people seek information to confirm an initial hypothesis rather than information that may disconfirm it. • People seek a single cause and do not tend to think in terms of multiple causes, and also fail to recognize many of the alternatives that are available and adopt an approach that is familiar or that seems to offer "a way out" of the problem. • Focused attention (*i.e.*, mental effort) at will becomes more difficult, most likel y due to the scope and degree of distraction of attention processes. • People resort to encysting (excessive attention directed to possibly insignificant details while important aspects are disregarded) and thematic vagabonding (for example, when diagnosing a fault jumping from issue to issue, but never pursuing any theme to its natural conclusion, often picking up previously abandoned attempts, forgetting that they were already pursued).

Table 40.3. (continued)

Other Human Limitations
• Emotional states (as may be induced by personal difficulties, including problems a person may be having with coworkers) and the state of fear (as may be induced when performing under perceived dangerous circumstances) can induce various forms of physiological and psychological stress that, in turn, can produce many of the tendencies people display under stress. Overall, one may expect to see a loss in orientation (failing to remember where one is in the task or what one is supposed to do) and a lack of attention. • When people become fatigued, their ability to focus their attention and mentally process information becomes reduced, and their physical responses (especially in response to cues) become slower and more variable (*i.e.*, less controlled). • Disturbances to circadian rhythms due to sleep loss, shift changes, or other factors can lead to physiological and psychological stress responses.

References

[1] Kirwan B. A Guide to practical human reliability assessment. London: Taylor and Francis, 1994

[2] Kumamoto H, Henley EJ. Probabilistic risk assessment and management for engineers and scientists, Second Edition. Piscataway, NJ: IEEE Press., 1996

[3] Hollnagel E. Cognitive reliability and error analysis method. NewYork: Elsevier, 1998

[4] Bello GC, Colombari V. The human factors of risk analyses in process plants: The control room operator model "TESEO." Reliability Engineering 1980 1:3-14.

[5] Swain AD, Guttmann HE. Handbook of human reliability analysis with emphasis on nuclear power plant applications. NUREG/CR-1278, Washington, DC: U.S. Nuclear Regulatory Commission 1983.

[6] Wallace B, Ross A. Beyond human error: taxonomies and safety science. Boca Raton, FL: CRC Press, 2006

[7] CCPS (Center for Chemical Process Safety). Guidelines for Preventing Human Error in Process Safety. New York: American Institute of Chemical Engineers, 1994

[8] Koppel R, Metlay JP, Cohen A, Abaluck B, Localio AR, Kimmel S, Strom BL. Role of computerized physician order entry systems in facilitating medical errors. JAMA 2005; 293:1197–1203.

[9] Sharit J. Human error. In: Salvendy G, editor. Handbook of human factors and ergonomics, Third Edition. New York: Wiley, 2006; 708–760.

[10] Wears RL, Berg, M. Computer technology and clinical work: Still waiting for Godot. JAMA 2005 293:1261–1263.

[11] Perrow C. Normal accidents: Living with high-risk technologies. Princeton, NJ: Princeton University Press, 1999.

[12] Kirwan, B, Ainsworth LK. Guide to task Analysis. London: Taylor and Francis, 1992.

[13] Luczak H. Task analysis. In: Salvendy G, editor. Handbook of human factors and ergonomics, Second Edition. New York: Wiley, 1997; 340–416.

[14] Shepherd A. Hierarchical task analysis. London: Taylor and Francis, 2000.

[15] Wickens CD, Lee JD, Liu Y, Becker SE. An introduction to human factors engineering, Second Edition. Upper Saddle River, NJ: Pearson Education, 2004.

[16] CISHC (Chemical Industry and Safety Council). A Guide to Hazard and Operability Studies. London: Chemical Industries Association. 1977.

[17] CCPS (Center for Chemical Process Safety). Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples. New York: American Institute of Chemical Engineers, 1992

[18] Comer PJ, Fitt FS, Ostebo R. A Driller's HAZOP method. Society of Petroleum Engineers, SPE 15867, 1986.

[19] Sharit J. Perspectives on computer aiding in cognitive work domains: Toward predictions of effectiveness and use. Ergonomics 2003; 46:126–140.

[20] Hollnagel E. Barriers and accident prevention. Aldershot, England: Ashgate, 2004.

41

Risk Analysis and Management: An Introduction

Krishna B. Misra

RAMS Consultants, Jaipur, India

Abstract: Risk is the possibility of a hazardous event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of consequence (or impact) and likelihood of the event. Qualitatively, risk is considered proportional to the expected losses which can be caused by an event and to the probability of this event. Quantatively, it is the product of probability of hazardous event and the consequences. General views about risk perception and risk communication are discussed that help decision making. Risk management and risk governance along with probabilistic risk assessment and alternative approaches to risk analysis are also discussed.

41.1 Introduction

From the time of emergence of *Homo sapiens* on this planet, man with his intellect, inventive nature, ingenuity, and skills has always been trying to improve his living conditions and create favorable conditions for his survival. In this process, man created man-made systems for his own benefit and comfort. The history of industrial development indicates that as man has tried to use technology to improve his standard of living, in doing so several new problems not anticipated earlier have cropped up. Technology became a means to provide objects and conditions for sustenance and contentment, and technology can be viewed as the changing environment of humanity. Ingenuity and innovation were required to overcome several practical problems associated with new inventions and technological improvisations. In fact, right from the dawn of the industrial revolution, safety and dependability have been very much on the mind of man, and through innovative designs man has been resolving these safety and reliability problems very ably.

41.1.1 Preliminary Definitions

All technological advancements have *hazards* associated with them. A *hazard* is an implied threat or danger of possible harm. It is a potential condition to become a loss. A *stimulus* is required to cause the hazard to transfer from the potential state to a loss (or accident). This stimulus could be a component failure, a condition of the system, an operator failure, a maintenance failure, or a combination of other events and conditions. Thus a *stimulus* can be defined as a set of events or conditions that transforms a hazard from its potential state to one that causes harm to the system, property, or personnel. An *accident* is usually considered as the loss of a system or part of a system, injury to or fatality of operators or

personnel in proximity, and damage of property such as equipment or hardware. Technically speaking, an accident can be defined as a dynamic mechanism that begins with the activation of a hazard and flows through the system as series of events in a logical sequence to produce a loss. Simply put, an accident is an undesired and unplanned event. Now coming to the definition of *risk* in simple terms, it can be called the expected value of loss. Risk is associated with likelihood or possibility of harm. It would not be out of place to mention safety here and to underline its difference from risk, which some people often misunderstand. Safety, in simple terms, is the condition of being free from undergoing or causing harm, injury or loss. Safety can be thought of as characteristics of a system, like quality, reliability, or maintainability. Safety can be defined as an attribute of a system that allows it to function under predetermined conditions with an acceptable minimum accidental loss or risk. *System safety* is a planned, disciplined, systematically organized, and before-the-fact process characterized by an *identify-analyze-control* strategy. In fact, the emphasis is placed on an acceptable level of safety designed into the system before it is produced or put to operation. *Hazard analysis* is at the core of the system safety approach. Anticipating and controlling hazards at the design stage of an activity is the cornerstone of system safety analysis. Incidentally, system safety is not *failure analysis* since *hazard* has wider connotation than a *failure*. Hazard involves risk of loss or harm. A failure on the other hand is an unintended state of operation; a failure can occur without a loss. On the other hand, severe accidents have occurred while a unit was operating as intended, *i.e.,* without a failure.

41.1.2 Technological Progress and Risk

All technological developments in the history of mankind have had risks associated with them. Therefore one has to look into the benefits accruing from these developments and the risks that go with the use of such technological innovations. In fact, man has to learn to live with them and accept risks as part of life. But before we come to the subject of acceptability of risk, let us take a glance at technological developments chronologically.

Steam Age Accidents: In 1866, during the steam age, there were 74 steam boiler explosions in England, resulting in 77 deaths. This was reduced to 17 explosions with 8 deaths in 1900 as a result of inspections performed by Manchester Steam Users Association. Better designs, such as tube-fired boilers, and boiler inspections reduced it further to about once every 100,000 vessel-years.

Rail Accidents: The history of railroad travel is also very old and it is full of accidents, the causes of which can be traced either to natural calamities, to technical faults in the locomotives or the signaling system, or to human error. Derailing has been a major cause of accidents. The worst accident was in Sri Lanka in 2004 due to a tsunami, where some 1700 persons died, followed by one in Bihar, India in 1981, where over 800 persons died due to derailment and plunging of coaches into a river. Head-on collisions have also been reported. A Japanese train crash in 2005 is said to have occurred, killing 106 and injuring over 555 passengers due to driver's over-speeding to keep train schedule. This was Japan's most serious accident after a 1963 Yokohama train accident, when two passenger trains collided with a derailed freight train killing 162 passengers. The Intercity Express high speed train in Germany near Hanover met an accident on June 3, 1998 due to the breakage of the rim of an axle followed by a chain of events leading to a crash in which more than 101 were dead and several others injured. The train was travelling at a speed of 200 km per hour.

Marine Accidents: Ships, being the oldest mode of transport and trade, have their own risks associated with them. Later on, submarines were also added. Collision and grounding happen to be major causes of accidents throughout the long maritime history. The luxury liner Titanic was considered unsinkable until it sank on its maiden journey. Besides these, there have been many cases of engine failures, other technical faults, and fires onboard. The main difficulty is facility of repairs while on the high seas. Oil tankers have had oil spills, leading to ecological hazards and threat to marine life.

Road Accidents: With the development of personal vehicles or cars for transport towards the end of nineteenth century, these vehicles also became sources of risk. The first human fatality associated with a motor vehicle was a pedestrian killed in 1899. In 1990, about 5 million people died worldwide as a result of injury. It is estimated that by the year 2020, 8.4 million people will die every year from injury, and injuries from road traffic accidents will be the third most common cause of disability worldwide and the second most common cause in the developing world. Also, it is worth noting that the statistics show a ten to one ratio of in-vehicle accident deaths between the least safe and most safe models of car.

Aviation Accidents: Man entered the aviation age around the beginning of the twentieth century. In the beginning, the safety criteria of aircrafts was in terms of mean permissible failure rate but by 1940s the safety criteria began to be expressed in terms of the accident rate, and a figure of one accident per 10^5 hours of flying was acceptable. During the 1960s it was reduced to one in 10^6 landings of the aircraft, and finally with automatic landing systems it was reduced to one in 10^7, and travelling by air became safer and popular.

With the air traffic increasing enormously and airplane security having been advanced considerably, the accident data analyzed between 1970 and 2004 shows that accidents have decreased from over 300 in the 1970s to approximately 250 in the 1980s and 1990s. The maximum number of accidents was found in the year 1970, with a total of 38 planes. Since the late 1990s, the number of plane crashes has stabilized to approximately 22 per year.

The Tenerife Disaster remains the worst accident in aviation history. In this disaster, which took place on March 27, 1977, 583 people died when a KLM Boeing 747 attempted take-off without clearance and collided with a taxiing Pan Am 747 at Los Rodeos Airport. Pilot error, communications problems, fog, and airfield congestion (due to a bomb threat at another airport) all contributed to this catastrophe. Also, the crash of Japan Airlines Flight 123 in 1985 is the worst single-aircraft disaster. In this crash 520 died on board a Boeing 747. The aircraft suffered an explosive decompression, which destroyed its vertical stabilizer and severed hydraulic lines, making the 747 virtually uncontrollable.

Nuclear Age Accidents: Then came the nuclear age around middle of 1950s, and man has attempted, rather successfully, to anticipate the hazards before they would occur and learn to avoid them through design, control and regulation. But even after taking all these steps, accidents have taken place in nuclear plants, and the two most serious nuclear accidents, TMI-2 and Chernobyl-IV, had energy planners reconsider the desirability of nuclear option in the energy sector. On October 7, 1957, at Windscale Pile No. 1, north of Liverpool, England, a fire in a graphite-cooled reactor spewed radiation over the countryside, contaminating a 200-square-mile area. On March 28, 1979, at Three Mile Island near Harrisburg**,** Pa, USA, one of two reactors lost its coolant, which caused overheating and partial meltdown of its uranium core. Some radioactive water and gases were released. This was the worst accident in U.S. nuclear-reactor history.

The Chernobyl accident was the worst in the history of nuclear power plants, and as a result of this accident some 203 people were hospitalized with severe thermal burns and severe radiation exposure, while 31 people died (which is rather a very small number). Some 3,36,000 people in Ukraine, Belarus and Russia were relocated. About one-fifth of the population of Byelorussia was subjected to radioactive exposure of various intensities, and the republic lost over 1.6 million hectares (or 20%) of its farm land and one million hectares of its forests were affected by the nuclear radiation.

An uncontrolled chain reaction in a uranium-processing nuclear fuel plant in Japan on September 30, 1999 spewed high levels of radioactive gas into the air, killing two workers and seriously injuring one other. More recently, on July 17, 2007, radiation leaks, burst pipes, and fires at a major nuclear power plant at Kashiwazaki, Japan occurred following a 6.8 magnitude earthquake near Niigata. Japanese officials, frustrated at the plant operators' delay in reporting the damage, closed the plant a week later until its safety could be confirmed. Investigations revealed that the plant

had been sitting right on the top of an active seismic fault.

Space Age Accidents: The dawn of the space age in the latter half of the 1960s brought another technological feat to the credit of man's achievements, and along with it came a host of disasters. In June 1971 during Soyuz 11, all three Soviet cosmonauts were found dead in the craft after its automatic landing. The cause of death was reported to be due to loss of pressurization in the space craft during reentry into Earth's atmosphere. Again on March 18, 1980, a Russian Vostok rocket exploded on its launch pad while being refueled, killing 50 at the Plesetsk Space Center. On January 28, 1986, the *Challenger* **s**pace shuttle exploded 73 seconds after liftoff, killing all seven American crew members. A booster leak ignited the fuel, causing the explosion. On February 1, 2003, the *Columbia* **s**pace shuttle broke up on reentering Earth's atmosphere on its way to Kennedy Space Center, killing all seven crew members. Foam insulation fell from the shuttle during launch, damaging the left wing. On reentry, hot gases entered the wing, leading to the disintegration of the shuttle.

Chemical Plant Accidents: Accidents in chemical plants have had a very long history, and they have become quite alarming in intensity. Awards totaling $717.5 million were granted to next-of-kin and injured (29 were killed and 56 were injured) following an explosion at a Pyrotechnic plant in 1971, in which, according to the legal testimony, the plant operator had previously classified the ingredients and products as "flammable" instead of "explosives". A chemical company was fined $13.2 million for illegally dumping toxic chemicals into a city waste-treatment system. The city itself was previously fined $10,000 for permitting discharge of the pollution into the river. The contamination extended downriver into a bay and resulted in a major disruption of both commercial and sport fishing through 1980. According to one estimate, the entire 65 mile stretch of the river that had to be dredged would require several years and cost up to $200 million.

In 1974, an explosion took place in Nypro UK Chemical plant at Flixbourough, in which twenty-eight people were killed and some £36 million were paid towards the fire and accident damage following this explosion. The Bhopal gas tragedy and its disastrous consequences raise doubts over man's victory over nature to satisfy his materialistic needs. This tragedy, which struck on the night of December 2-3, 1984 due to leakage of methyl isocyanate gas on the unsuspecting sleeping population near the plant, left over 3700 people dead and about 150,000 affected. The compensation paid to the victims, decided mutually between the Union Carbide Company and the Government of India through an out-of-court settlement, was $470 million.

Water-reactive chemicals also deserve special mention, since their release almost always results in water contact with the material. In Somerville, Massachusetts a tank car ruptured on April 3, 1980, leaking phosphorous tri-chloride from the car into a nearby ditch. One observer reported that the responding fire company deliberately applied water to hasten hydrolysis, and hence increased the acidity and opacity of the cloud. In this event, 23,000 persons were reported evacuated, 120 persons reported to area hospitals for treatment, and the damage from the acid gas corrosion alone was estimated at least half a million dollars.

A liquefied petroleum gas leaking from a pipeline alongside the Trans-Siberian railway in the Ural Mountains near Uta, Russia, 72 miles east of Moscow, exploded on June 3, 1989 and destroyed two passing passenger trains, killing 575 and injuring 723 of an estimated 1200 passengers on both trains.

Sometimes a deliberate act on the part of a negligent manufacturer can cause havoc to the environment and surrounding habitat, which may threaten the life support system of earth. A major electric manufacturer was fined $4 million, in addition to an agreement to conduct a research program on environmental effects of PCB in order to assist in partial clean up of the upper Hudson river, because of its contamination over many years of the PCB used in electric capacitors and transformers. The present level of control is such that the plant now discharges less than one gram *per* day into the river (according to plant management). The cost of freeing the 35.7 mile

stretch of the river above Troy, New York was estimated at $150 million, as several towns and communities draw their water supply from this river.

Fire Accidents: On May 26, 1954, an explosion and fire on aircraft carrier *Bennington* killed 103 persons on board off Quonset Point, RI., USA. Again, on July 29, 1967, a fire on U.S. carrier *Forrestal* killed 134 persons on board off North Vietnam. A power-plant fire in Caracas, Venezuela left 128 dead on December.18-21, 1982. A fire on May 10, 1993 in a doll factory near Bangkok, Thailand killed at least 187 people and injured 500 others. It was the world's deadliest factory fire.

Coal Mine Accidents: On January 21, 1960, a coal mine explosion killed 437 in Coalbrook, South Africa. On November.9, 1963, an explosion in a coal mine at Omuta, Japan killed 447. A fire in a coal mine on May 28, 1965 in Bihar, India killed 375 persons. Another disaster, caused by an explosion followed by flooding in a coal mine at Dhanbad, India, killed 372 persons on December 27, 1975. In China too, a gas explosion at a coal mine on June 20, 2002 killed 111 people. The mining industry is one of the most unsafe industries in China; it is estimated that more than 5,000 mining-related deaths occurred in 2001. Again, a gas explosion killed 209 miners at the Sujiawan mine in Liaoning Province, China on February 14, 2005. It was the single deadliest reported mine disaster in China since 1949. A methane explosion in a coal mine in March 2007 in Ulyanovskaya, Russia killed 110 people, making it the worst mine disaster in recent Russian history.

All these events from the past are just a part of the scenario, which is full of hazards of all kinds and only indicate that the technological systems will continue to be used, but the least we can do is to improve the performance of plants, systems and products and design them to be safe enough and ensure that they have a very low acceptable risk and that the ecological and economic consequences of the possible accidents are minimal.

41.1.3 Risk Perception

Risk acceptability is always a subjective matter and depends upon the perception of the decision maker about the characteristics and severity of a risk. If the decision maker is forced to trade off well-being with monetary benefits, it would be easier to establish a criterion to accept a risk by making sure that the present worth of benefits is greater than the present worth of risk. But to many this approach is not acceptable as it places a monetary value on human life and well being. Several theories have been proposed to explain why different people make different estimates of the dangerousness of risks. Another way of looking at the acceptability of risk is to compare the risk under consideration with risks which were previously judged to be acceptable. The comparison is made by a risk spectrum curve, which shows the relationship between frequency and loss level. Logarithmic scales are generally used on both axes. Farmer's curve [1] is one such method of judging the risks. Risk spectra that exhibit higher frequency at higher levels of loss are less acceptable than otherwise. However, higher frequency at low loss levels will not be considered as critical. However, generalization based on this approach may not be appropriate.

Two major families of theory have been developed by social scientists: the psychometric paradigm and cultural theory. The study of risk perception arose out of the observation that experts and laymen often disagreed about how risky various technologies and natural hazards were. For example, most experts concluded that nuclear power is relatively safe, but a substantial portion of the general public sees it as highly dangerous. The obvious explanation seemed to be that the experts, having considered the evidence carefully and objectively, have a more accurate picture of the risks than did general public. Many experts continue to believe this theory. However, social science research on risk perception has been largely challenging this and proposing alternate explanations.

Starr, in an important paper [2], as early as 1969 offered an explanation to what risks are considered acceptable by the society. He assumed that society

had reached equilibrium in its judgment of risks, so whatever risk levels actually existed in society were acceptable. His major finding was that people accept risks 1,000 times greater if they are voluntary (*e.g.*, driving a car) than if they are involuntary (*e.g.,* having a nuclear plant in the neighborhood). In fact there are more people dying of road accidents than due to nuclear accidents [4] but the general public is often averse to nuclear power.

41.1.4 Risk Communication

Risk communication is the interactive exchange of information and opinions throughout the risk analysis process and concerns risk, risk-related factors, and risk perceptions among risk assessors, risk managers, consumers, industry, the academic community, and other interested parties and also includes the explanation of risk assessment findings and the basis of risk management decisions. Risk communication is a tool for creating the understanding that:

- Every choice/decision requires an understanding of their its risks and benefits,
- Closing the gap between lay people and experts, and
- Helping people make more informed and healthier choices.

Simple steps that can ensure the success of risk communication consist of:

- Understanding the underlying cognitive processes, values, and concerns brought by various sections of the society, and likely responses of these sections to risk issues;
- Developing strategies to enhance trust and minimize conflict between these sections on risk issues; and
- Developing organizational policies and messages responsive to the risk concerns of these sections.

41.2 Quantitative Risk Assessment

No industrial activity [5, 10, 11, 15, 22, 34, 54, 58, 60, 61, 68, 70, 71, 76] is entirely free from risk, since it is not possible to eliminate every eventuality by safety measures. However, when risks are high, system designers must consider the possibilities of additional preventive or protective risk-reduction measures that can be achieved and judge whether it would be reasonable to implement these additional measures. Therefore, it becomes imperative to assess the risk of an industrial activity/plan quantitatively and ensure its safety before it is undertaken for construction or commissioning.

In fact, quantitative risk analysis [52, 76, 77] consists of seeking answers to the following questions:

- What can possibly go wrong that could lead to a hazardous outcome?
- How likely is this event?
- If that happens, what consequences can be expected?

To answer the first question, scenarios of events leading to the outcome should be defined, and to answer the second question, the likelihood of these scenarios must be evaluated. Lastly, to answer the third question, the consequences of each scenario should be evaluated. Therefore, quantitatively, the risk is defined by the following triplet:

$$R = <S_i, P_i(\text{or } Fi), C_i> \quad i=1, 2,..., n \qquad (41.1)$$

where S_i, P_i, (or Fi), and C_i are the ith scenario of events, leading to hazard exposure, likelihood (or frequency) of scenario i and the consequences of scenario i (a measure of the degree of damage or loss), respectively. The likelihood of event E_i is expressed in terms of the probability of that event, and the frequency is expressed per year or per event basis in units of time. Lastly, C_i is expressed in terms of damage to property, number of fatalities, dollars loss, *etc.*

The results of risk estimation are used to interpret various contributors to risk which can be compared and ranked. The process consists of :

1. Calculating and displaying graphically the risk profile on a logarithmic scale.
2. Calculating the total expected risk from

$$R = \sum_i P_i \; C_i . \qquad (41.2)$$

There are two ways of interpreting results. One way is to calculate expected values using (41.2) and is useful when the consequences are in financial terms. Another way is to construct a risk profile. In this case risk values are plotted against consequence values. Sometimes the logarithm of probability that the total consequence C exceeds C_i is plotted against the logarithm of C_i. This is also known as *Farmer's curve* [1] and was a landmark in reactor safety study [4].

Quantitative risk assessment usually involves [8, 15, 16, 20, 26, 68, 69, 72, 73, 74, 75, 76] three stages. These are: *risk identification* (the recognition that a hazard with definable characteristic exists); *risk estimation* (the scientific determination of the nature and level of the risks); *risk evaluation* (judgment about the acceptability or otherwise of risk probabilities and the resulting consequences).

Risk identification and estimation are both concerned with collecting information on:

- The nature and extent of the source;
- The chain of events, pathways and processes that connect the cause to the effects; and
- The relationship between the characteristics of the impact (dose) and the types of effects (response).

Through risk identification, we recognize that a hazard exists and try to define its characteristics such as chemical, thermal, mechanical, electrical, ionizing or non-ionizing radiation, biological, *etc*. Each of the identified hazards is examined to determine all physical barriers that contain it or can intervene to prevent or minimize the exposure to the hazard. Identification of each of the barriers is followed by a concise definition of the requirements for maintaining each of them.

Identification of Sources or Risk

The first step in a system risk analysis is the identification of the sources of risk to the system. In being able to identify sources of risk, it is essential for the analyst to be familiar with the system under consideration. Typically, a study or review team should be established. The team will comprise mainly managers, engineering staff, operators, and other personnel who are involved in the operation of the system or who contribute to its performance. The range of knowledge and experience of the study team is a major factor in its effectiveness and hence in the competence of the study. However, it should be recognized that it may not be possible for the team to identify all possible failure scenarios or hazards, particularly where these arise from "unforeseen" events or processes.

The following techniques have been used in the identification of sources of risk:

1. Preliminary hazard analysis (PHA) [3];
2. Failure modes and effect analysis (FMEA) [26, 56, 57];
3. Failure mode, effect and criticality analysis (FMECA) [22];
4. Hazard and operability studies (HAZOP) [3].
5. Incident databanks.

These techniques have been used for a large range of engineering systems, with the possible exception of HAZOP, which tends to be specific to the chemical and process industries. In addition, various other methods have been proposed, though these are often adoptions of the above methods to suit a specific system or problem. It will be seen that the methods to be described tend to be complementary; for example, guide lists, checklists or reference to incident databanks are often used to check that no source of risk has been omitted from the analysis. PHA is used to identify the major hazards for a system, their causes, and the severity of the consequences. Typically it is used at the preliminary design stage. The identification in a PHA of major hazards will usually invoke more detailed analyses using methods such as FMEA, FMECA and HAZOP because of its preliminary status, and it would not be expected that a PHA will identify failure of specific individual equipment which has the potential to lead to a major hazard. This is the role for FMEA, FMECA and HAZOP. FMEA is an inductive analysis because it starts at the possible outcomes and works backwards to obtain all possible causes. Hence it is essential that the identification of failure modes be as extensive as possible. This may be difficult, particularly for large systems. For this reason, generic guidelines or checklists are often

used to ensure that all failure modes are considered. The analysis involved in a FMEA generally is presented in a tabulated format in a manner similar to that used for a PHA. FMECA, or simply criticality analysis, is a logical extension of FMEA in which failure events are categorized according to the seriousness of their possible effect. In FMECA both the failure frequency (probability) and the failure effect (consequence) are assessed subjectively to determine the criticality of each failure mode. This should take account of each component and each sub-system. The failure frequency is rated in terms of a subjective likelihood such as expressed by "very low, low, medium, and high". The severity is assessed into one of a number of subjective severity levels. The HAZOP technique was developed by Lawley [3] in 1974 at ICI and is widely used in the chemical and the process industries to identify hazards or operating problems in new or existing plants. The HAZOP technique is a systematic process in which process flow diagrams are used to consider each plant item (*e.g.,* pipes, valves, computer software) in turn, so that problems which could occur with these items may be considered.

Results from a HAZOP usually are summarized in tabular worksheet form. The tables normally contain the following entries:

1. *Item:* individual components in the system (*e.g.*, pipes, vessels, relief valves);
2. *Deviation:* identify what can go wrong (*e.g.*, more pressure, no transfer, less flow);
3. *Causes:* causes of each deviation (*e.g.*, equipment failure, operator error);
4. *Consequences:* identify effects on other components, operability and hazards associated with each deviation (*e.g.*, line fracture, backflow, leakage, fire, explosion, toxic release, personnel injury); and
5. *Actions:* measures or actions required to further reduce the deviations or the severity of the consequences (*e.g.,* process design changes, equipment changes or modifications).

Risk Estimation

The next step in risk assessment is to define those scenarios in which the barriers may be breached and then make the best possible estimate of the probability or frequency for each exposure. Often, risks are measured for some time before their adverse consequences are recognized. These include the magnitude, spatial scale, duration and intensity of adverse consequences and their associated probabilities, as well as a description of the cause and effect links. Both risk estimation and identification [26] can involve modeling, monitoring, screening, and diagnosis.

Accident data, "near misses", reliability data and other statistics that describe the past performance of systems also may be used to help identify potential major hazards in a system and their causes and consequences. The techniques described above assist in the identification of those individual system elements (components and subsystems) that are potentially hazardous. This information may be used in the development of a representation of the overall system in terms of logic diagrams. These identify the sequences or combinations of events or processes necessary for system failure to occur. As noted earlier, such system representation diagrams are an aid in the understanding of the behavior of the system, and hence may suggest, without formal risk analysis, obvious measures for reducing the risk of system failure. Of course, detailed understanding of the system and its representation in a logical fashion is required for quantitative analysis of the system. Such analysis also requires quantification of system element performance. The quantification of the overall system reliability has been discussed in more detail in Chapter 19 in this handbook.

The essential (and most common) techniques used for schematic representation of a system (*i.e.*, its "modeling") are:

1. Fault trees [13, 17, 20, 21, 23, 27, 31, 32, 36, 42, 59, 63, 79] and
2. Event trees [7, 18, 26, 33, 45, 51, 76].

A decision tree is a special case of event tree. Other methods, such as fault graphs [30], cause-consequence diagrams [58], and reliability block

diagrams [59] incorporate significant features of event tree and fault tree techniques and will not be discussed. Fault trees and event trees have much in common. Whether one or the other or some combination is applied depends much on the preferences and practices within a given industry.

Fault trees and event trees have been applied extensively for qualitative and quantitative risk studies in the nuclear industry and the chemical process industries and to a lesser extent elsewhere. Automated fault tree generation [12, 13, 14, 36] has also received attention from researchers, but today expert systems can be developed to carry out FMEA, FTA and reliability and safety analysis as was discussed in Chapter 19 of this handbook. Digraphs and causal trees [64] have also been used in system safety and risk analysis. Two landmark risk analysis applications of fault trees and event trees were in the US nuclear safety study (RSS, 1975) [4]. It is the main method recommended for US nuclear risk studies [7, 46], in part because of its ability to model very complex accident sequences, including those involving dependency between events. Considerable amount of work has been done in the area of human reliability analysis [18, 19, 35, 39, 40, 43, 47, 55, 66, 73, 76]. Also, the work in the aerospace industry for human reliability analysis has made use of event tree methods extensively. Event trees and fault trees are best developed by a study team (*i.e.*, a panel of specialists), and their discussions may be likened to a "brain-storming" session where specific risks, events and scenarios and their control are suggested. It is at this stage that decisions can be made as to which risks are to be included and omitted from a risk analysis. In other words, the scope of the risk analysis can be defined.

We have included a detailed and exclusive coverage of fault trees in Chapter 38 of this handbook.

It is sometimes assumed, for ease of analysis, that any dependence between the outcomes of events may be ignored. This assumption usually is incorrect. System risk estimates calculated on the basis of assumed complete dependence between events may be considerably greater than estimates determined for the same events being assumed to be completely independent. Dependence between event failures (also known as cascade failures) can occur when more than one component in a system fails simultaneously due to a common cause. In this case the components do not fail independently of each other. For example, an external cause (such as environmental loads like wind and earthquake or man-imposed factors) may affect more than one component in the system. In general, dependent failures can have a dramatic effect on the risk associated with a project and must be properly identified and accounted for. It follows that the treatment of dependency between events is an important matter for risk analysis. There has been considerable amount of research in handling common cause failures in risk and safety analyses [6, 9, 14, 24, 28, 29, 37, 38, 44, 65, 67, 76, 78].

The estimation of system risk requires the quantitative description of both the frequency and the performance of those system elements directly influencing system risk. This means that the performance of components, items of equipment, loads, resistances, and human actions must be known, and the consequences of failure must be able to be estimated. The quantitative description of the performance of each system element usually will be a variable—either a point estimate (*i.e.*, deterministic) variable (*e.g.*, mean failure rate) or a random variable (*e.g.*, probability distribution of failure rates).

In order to cover common cause failures and human aspects of the risk assessment problem, we have included Chapter 39 exclusively on common cause failure modeling and Chapter 40 on human-system interaction for the benefit of the reader.

Risk Evaluation

The range of effects produced by exposure to a hazard may encompass harm to people, damage to equipment, and contamination of land and facilities. Therefore a third component of *risk assessment* is risk evaluation, in which judgment is made about the significance and acceptability of risk probabilities and corresponding consequences. This stage leads to policy formulation. Evaluation techniques seek to compare risks against benefits, as well as to provide ways in which the social acceptability of risks can be judged.

After the risk has been identified, estimated and evaluated (or any combination of the three), there comes a point where some kind of intervention (or deliberate decision not to intervene or to delay action) must be made. What is the course of development that is "safe enough?" A safe or less risky course of development would be one which would be compatible with the environment and can be called *eco-development*. It would not only minimize or reduce risks to acceptable levels for those who are subjected to risk, but also for those who create risks and those responsible for managing them. There is always a cost attached to the risks and the benefits flowing from a project, plant or a system. Therefore one has to work out the *risk/benefit* ratio. In considering risk/benefit trade-offs, it is essential to remember that for every benefit we usually incur some risk or cost, however small it may be.

Through safe design and better performance of these systems, we can minimize the ecological impacts and associated losses. Lastly, we have worked out the advantages accruing from these systems *vis-à-vis* the risk involved in using them. In other words, we must address the issue of acceptable risk *vis-à-vis* employing the technologies.

41.3 Probabilistic Risk Assessment

Definition of Objectives: As the first step, the objectives of probabilistic risk assessment (PRA) or probabilistic safety assessment (PSA) are set and defined. The resources required for each analytical options are evaluated, and the most effective alternative is selected.

Physical Layout of the System: The physical layout of the system or process, including facility, plant and design, administrative controls, maintenance and test procedures, as well as protective systems (those which maintain safety), is necessary to start the PRA. This will help generate all possible scenarios. All major safety and emergency systems must be identified and taken into consideration.

Identification of Initiating Events: Here we identify all those sets of events that could result in hazard exposure. The first step is to identify sources of hazards and barriers around these hazards. The next step is of course to identify events that can lead to a direct threat to the integrity of barriers.

Sequence of Scenario Development: In this step all possible scenarios are considered that encompass all the potential paths that can lead to loss of containment of the hazard, following the occurrence of an initiating event. The scenarios are often displayed by event trees.

System Analysis: The procedure followed in this step is to develop a fault tree for each event tree heading. Model dependencies and common cause failures models and all potential causes of failures, of hardware, software, test and maintenance, and human errors are included in the development of a fault tree. External events are also considered.

Data Analysis: At this point, we determine generic values of failure rates and failures on demand probabilities for each component in the fault tree. We also determine test, repair and maintenance data from generic sources or from experience; the frequency of initiating events and other component from experience or generic sources; and the common cause failures probabilities likewise.

Quantification: Fault tree and event tree sequences are quantified to determine the frequencies of scenarios and associated uncertainties in the computation.

To provide an insight of PRA to the reader, Chapter 43 on probabilistic risk assessment, including a case study, is included in this handbook. Also Chapter 71 on PRA as applied to nuclear power plants is included in this handbook to provide detailed in formation to the reader. In fact, PRA in the case of nuclear plants has three levels. Level I PRA simply calculates the core melt probability and is purely a system failure event. Level II considers the probability of failure of containment, and Level III considers the probability of release of radioactivity to the surroundings and its consequences.

41.3.1 Possibilistic Approach to Risk Assessment

We have seen there is always a gap between perceived risk and statistical risk. This is basically due to the fact that statistical risk is based on the probability theory of random ocurrences of events, whereas human thinking works on the basis of possibility. Attempts have been made to capture the subjectivity in human thinking by objectively formulating the risk assessment problem on the platform of fuzzy set theory, which appears to make this possible. Several contributions [25, 41, 49, 50, 53, 60, 62] have been made in the direction of a possibilitistic approach using fuzzy set theory, but at this moment, the researchers are transforming the problem by taking recourse to probability and possiblity compatibility principles as has been suggested in [25, 48, 50]. A better approach would be to assess system performance in a possibilitic framework directly (as is suggested in [49]), thus bringing modeling close to the way the human brain processes the situation.

Dempster–Shafer theory also provides an alternative to the probabilistic approach. For the benefit of the reader, we have included Chapter 31 on these aspects of the problem in this handbook. In fact, in the opinion of the author, fuzzy set theory provides a natural and very appropriate approach to overcome the problem of statistical risk and uncertainties associated with it and to resolve the problem of perceived and statistical risk. Human thinking is close to the possibilistic approach and does not rely on statistical values even if supported by tight confidence limits.

41.4 Risk Management

Risk management is an activity which integrates recognition of risk, risk assessment, developing strategies to manage it, and mitigation of risk using managerial resources. The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk. Some traditional risk managements are focused on risks stemming from physical or legal causes (*e.g.*, natural disasters or fires, accidents, death, and lawsuits). Financial risk management, on the other hand, focuses on risks that can be managed using traded financial instruments.

The objective of *risk management* is to reduce different risks related to a pre-selected domain to the level accepted by society. It may refer to numerous types of threats caused by environment, technology, humans, organizations, or politics. On the other hand it involves all means available. In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled in descending order. In practice the process can be very difficult, and balancing between risks with a high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

Intangible risk management identifies a new type of risk—a risk that has a 100% probability of occurring but is ignored by the organization due to a lack of identification ability. For example, when deficient knowledge is applied to a situation, a knowledge risk materializes. Relationship risk appears when ineffective collaboration occurs. Process-engagement risk may be an issue when ineffective operational procedures are applied. These risks directly reduce the productivity of knowledge workers and decrease cost effectiveness, profitability, service, quality, reputation, brand value, and earnings quality. Intangible risk management allows risk management to create immediate value from the identification and reduction of risks that reduce productivity.

Risk management also faces difficulties allocating resources. This is the idea of opportunity cost. Resources spent on risk management could have been spent on more profitable activities. Again, ideal risk management minimizes spending while maximizing the reduction of the negative effects of risks.

Steps in the risk management process:

- Identification of risk in a selected domain of interest;
- Planning the remainder of the process;

- Mapping out the following: the social scope of risk management, the identity and objectives of stakeholders, and the basis upon which risks eventually will be evaluated (constraints);
- Defining a framework for the activity and an agenda for identification;
- Developing an analysis of risks involved in the process; and
- Mitigation of risks using available technological, human, and organizational resources.

Chapter 44 has been included in the handbook to discuss the subject of risk management in detail.

41.5 Risk Governance

It is true that individual capacities and responsibilities of different players, *viz*, government departments, the scientific community, NGOs, business community, or society at large in the arena of risk are limited, and it is absolutely desirable to have some kind of coordination and understanding between their goals, perceptions and activities, particularly to cope with disasters that require coordinated efforts of all sections and cutting across the boundaries of the countries, sectors, hierarchical levels, disciplines.

Risk governance is a concept that not only includes "risk management" or "risk analysis", it also looks at how risk-related decision-making can be affected to meet the major challenges facing society today, particularly those related to natural disasters, food safety or critical infrastructures. Risk governance also takes in view factors such as historical and legal backgrounds, guiding principles, value systems, and perceptions as well as organisational imperatives.

To put in place the framework and coordinate risk governance efforts, an independent organization named *International Risk Governance Council* (IRGC) was founded in June 2003 at the initiative of the Swiss government. The mission of IRGC is to help the understanding and management of global emerging risks that impact human health and safety, the environment, the economy, and society at large, besides developing the concepts of risk governance, anticipating major risk issues, and providing risk governance policy recommendations for key decision makers.

IRGC undertakes project work in four main areas:

- Risks associated with the mitigation of or adaptation to the effects of climate change.
- The security of energy supplies.
- Disaster risk governance.
- Risks associated with new technologies.

IRGC is a foundation funded by several governments and industries. The organizational structure comprises a Board, a Scientific and Technical Council, an Advisory Committee and a full-time Secretariat based at the foundation's headquarters located in Geneva, Switzerland.

Considering the importance of the subject, this handbook has included Chapter 45 on risk governance.

References

[1] Farmer FR. Reactor safety and siting: A proposed risk criterion. Nuclear Safety 1967; 8: 539.
[2] Starr C. Social benefits versus technological risk. Science 1969; 165:1232–1238.
[3] Lawley HG. Operability studies and hazard analysis. In, Howe J (editor) Chemical Engineering Progress. American Institute of Chemical Engineers 1974; 70(4): 45–56.
[4] WASH-1400 (NUREG-75/014). Reactor Safety Study: An assessment of accident risks in commercial nuclear power plants, Nuclear Regulatory Commission, USA Oct. 1975.
[5] Brown DB. Systems analysis and design for safety. Prentice Hall, Englewood Cliffs, NJ,1976.
[6] Apostolakis GE. The effect of certain class of potential common-cause failures on the reliability of redundant systems. Nuclear Engineering Design 1976; 36: 123–133.
[7] Levine S, Vesely WE. Important event-tree and fault-tree considerations in the reactor safety studies. IEEE Transactions on Reliability 1976; Aug., R-25 (3): 132–139.
[8] Fussell JB, Lambert HE. Quantitative evaluation of nuclear system reliability and safety characteristics. IEEE Transactions on Reliability 1976; Aug., R-25 (3): 178–183.

[9] Vesely WE. Estimating common-cause failure probabilities in reliability and risk analyses: Marshall–Olkin specializations. In Fussel JB, Burdick GR, editors. Nuclear systems reliability engineering and risk assessment. SIAM, Philadelphia, PA, 1977; 314–341.
[10] Rowe WD. An anatomy of risk, Wiley, New York, 1977.
[11] Lewis EG. Nuclear power reactor safety. Wiley, New York, 1977.
[12] Misra KB, Thakur R. Development of fault tree for reliability studies of a data processing system. International Journal of System Sciences 1977; 8(7): 771–780.
[13] Willie RR. Computer aided fault tree analysis. Operation Research Center, ORC, University of California, Berkeley 1978; Aug., 78–14.
[14] Apostolakis G, Garribba S, Volta G. Synthesis and analysis methods for safety and reliability studies, Plenum, New York, 1980.
[15] McCormick NJ. Reliability and risk assessment, Academic Press, New York, 1981.
[16] Kaplan S, Garrick J. On the quantitative definition of risk. Risk Analysis 1981; 1(1).
[17] Vesely WE, Goldberg FF, Roberts NH, Haasl DF. Fault tree handbook. NUREG-0492, US NRC, 1981.
[18] Rasmussen J. Human reliability in risk analysis. In Green AE, (Ed.) High risk safety technology. Wiley, London 1982; 143–170.
[19] Adams JA. Issues in human reliability. Human Factors 1982; 24: 1–10.
[20] Taylor TR. Algorithm for fault tree construction. IEEE Transactions on Reliability 1982; June, R-31 (2): 137–146.
[21] Joller JM. Constructing fault-trees by stepwise refinement. IEEE Transactions on Reliability 1982; Oct., R-31 (4): 333–338.
[22] Fawcett HH, Wood WS. Safety and accident prevention in chemical operations, Wiley, New York, 1982.
[23] Cummings DL, Lapp SA, Powers GJ. Fault tree synthesis from a directed graph model for a power distribution network. IEEE Transactions on Reliability 1983; June, R-32 (2): 140–149.
[24] Dunglinson C, Lambert H. Interval reliability for initiating and enabling events. IEEE Transactions on Reliability 1983; June, R-32 (2): 140–163.
[25] Tanaka H, Fan LT, Lai FS, Toguchi K. Fault-tree analysis by fuzzy probability. IEEE Transactions on Reliability 1983; Dec., R-32 (5): 453–457.
[26] Roland HE, Moriarty B. System safety engineering and management. Wiley, New York, 1983.
[27] Modarres M, Dezfuli H. A truncation methodology for evaluating large fault trees. IEEE Transactions on Reliability 1984; Oct., R-33 (4): 320–322.
[28] Evans MGK, Parry GW, Wreathall J. On the treatment of common-cause failure in system analysis. International Journal of Reliability Engineering 1984; 9(2):107–115.
[29] Walle RA. A brief survey and comparison of common-cause failure analysis NUREG/CR-4314, Los Alamos National Laboratory, Los Alamos, NM, 1985.
[30] Alesso HP, Prassinos P, Smith CF. Beyond fault trees to fault graphs. International Journal of Reliability Engineering 1985; 12 (2): 79–92.
[31] Lee WE, Grosh DL, Tillman FA, Lie CH. Fault tree analysis, methods and applications- a review. IEEE Transactions on Reliability 1985; Aug., R-34 (3): 194–203.
[32] Wilson JM. Modularizing and minimizing fault trees. IEEE Transactions on Reliability 1985; Oct., R-34(4): 320–322.
[33] Lakner AA, Anderson RT. Reliability engineering for nuclear and other high technology systems: A practical guide. Elsevier, New York, 1985.
[34] Westman, WE. Ecology, impact assessment, and environmental planning, Wiley, New York, 1985.
[35] Dhillon BS. Human reliability with human factors. Pergamon, New York, 1986.
[36] Kumamoto H, Henley EJ. Automated fault tree synthesis by disturbance analysis. Industrial and Engineering Chemistry Fundamentals. 1986, 24(2): 2333–239.
[37] Heising CD, Luciani DM. Application of a computerized methodology for performing common cause failure analysis: The Mocus–Bacfir Beta Factor (MOBB) code. Reliability Engineering 1987; 17(3):193–210.
[38] Hoghes RP. A new approach to common cause failure. International Journal of Reliability Engineering 1987; 17(3): 211–236.
[39] Sharit J. A critical review of approaches to human reliability analysis. International Journal of Industrial Ergonomics 1988; 2:111–130.
[40] Inagaki T, Ikebe Y. A mathematical analysis of human-machine interface configurations for a safety monitoring systems. IEEE Transactions on Reliability 1988; April, R-37(1): 35–40.
[41] Onisawa T, Nishiwaki Y. Fuzzy human reliability analysis on the chernobyl accident. Fuzzy Sets and Systems 1988; 28:115–127.
[42] Kohda T, Henley EJ. On diagraphs, fault trees and cut sets. Reliability Engineering and Systems Safety 1988, 20 (1): 35–61.

[43] Apostolakis GE, Bier VM, Mosleh A. A crique of recent models for human error rate assessment. Reliability Engineering and System Safety 1988; 22: 201–217.
[44] Hokstad P. A shock model for common-cause failure. Reliability Engineering and System Safety 1988; 23(2): 127–145.
[45] Fullwood, RR, and Hall RE. Probabilistic risk assessment in the nuclear industry: Fundamentals and applications, Pergamon, Oxford, 1988.
[46] International Nuclear Safety Advisory Group: Basic safety principles for nuclear power plants, Safety Series, No. 75-INSAG-3, IAEA, 1988.
[47] Dougherty Jr. EM, Fragola JR. Human reliability analysis: a systems engineering approach with nuclear power plant applications. Wiley, New York, 1988.
[48] Onisawa T. An application of fuzzy concepts to modeling of reliability analysis. Fuzzy sets and Systems 1990; 37: 389–393.
[49] Misra KB, Weber GG. A new method for fuzzy fault tree analysis. Microelectronics and Reliability 1989; 29(2): 195–216.
[50] Misra KB and Weber GG. Use of fuzzy set theory for level-1 studies in probabilistic risk assessment. Fuzzy Sets and Systems 1990; 37: 139–160.
[51] Kenaranuie R. Event-tree analysis by fuzzy probability. IEEE Transactions on Reliability 1991; April, R-40 (1): 120–124.
[52] Inagaki T. Interdependence between safety-control policy and multiple sensor schemes via Dempster–Shafer theory. IEEE Transactions on Reliability 1991; June, R-40 (2): 182–188.
[53] Guth MAS. A probabilistic foundation for vagueness and imprecision in fault tree analysis. IEEE Transactions on Reliability 1991; Dec., R-40 (5): 563–571.
[54] Greenberg, HR , Cramer JJ (Eds.), Risk assessment and risk management for the chemical process industry, Van Nostrand Reinhold, New York, 1991.
[55] Sharit J, Malon DM. Incorporating the effect of time estimation into human-reliability analysis for high-risk situation. IEEE Transactions on Reliability 1991; June, R-40(2): 247–254.
[56] Zaitri CK, Keller AZ, Fleming PV. A smart FMEA (failure modes and effects analysis) package. Proceedings Annual Reliability and Maintainability Symposium, Las Vegas, Nevada, USA; Jan 21–23, 1992; 414–421.
[57] Russomanno DJ, Bonnell RD, Bowles JB. Computer-aided FMEA forward an artificial intelligence approach. Fifth International Symposium on Artificial Intelligence, AAAI Press, New York, 1992; 103–112.
[58] Henley EJ, Kumamoto H. Probabilistic risk assessment-reliability engineering, design and analysis. IEEE Press, New York, 1992.
[59] Misra, K.B., Reliability analysis and prediction: A methodology oriented treatment, Elsevier, Amsterdam, 1992.
[60] Misra K.B. (Ed.), New trends in system reliability evaluation, Elsevier, Amsterdam, 1993.
[61] Modarres M. Reliability and risk: What an engineer should know about. Marcel Dekker, New York. 1993.
[62] Soman KP, Misra KB. Fuzzy fault tree analysis using resolution identity. International Journal of Fuzzy Sets and Mathematics 1993; 1:193–212.
[63] Kumamoto Hiromitsu. Fault tree analysis. In Misra KB, editor. New trends in system reliability evaluation. Elsevier, Amsterdam, 1993; 249–310.
[64] Kohda Takehisa, Inoue Koichi. Diagraphs and causal trees. In Misra KB, editor. New trends in system reliability evaluation. Elsevier, Amesterdam, 1993; 313–336.
[65] Hokstad Per. Common cause and dependent failure modeling. In Misra KB, editor. New trends in system reliability evaluation. Elsevier, Amsterdam, 1993; 411–441.
[66] Sharit Joseph. Human reliability modeling. In Misra KB, editor. New trends in system reliability evaluation. Elsevier, Amsterdam, 1993; 369–408.
[67] Dhillon BS, Anude OC. Common-cause failures in engineering systems: A review. International Journal of Reliability, Quality, and Safety 1994; 1(1): 103–129.
[68] Misra, K.B. (Ed.). Clean production: environmental and economic perspectives, Springer, Berlin, 1996.
[69] Stewart MG, Melchers RE. Probabilistic risk assessment of engineering systems. Chapman and Hall, New York, 1997.
[70] Modarres M, Kaminskiy M, Krivtsov V. Reliability engineering and risk analysis: A practical guide. Marcel Dekker, New York, 1999.
[71] Cagno E, Giulio A.Di, Trucco P. Risk and causes of risk assessment for an effective industrial safety management. International Journal of Reliability, Quality, and Safety 2000; 7(2): 113–128.
[72] Hayakawa Yu, Paul S. F. Yip. A Gibbs-sampler approach to estimate the number of faults in a system using capture-recapture sampling. IEEE Transactions on Reliability 2000; Dec., 49(4):342–350.
[73] Pasquini Alberto, Pistolesi Giuliano, Rizzo Antonio. Reliability analysis of systems based on software and human resources. IEEE Transactions on Reliability 2001; Dec., 50(4): 337–345.

[74] Jin Tongdan, Coit David W. Variance of system-reliability estimates with arbitrarily repeated components. IEEE Transactions on Reliability 2001; Dec., 50(4): 409–413.
[75] Wang J, Yang JB. A subjective safety and cost based decision model for assessing safety requirements specifications. International Journal of Reliability, Quality, and Safety 2001; 8(1): 35–57.
[76] Modarres M. Risk analysis in engineering: Techniques, tools and trends. Taylor and Francis, New York, 2006.
[77] Latino RJ, Latino KC. Root cause analysis: Improving performance for bottom-line results. Taylor and Francis, New York, 2006.
[78] Lixuan Lu, Lewis G. Reliability evaluation of standby safety systems due to independent and common cause failures. IEEE International Conference on Automation Science and Engineering CASE '06 2006; 8–10 Oct.: 264–269.
[79] Limnios Nikolaos. Fault trees. ISTE, London, 2007.

42

Accident Analysis of Complex Systems Based on System Control for Safety

Takehisa Kohda

Kyoto University, Kyoto, Japan

Abstract: In modern complex systems such as chemical and nuclear plants, as its hardware system reliability increases due to the advancement of technology, systemic failures such as software design errors become a significant contributor to system accidents. State-of-the-art computers have made many technology-based systems so complex that new types of accidents now result from dysfunctional interactions between system components, further adding to the number of accidents resulting from component failure. Other factors, such as management effectiveness and organizational constraints, must also be considered as part of a failure prevention strategy. Conventional event-based analysis methods such as fault trees cannot be always applied to such types of accidents. This chapter applies a concept of system control for safety to the accident analysis in two ways. The first part deals with accident cause analysis, while the second part deals with the accident analysis in the defense-in-depth approach.

42.1 Introduction

Accident analysis plays an important role in both accident investigation and risk assessment, and both aspects are required for effective risk/safety management. In the identification of accident causes, an accident model plays a fundamental role in accident investigation and accident cause analysis. The depth or resolution of an analysis result depends on its accident model. One conventional accident model is an event-based (or sequential) model, such as event trees [1], where the system accident is the end state of a cause-effect sequence initiating from a deviation caused by a failure event such as component failure, human error, or external disturbance. However, the remarkable progress in computer and information technology makes interactions among system components so complex that a new type of accident appears, namely, a deviation not corresponding to a fault can lead to an accident even though components behave as they are specified. This accident is called a systemic accident. Further, since one of the main accident contributors, human error, is greatly affected by organizational and management factors, the background factors of both human errors and component failure must be considered for effective countermeasures. Unfortunately, the event-based model cannot address these problems properly, because it stops the identification process of system accident causes at the component failure level. Root causes are rarely identified. To meet the demands in this situation, a system accident cause

analysis method based on the concept of system control for safety [2, 3] has been devised. The first part of this chapter introduced this kind of method [4] and shows the accident analysis of a railway accident [5].

In PRA (Probabilistic Risk Assessment) [1], firstly all possible accident event sequences leading to a severe accident must be identified, and then an appropriate measure must be taken for a specific accident sequence selected based on its estimated risk. Thus, the derivation of accident occurrence conditions is the most important part of PRA, whose correctness determines the validity of analysis results. However, the derivation conventionally depends on the subjective judgment of system analysts and designers, which might cause an error. To obtain an objective accident occurrence condition, the second part applies the concept of "safety control functions" to not only the derivation of accident occurrence conditions in an event tree model for a specific disturbance or initiating event, but also the analysis of their failure conditions. An illustrative example of a collision accident on a single railway track shows the applicability and effectiveness of the proposed method [6].

42.2 Accident Cause Analysis Based on Safety Control

42.2.1 Safety from System Control Viewpoint

The conventional accident model in the PRA assumes that an accident is caused by an abnormal event leading to a system failure with malfunctions of protective systems, and focus on the identification of contributing factors to the significant accident scenarios [1]. In the presented model [2, 4], system safe states are considered to be always maintained under the system control for safety, and an accident can occur due to deviation from the system boundary conditions under the safety constraints. Since the complete prevention of a failure is impossible, more attention should be paid to the entire system safety control functions than to component failure. System normal states cannot be maintained without the system control for safety. From the system control viewpoint, the system can be represented in terms of three basic concepts: safety constraints, safety control loop, and hierarchical structure.

42.2.1.1 Safety Constraints

The proposed model is based on the relationship between system components from a systems control viewpoint. Components are largely divided into two classes: controlling and controlled ones. Figure 42.1 shows a schematic relation of two components, where the upper component controls the lower component.

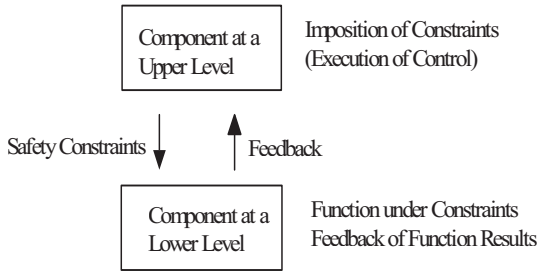


Figure 42.1. Safety constraints and feedback

Since the behavior of the lower component is constrained by the objective of the upper component, a control action of the upper component can be represented as a safety constraint imposed on the lower component. The response of the lower component can be represented as its feedback to the upper component. Based on the feedback, the upper component must modify its control action to maintain its objective. Using this control loop composed of safety constraint and feedback, the goal state of system control can be maintained. The entire system structure from the viewpoint of system safety can be reconfigured based on the interactions required to satisfy the system safety constraints.

42.2.1.2 System Control Loops

To maintain the control relation successfully, the controller must have some functions. Assume a basic system control function shown in Figure 42.2.

Based on the general theory of systems control [7], the following requirements must be satisfied

for the system control function to achieve its objective function.

1. The controller must have a goal to achieve.
2. The controller must be able to affect the state of a system to be controlled.
3. The controller must be (or have) a model of the controlled system.
4. The controller must be able to estimate the state of the system.

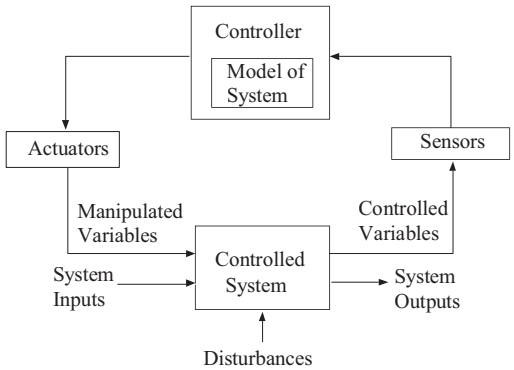


Figure 42.2. Basic control function

In Figure 42.2, controllers such as human operators and computers must obtain the information on the system state to be controlled (Requirement 4) and control the manipulated variables using the actuators to keep the controlled system within the system safety boundary conditions. Based on the system control model, a system accident can occur due to its dysfunction, which may be caused not only by its component failure, but also by an incorrect system model or incorrect control rules. The latter corresponds to systemic failure.

From the requirements for successful system control, causes of its malfunction can be classified as shown in Table 42.1 [3]. In this classification, possible factors other than component failure can be identified. Classification 1 is dysfunction related to the imposition of safety constraints, classification 2 is the dysfunction related to the execution of system control actions, and classification 3 is related to dysfunction caused by the feedback mechanism. A systemic failure can be identified as a control function error due to an incorrect system model. A system accident analysis is performed based on the assumption that dysfunction of safety control loops causes a system accident.

Table 42.1. Causes of malfunctions of system control

1. Inadequate control commands (or imposition of constraints)
1.1 Unidentified hazards
1.2 Inappropriate, ineffective or missing control for identified hazards; Design of control algorithm does not impose constraints; Inconsistent, incomplete, or incorrect system model; Inadequate coordination among controllers and decision makers
1.3 Inadequate controller operation
2. Inadequate execution of control action
2.1 Communication flaw between controller and actuator
2.2 Inadequate actuator operation
2.3 Time lag
3. Inadequate or missing feedback
3.1 No provision in system design
3.2 Communication flaw between system and controller
3.3 Time lag
3.4 Inadequate sensor operation

42.2.1.3 Hierarchical Control Structure for Safety

Based on the control relation, components can be decomposed into two classes: controlling and controlled ones. This viewpoint shows a kind of hierarchical structure. The higher level (controlling part) imposes safety constraints on the lower level (controlled part) as its safety control, while the lower level feeds the result of its performance back to the higher level. All the components in a system organization can be related to one another based on the control structure, and thus the effect of decisions at the management level on the operational level can be considered. In other words, the effect of organizational factors on an accident can be analyzed.

Figure 42.3 shows an example of the system control structure composed of design, manufacturing, operation, and maintenance of an artifact

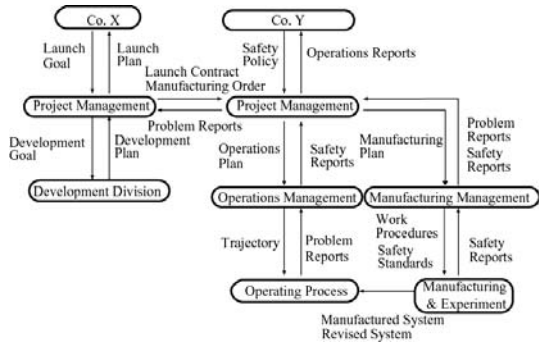


Figure 42.3. An example of hierarchical control structure

[8]. Two basic hierarchical structures, system development and operation, can be identified. An arrow shows information flow or action flow between two components: a component at an upper level imposes safety constraints on its lower component, while the lower level component gives the feedback of its performance result to its upper component. If the feedback information is not consistent with the safety constraint, the corresponding control loop may produce a dysfunction, whose effect propagates across the related hierarchical structure. Thus, based on the hierarchical structure of control loops, the effect and cause of a dysfunction of a safety control function can be analyzed.

42.2.2 Accident Analysis Procedure

To identify causal factors of a system accident to be analyzed, the general accident analysis procedure using the concept of system control for safety can be described as follows:

(1) Definition of system accident: A system accident or system danger must be defined to represent the abnormal system state condition explicitly. As shown in Figure 42.3, the system accident state generally appears as an abnormal state at the lowest level of system operation or the operating process.
(2) Identification of proximate control systems: By checking whether it can detect the abnormal state condition defined at step (1), any proximate control system related to the system accident can be identified.
(3) Identification of dysfunctions of proximate control systems: For each proximate control system obtained at step (2), all possible dysfunctions can be identified as proximate causes of the system accident by examining whether it meets any possible dysfunction condition in the checklist.
(4) Repetitive identification of dysfunctions of the related control systems: By regarding a dysfunction obtained at step (3) as an abnormal system state condition at step (1), background factors of the dysfunction can be obtained in the same way as steps (1) to (3). This procedure should be repeated until further expansion is impossible for any identified dysfunction.

Thus, the proposed method can identify background factors at the upper level by tracing related control systems sequentially from proximate control systems to control systems at upper levels. In other words, all latent problems in the hierarchical control structure can be identified step by step. Similarly, the effect of a proximate control system containing the system abnormal condition can be also investigated in the detail using the forward search in the hierarchical structure. Note that the overall hierarchical structure of control systems can be identified in two ways. One is through the step-by-step procedure in the identification process of the accident analysis. The other is based on the definition of control system specification at the system design stage.

42.2.3 Illustrative Example

Consider the train accident—a fall from an iron bridge—on 28 December 1988 in Japan [9]. Due to strong winds, seven out-of-service passenger cars of a train fell from an iron bridge accidentally, killing five workers at a food processing factory under the bridge and the train conductor, with six seriously injured persons.

42.2.3.1 System Control for Train Protection

In addition to a height of 41 m, the geographical location of the bridge—between two mountains—makes the passage of wind from the sea narrowed,

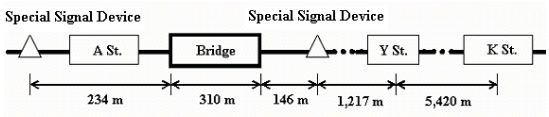


Figure 42.4. Location of special signal devices, stations and bridge

causing an increase of wind velocity. So, passenger trains can be easily exposed to strong wind conditions. Therefore, while the ordinary operating rule of the railway stops a train in case the instantaneous wind velocity is over 30 m/sec, the allowable maximum instantaneous wind velocity in this district is fixed as 25 m/s. Figure 42.4 shows position relations among the iron bridge, nearby stations, and the special signal devices.

The wind warning system was composed as follows.

1. The wind velocity on the bridge was measured by two sets of three-cup formula anemometers installed in the bridge piers, and their output signals were transmitted to the following three places: a strong wind alarm device at the CTC (Centralized Traffic Control) center, and a strong wind alarm device at Y station, and a strong wind alarm device and a wind velocity recorder at K station.
2. Depending on the larger measurement value of the two anemometers, three kinds of warning alarms can be issued. If the maximum instantaneous wind speed (MIWS) is larger than 15 m/sec, the yellow light comes on. If the MIWS is larger than 25 m/sec, the red light comes on and a buzzer sounds. The light and alarm buzzer were set to stay on for three minutes. However, if the alarm buzzer was stopped by an operator, it would not be available for three minutes, and then would be restored to run based on wind velocity measurement. Further, the alarm device does not show the wind velocity.
3. If one of the strong wind alarm devices issues the alarm with a MIWS of 25 m/sec or larger, the operator at the CTC center will change the corresponding signals to stop signals by remote control.
4. Two special signal devices, whose purpose is to stop a train in an emergency situation, are placed at both sides of the bridge: 234 m in the upside and 146 m in the downside. The operator at the CTC center operates the special signal devices by remote control.

One of two anemometers had broken down about one month before the accident, and it had not been repaired when the accident occurred. Due to the difference in their installation place, the monitored values were different. The anemometer broken at the time tended to show the larger value. Moreover, fences or frames to prevent trains from falling off the bridge were not attached at the time of the train accident due to weakness in the bridge piers.

42.2.3.2 Accident Background

In 1961, an alarm interlocked with a wind velocity transmitter was installed for upward trains, and a special signal device was installed and operated manually at Y station. Later, in 1970, the introduction of the CTC changed the operational environment. The special signal device was operated by the CTC center, and the alarm device was removed. Then, another special signal device was installed for downward trains. Before the accident, one of the anemometers was out of order. The accident occurred as follows:

9:00: Persons-in-charge were checked at the roll call.

Before 13:00: The yellow light came on, which showed that the MIWS was over 15 m/sec.

13:10: The red light and buzzer came on, which showed that the MIWS was over 25 m/sec. The CTC center made inquiries about the wind condition at K station, and K station answered, “Although the wind blew at 25 m/sec before, it is now blowing at 20 m/sec”. The CTC center did not turn on the special signal devices.

13:15: The train left K station toward the bridge.

13:21: The red light and buzzer came on, and the staff at K station telephoned the operation staff at the CTC center, “The recorder shows that the wind is now blowing at 30 m/sec or more at the moment, doesn’t it?” However, the operation staff

regarded it as a thing of the past and judged that the wind had lessened to below 25 m/sec. The train passes Y station.

13:23: The train passed by the special signal device.

13:25: The train was lashed by the strong wind and caused to fall from the bridge.

42.2.3.3 System Control for Wind Protection

The system control structure for the safe passage of a train over the iron bridge is shown in Figure 42.5. Most of relations between components have a single directed path, and there exist few control loops with safety constraints and feedback.

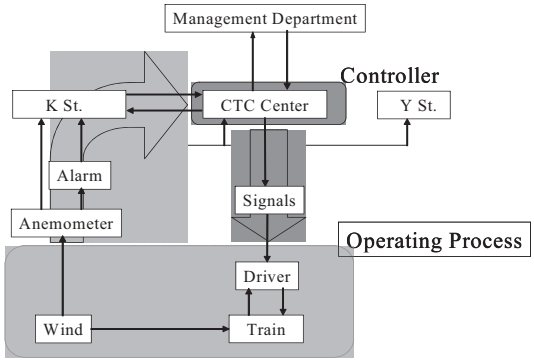


Figure 42.5. Control systems for wind protection

Although a train and its driver compose a control loop, the driver cannot directly monitor the effect of wind on the train, nor can he control it. Therefore, the protective measure against the influence of a wind is a feedback control where the CTC center plays the role of a controller. Wind is monitored by anemometers, and based on the alarm information, the CTC center gives a stop command to the driver through the special signaling device. The driver corresponds to a kind of actuator in the control loop and stops the train according to the signal devices. The management department affects the safety measures of the CTC center by giving it the operational instructions and so on. This constitutes another control loop.

42.2.3.4 Accident Cause Analysis

Since the control loop against the effect of wind cannot control the wind directly, the protective action is to stop the operation of a train when winds are strong. The control loop—which consists of wind, an anemometer, an alarm device, the CTC center, a special signaling device, a driver, and a train—is a proximate control loop related to the accident. Since the apparent cause of the accident is the inaction of the proximate control loop for the wind protection, applying the checklist about the cause of its malfunction can give the results shown in Table 42.1.

Although the accident occurred directly because the train passed through the bridge with strong winds, the incorrect judgment concerning the effect of the wind and the insufficient feedback of the wind conditions are obtained as the causal factors. For the former case, the adequate real-time information on the wind velocity was not available, and the feedback system of adequate information on wind is to be improved. The latter corresponds to the judgment error of the CTC center about the recognition of the influence of wind, but the judgment of the CTC center is affected by the

Table 42.2. Dysfunction in operating process

Check Item	Present	Note
1		
1.1	No	Danger of a train fall was recognized
1.2		
1.2.1	No	Following the rule could prevent the accident
1.2.2	Yes	Regardless of alarms, the staff at the CTC center did not issue the stop signal, and instead made inquiries to K station
1.2.3	-	
1.2.4	-	
2	No	No abnormality was identified in signal devices or driver actions
3		
3.1	-	
3.2	Yes	The report from K station was misunderstood
3.3	Yes	The alarm did not show the real time information on the site, and continued to ring for three minutes
3.4	Yes	The more conservative anemometer was not operational

Table 42.3. Dysfunction of operation management

Check Item	Present	Note
1.		
1.1	-	
1.2		
1.2.1	-	
1.2.2	Yes	The CTC center had overarching authority on train operation
1.2.3	-	
1.2.4	-	
2	-	
3		
3.1	-	
3.2	-	
3.3	-	
3.4	Yes	Customary practice of violating the rule (inquiry to K station) was overlooked

control loop between the CTC center and the operation management department.

Applying the checklist about the cause of malfunctions of a control loop, background factors of the immediate factors are obtained as shown in Table 42.3. As the CTC center had the overarching authority on the train operation, not only the appropriate treatment at the site became difficult, but also the understanding of the current conditions at the site. These causal factors can be clarified by investigating the hierarchical control structure in the operation of wind protection from the viewpoint of the malfunction of management structure.

In this example, the accident cause analysis is examined based on the position that an accident originates in the malfunction of the system control for safety, and it is shown that the background factors are systematically identified based on the hierarchical control structure of the system from the direct cause of the accident.

42.3 Accident Occurrence Condition Based on Control Functions for Safety

In PRA, all possible accident event sequences leading to a severe accident must be identified, and then appropriate measures must be taken for a specific accident sequence, selected based on its estimated risk. Thus, the derivation of accident occurrence conditions is the most important part of PRA, the correctness of which determines the validity of analysis results. However, the derivation conventionally depends on the subjective judgment of system analysts and designers, which might cause an error. To obtain objective accident occurrence conditions, the concept of "safety control functions" is applied to not only the derivation of accident occurrence conditions in an event tree model for a specific disturbance or initiating event, but also the analysis of their failure conditions [10]. An illustrative example of a collision accident on a single track railway shows the applicability and effectiveness of the proposed method [6].

42.3.1 General Accident Occurrence Conditions

Generally speaking, to prevent and mitigate a system accident, several types of safety protective systems are installed in such large scale systems as chemical and nuclear plants and railway systems. The concept of "independent protection layers" [11] or "defence in depth" [12] is a standard approach for safety design in these complex systems. To mitigate the effect of a failure of some protective system, another independent protective system is installed in the system. Figure 42.6 shows a schematic diagram for multilayered protective systems in a chemical plant. Considering the occurrence of an accident in this kind of system, the accident occurs due to the failure of its safety control functions. Here, safety control functions mean not only safety protective systems, but also human actions to reduce the risk caused by a disturbance or component failure. A safety control system corresponds to a set of components which accomplish a safety control function. If a safety control system is normal, it can accomplish its function to prevent or mitigate a disturbance.

Thus, for a system accident to occur, the following two conditions must be satisfied:

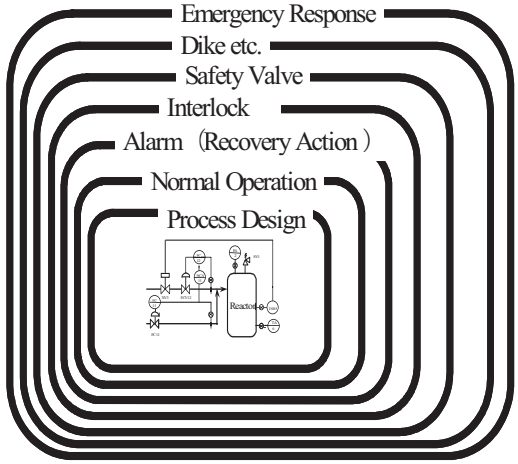


Figure 42.6. Independent protection layers

(C1) A disturbance such as human error and component failure must occur which can cause an initial deviation leading to a system accident.

(C2) Safety control systems must fail which would otherwise prevent or mitigate the disturbance.

As shown in Figure 42.7, accident occurrence conditions in the event tree can be represented as logical AND combinations of the occurrence conditions of a disturbance and the failure conditions of safety control functions related to the disturbance. To obtain the accident occurrence conditions, both disturbances leading to system accidents and safety control systems related to them must be identified.

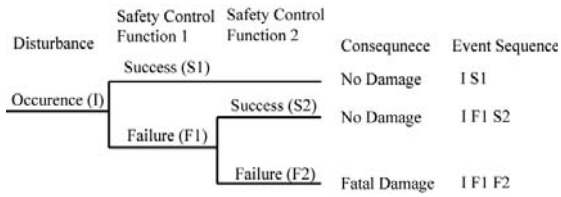


Figure 42.7. Event tree for a system accident

42.3.2 Occurrence of Disturbances

To identify a disturbance or initiating event which can cause a system accident, there are two types of approaches: bottom-up and top-down. The former corresponds to FMEA (Failure Mode and Effect Analysis) [13], while the latter corresponds to FTA (Fault Tree Analysis) [14]. In the FMEA, the possible effect of a component failure, human error, or external event is evaluated from the component level to the system level using functional relations among components in the system hierarchical structure. Based on its effect on the system, a disturbance to be considered for the safety design can be selected. On the other hand, in the FTA, an end state or a system accident to be prevented and mitigated is defined firstly, and then a logic tree is constructed step-by-step, which shows the cause-effect relationship between the system accident and basic events representing component failure and human errors. Minimal combinations of basic events (or component failures) and disturbances leading to the system accident can be obtained, each of which corresponds to an occurrence condition of the specified system accident. In the proposed method, the FMEA approach is applied to the selection of an initiating event based on the previous accident data. So, the disturbance to be mitigated is given first.

42.3.3 Safety Control Function Failure

Safety control functions, which can prevent or mitigate a specific abnormal event, are generally composed of three basic functions: detection, diagnosis, and execution. Detection consists of monitoring system states continuously or periodically to get information on the current state of the plant, and detecting any abnormality. Diagnosis is composed of identifying the cause of the system abnormality and selecting an appropriate control action. Execution corresponds to the execution of the selected control action. Corresponding to these basic functions, the safety control system can be composed of three parts: sensing part, controlling part, and executing part. The primary function of a component can show which part of a safety control system it constitutes. For each disturbance or initiating event, safety control functions which can prevent it must be identified. By examining whether its sensing part

can detect the effect of a disturbance or not, a safety control system related to the accident can be easily identified. Investigating the information flow from the sensing part, the whole structure of a safety control system can be identified, where each basic function can be achieved by a different system component such as a human operator or a computerized machine.

In obtaining the failure conditions of a safety control system, its decomposition into sensing, controlling, and executing parts can clarify what kinds of dysfunction can happen. It can, for example, obtain possible failure conditions in detecting a disturbance. The following questions must be answered: Is the subject disturbance assumed in the design? Which sensing part can detect the subject disturbance? How can the sensing part fail? In this way, all possible causes of the detection failure can be identified. For a safety control function to work successfully, all three basic functions must work successfully. Thus, the failure condition of a safety control system can be obtained as a logical OR combination of the failure conditions of each part. For example, consider an operator recovery action initiated by an alarm. The alarm corresponds to the detection of a disturbance, and the operator plays the role of diagnosis of the disturbance and execution of an appropriate action. In this case, both the normal function of the alarm and the successful performance of the human operator are essential to accomplish the safety control function. Human errors such as perceptional errors and mistakes must be considered, because the diagnosis and execution actions are required of human operators. Human factor analysis [15] should be performed by focusing on the basic functions allocated to operators, and this can also clarify the necessary interactions of human operators with system components.

42.3.4 Collision Accident Example

This section shows the details of the proposed method by analyzing a collision accident in a single track railway as shown in Figure 42.8.

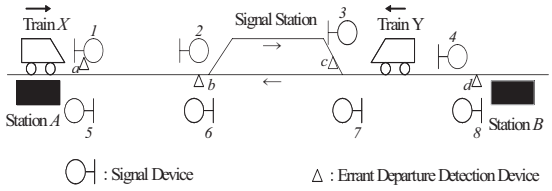


Figure 42.8. Single track railway

42.3.4.1 System Description

Consider a single track railway consisting of stations *A* and *B* and a signal station between them. At the signal station, each train always runs in the left-side track due to a turnout mechanism of points, which can make for a safe crossing of two trains at the signal station. The safety principle in a single track railway is that only one train is allowed to run in a block section. The single track between stations *A* and *B* can be largely divided into three block sections: (b1) the section between station *A* and the signal station, (b2) the section including the signal station, and (b3) the section between the signal station and station *B*. "Single track" implies that a collision accident can happen if two opposite trains exist together in block sections (b1) or (b3). To carry out the safety analysis, assume that eight signal devices and four errant departure detection devices [16] are installed as shown in Figure 42.8. Signal devices are used to keep one train in a block section. Here, signal devices are controlled by a "special automatic block" rule [16]; only one direction in a block section must be allowed for a train which enters it first. Errant departure detection devices can prevent an accident caused by the errant departure of a train ignoring the red signal. For example, if train *Y* accidentally passes across errant departure detection device *b* with signal *6* being red, signal *1* turns red to stop train *X* at station *A*. In this way, an errant departure detection device and a signal device paired together can prevent a collision accident.

42.3.4.2 Safety Control Function

In this example, a collision accident can occur if the safety principle is violated, or two trains exist together in a block section. To prevent a collision accident, the signal system and errant departure

detection devices are installed to maintain the safety principle. The signal system is regarded as a part of the safety control function, because it only gives train drivers orders to follow the safety principle. To achieve the safety control function, the final control action to stop a train must be taken by the driver. Thus, the signal system combined with train drivers constitutes a safety control system. Further, for a train to stop according to the driver action, its braking system must function successfully. Similarly, an errant departure detection device paired together with a signal device can be regarded as sensing and diagnosis parts of a safety control system to give a train driver orders to stop before entering the block section. Thus, an errant departure detection device, a signal device, and a driver with a braking system together comprise another safety control function. In both safety control systems, the final control action must be taken by a driver, whose error leads to a fatal accident even if the hardware devices are normal. Further, the frequency of human error may be much higher than the failure frequency of hardware components. Thus, the role of the driver in each safety control function is essential.

In addition to the above safety control actions, another general safety control action must be taken by drivers. A driver must stop his train if he cannot confirm its safety or if he detects an abnormal condition. This requirement implies that a driver by himself constitutes a safety control system—if he detects an abnormal condition, he must select an appropriate action to stop the train and execute that action. Similarly to the previous control actions, the braking system must be normal for the stop action to be accomplished. In this safety control procedure, detection is very important, which not only triggers the actions following it, but also limits the allowable time to take an appropriate action. In a collision accident, the available time when a driver detects a train approaching him has a large effect on the severity of an accident.

Thus, three kinds of safety control systems are assumed in this example: (s1) signal system and driver with braking system, (s2) errant departure detection device, signal, and driver with braking system, and (s3) drivers by themselves with braking systems.

42.3.4.3 Accident Occurrence Conditions

We now obtain accident occurrence conditions for a collision accident of trains *X* and *Y*. Let us assume an initiating event that train *X* accidentally departs from station *A*, neglecting signal *1* being red, after train *Y* leaves station *B* for station *A* and train *X* continues toward station *B*. Let this condition be denoted as (a0), the errant departure of train *X*.

We examine the availability of each safety control system for the errant departure of train *X*. For each safety control system to function, it must detect the occurrence of a disturbance. Firstly, this disturbance can be detected by errant departure detection device *a*, which turns signal *6* red, thereby preventing train *Y* from entering block section (b1). In safety control system (s3), drivers in trains *X* and *Y* can detect the effect of the disturbance or the possibility of a collision accident when the trains come within sight of each other. This detection can occur after the detection by errant departure detection device *a*. On the other hand, the signal system by itself cannot detect the effect of this disturbance. Thus, only safety control systems (s2) and (s3) can prevent the accident.

Next, we consider the effectiveness of safety control systems (s2) and (s3). Since safety control system (s2) prevents train *Y* from entering block section (b1), it will be of no effect if train *Y* is already in block section (b1) when errant departure detection device *a* detects the errant departure of train *X*. The initial position of train *Y* when train *X* makes an errant departure determines the effectiveness of safety control system (s2). Safety control system (s3) can be effective regardless of the initial position of train *Y*, because it functions just before a collision occurs. Thus, the initial position of train *Y* can be divided into two possible conditions:

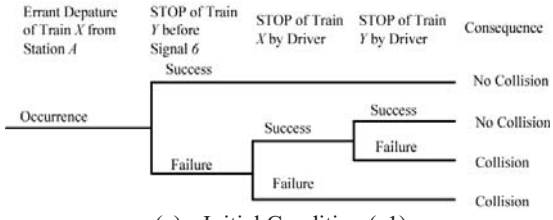
(a1) Train *Y* is running on the approach to signal *6* with a consistent signal condition, where at least signals *6* and *7* are green (to go) and signals *1* and *2* are red (to stop), and

(a2) Train *Y* is in block section (b1) after passing signal *6*.

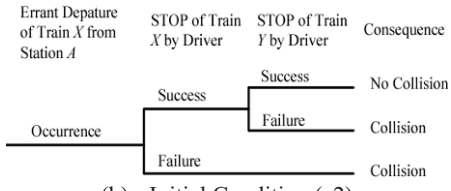
Available safety control systems can be obtained for each condition as follows.

For (a1), we obtain (s2) signal *6* with driver action and (s3) driver actions at trains *X* and *Y*.

For (a2), we obtain (s3) driver actions at trains *X* and *Y*.



(a) Initial Condition (a1)



(b) Initial Condition (a2)

Figure 42.9. Event tree representation

Figure 42.9 shows event trees for these two initial conditions. To avoid a collision accident, two countermeasures are possible in this single track railway: (c1) trains *X* and *Y* cross each other at the signal station and (c2) trains *X* and *Y* stop before the collision. In initial condition (a1), two successful event sequences are possible. The event sequence at the top represents the first case (c1), where train *Y* stops before the exit of the signal station on the right side of train *X* so that they can cross each other. Even if countermeasure (c1) fails, countermeasure (c2) can be applied as shown in the second event sequence. Each driver notices the other train approaching him and stops his train. In initial condition (a2), since train *Y* passed by signal *6* before train *X* departed from station *A* accidentally, errant departure detection device *a* was of no effect. The only available counter-measure is (c2). The top event sequence in Figure 42.9(b) corresponds to this successful case. Comparing event trees for initial conditions (a1) and (a2), the event tree for (a2) has fewer safety control systems, and the drivers must play a more important role. As this example shows, the availability of safety control systems depends on the initial condition of where a disturbance or initiating event occurs. Not only its sensing action to detect a disturbance, but also its control action must be considered for a safety control system in evaluating its effectiveness on the disturbance.

42.3.4.4 Derivation of Accident Occurrence Conditions

To obtain accident occurrence conditions of a collision accident, failure conditions must be obtained for each safety control system related to its initiating event or disturbance. Since a safety control system is considered to be a series structure of sensing, diagnosis, and execution parts, its failure condition is a logical OR combination of the failure conditions of each part. The accident occurrence conditions can be obtained as a logical AND combination of a disturbance occurrence condition and the failure conditions of its effective safety control systems.

We now obtain failure conditions of safety control system (s2). Since it is composed of errant departure detection device *a* and signal *6*, the sensing part detects the errant departure of train *X* and gives warning to the driver of train *Y*. Detection failure is due to the failed-dangerous failure (or failure-to-detect) of the errant departure detection device *a* OR the communication failure of signal *6* (or failure to communicate information to the driver). The driver plays the role of diagnosis and execution. If signal *6* is red, the driver must stop train *Y* before exiting the signal station. Otherwise, the driver will continue to run train *Y*. Generally, a driver action initiated by a signal can be divided into the detection of the signal, the judgment and selection of an appropriate operation, and the execution of it. However, since the stop/go operation depending on the signal can be considered as a kind of stimulus-response action of a well-trained driver, omitting the judgment part, its error can be evaluated as a skill-based error. Failure to detect a red signal can be evaluated as a perceptional error. Even if the driver makes no error, a braking system failure can nullify his protective action. A braking system failure in train *Y* must be included as a failure condition of the driver's stop action. Thus, the failure condition of safety control system (s2) can

be represented as a logical OR combination of the following failure conditions:

(b1) the failed-dangerous failure of errant departure detection device *a*,
(b2) the communication failure of signal *6*,
(b3) the driver at train *Y* fails to detect the red signal,
(b4) the driver at train *Y* fails to stop his train, and
(b5) the braking system at train *Y* fails to stop train *Y*.

A stop action of a driver by himself can be also divided into (1) detection of an approaching train and (2) execution of a stop action while warning the other driver. Here, the diagnosis and selection of an appropriate action in this emergency condition can be committed as a single action combined with execution, because the countermeasure to be taken is obvious for the well-trained driver to prevent an accident. Since both drivers must stop their trains, the failure conditions of safety control system (s3) are obtained as a logical OR combination of the following conditions:

(c1) the driver at train *X* fails to detect train *Y* approaching,
(c2) the driver at train *X* fails to stop his train,
(c3) the braking system at train *X* fails to stop train *X*,
(c4) the driver at train *Y* fails to detect train *X* approaching,
(c5) the driver at train *Y* fails to stop his train, and
(c6) the braking system at train *Y* fails to stop train *Y*.

In both initial conditions, the drivers' errors must be evaluated for safety control system (s3). Although the logical expressions of the failure conditions are the same under both cases, the dependency among human errors must be considered by focusing on the differences in their event sequence conditions. For example, in the third sequence of the event tree for initial condition (a1) (see Figure 42.9(a)), the driver at train *Y* commits the same type of errors twice. A more accurate evaluation of human errors is to be desired, so a more detailed analysis of the above conditions must be performed from the viewpoint of human factors [15]. For simplicity of discussion, we do not expand the above conditions further.

Accident occurrence conditions for initial condition (a1) can be obtained as:

{a0 AND a1} AND {b1 OR b2 OR b3 OR b4 OR b5} AND {c1 OR c2 OR c3 OR c4 OR c5 OR c6}

Thirty minimal cut sets are obtained. For initial condition (a2), since safety function (s2) is of no effect, accident occurrence conditions can be obtained as:

{a0 AND a2} AND {c1 OR c2 OR c3 OR c4 OR c5 OR c6}

Comparing these two cases, the number of minimal cut sets is less in initial condition (a2), which means that initial condition (a2) is more dangerous and that drivers' control actions are more serious. In particular, a human error in driver action constitutes a single component failure condition of a system accident, neglecting the occurrence of the initial condition. Even in initial condition (a1), human errors of the driver at train *Y* appear as failure conditions (b3), (b4), (c4) and (c5). Further, the failure condition of braking systems at train *Y* appears as (b5) and (c6). Though safety control systems apparently seem redundant, the common cause failures, human errors of the driver of train *Y* and failure of the braking system at train *Y*, induce the simultaneous failure occurrence of safety control systems (s2) and (s3). To prevent this condition, an alternative protection measure must be devised. In the next section, the effect of adding an automatic train stop (ATS) (or automatic train protection, ATP) [17] is considered.

42.3.4.5 Evaluation of Improvement by ATS

To mitigate the effect of a driver's erroneous omission of stop actions, assume that ATSs are installed at all signals. The basic function of an ATS is to warn a driver approaching the red signal to stop the train, and to forcibly stop the train when the driver does not make an appropriate response. If a driver stops the train appropriately, the ATS will not force his action. The ATS can take an emergency stop action in place of a driver if he fails to do it. The ATS control action is activated

by the corresponding signal turning red. Thus, the ATS can supplement a safety control function performed by a signal paired with a driver. Figure 42.9 shows general event sequences including an ATS. The addition of ATSs can reduce the contribution of drivers' errors to a collision accident. Failure of a safety control system with an ATS requires failure of the ATS, which increases the size of its minimal cut sets. In other words, it decreases its occurrence probability or frequency.

Similarly to the safety control system, an ATS can be also divided into three parts. The sensing part consists of a wayside coil on the track to send information of a red signal to the train, and a pickup coil on a train to receive the information. Thus, the sensing part fails if either the wayside coil OR the pickup coil fails. The relay circuit on the train corresponds to the diagnosis part, which triggers an appropriate command signal to the execution part depending on the driver action. A diagnosis part failure occurs if the relay circuit fails. The control actions are divided into two types: warning by alarm and compulsory stop of the train. The execution parts correspond to the alarm system, and the braking system, respectively. Depending on the situation, the failure condition of the alarm or the braking system constitutes a failure condition of the execution part. Even if the alarm system fails, the normal braking system can prevent a collision accident. In this sense, the failure conditions of the execution part correspond to those of the braking system.

From the above consideration, the ATS cannot be effective for a safety control system without signals. In the above example, the ATS is effective for safety control systems (s1) and (s2), but not for (s3) where no signal devices are available. So, the addition of ATSs is effective only for initial condition (a1) where safety control system (s2) is available. Safety control system (s2) can be improved by adding ATSs, which is denoted as safety control system (s2′). The failure conditions of safety control system (s2′) can be obtained as:

(b1′) the failed-dangerous failure of errant departure detection device *a*,
(b2′) the communication failure of signal *6*,
(b3′-1) the driver at train *Y* fails to detect the red signal AND the detection failure of the ATS,
(b3′-2) the driver at train *Y* fails to detect the red signal AND the execution failure of the ATS,

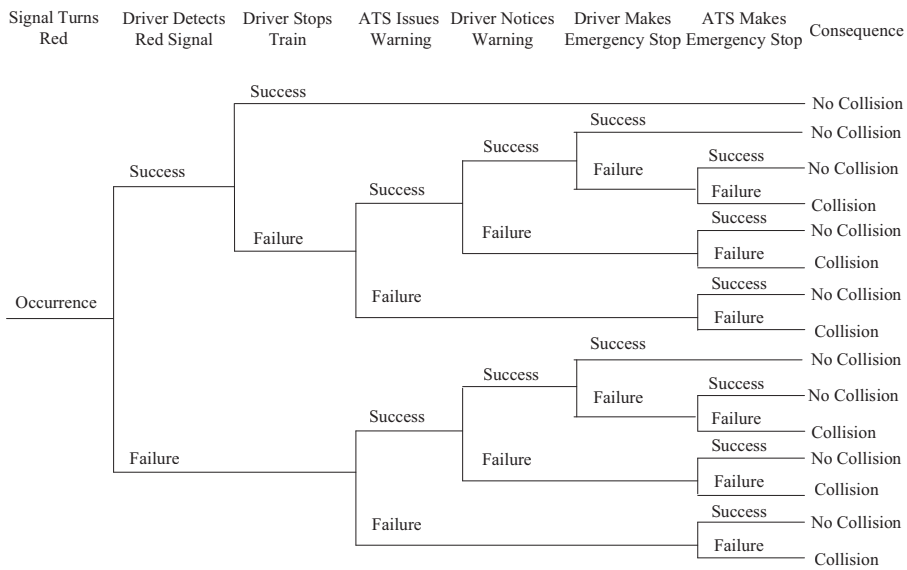


Figure 42.10. Event sequences for safety control system with ATS

(b4′) the driver at train *Y* fails to stop his train AND the execution failure of the ATS, and
(b5′) the braking system at train *Y* fails to stop train *Y*.

Compared with the previous failure conditions, the contribution of human errors in stopping the train according to the signal can be reduced by the addition of ATSs, because failure conditions of ATSs are required for the system accident to occur. Thus, a consideration from the viewpoint of safety control functions can clarify the effect of additional safety measures or devices on the safety control system.

42.4 Conclusions

This chapter considers the application of the concept of system control for safety to accident analysis. The first part of this chapter presents a system accident cause analysis based on the concept of system control for safety. By investigating the causes of malfunctions systematically according to the system hierarchical control structure, from the operating process where a system accident occurs to the top level such as management department of a company, background factors of a proximal accident cause can be identified as dysfunction of control loops at upper levels. Additional studies are being planned to improve and extend the proposed method by applying it to more practical problems such as the development of prevention measures against system accidents from the viewpoint of system control for safety.

The second part applies the concept of "safety control functions" to the derivation of accident occurrence conditions. As shown in the simple illustrative example of a collision accident, the decomposition of a safety control function into detection, diagnosis and execution can simplify not only the identification of safety control functions related to a disturbance or initiating event, but also the derivation of their failure conditions, including hardware and human actions. Safety devices and safety actions by human operators can be organized into a safety control system, which can perform a safety control function as a whole in the accident sequence. To devise an effective countermeasure, the proposed method can consider not only the cognitive aspects of human actions in a safety control function, but also the role of each component in the overall system safety control function. Depending on the initial condition when a disturbance occurs, the event sequences can be easily modified by identifying available safety control systems. Though the qualitative analysis is discussed to derive system accident occurrence conditions, the quantitative analysis is the next step in this research. Time dependency must also be considered in the evaluation of error probability. Considering the operation process of safety control functions, on-demand failure probability [10] must be utilized to evaluate the failure probability of safety control systems.

References

[1] NASA, Probabilistic risk assessment procedure guide for nasa managers and practitioners. Ver. 1.1, NASA, 2002.
[2] Rasmussen J. Major accident prevention: What is the basic research issue? Proc. 1998 ESREL Safety and Reliability Conference, 1998; 739–40.
[3] Leveson N. A new accident model for engineering safer systems. Safety Science 2004; 42:237–70.
[4] Kohda T, Takagi Y. Accident cause analysis of complex systems based on safety control functions. Proc. Annual Reliability and Maintainability Symposium, Newport Beach, CA, January 2006.
[5] Kohda T, Adachi G. Accident cause analysis based on system control function. Proc. Safety Engineering Symposium (in Japanese) 2006; 115–8.
[6] Kohda T, Fujihara H. Accident occurrence conditions in railway systems. International Journal of Performability Engineering, Part II 2007; 3(1):105–16. http://www.ijpe-online.com/ html/ past_issues.html .
[7] Ashby WR. An introduction to cybernetics. Chapman and Hall, London 1956.
[8] ESA, ARIANE 5 Failure—Full Report, 1996. http://www.esrin.esa.it/htdocs/tidc/Press/Press96/ ariane5rep.html .
[9] Japan Society for Safety Engineering, Accidents and Disasters: Cases and Their Measures—Prescription for Prevention of Similar Accidents. Yokendo, (in Japanese), 2005; 93–9.

[10] Kohda T, Nakagawa M. Accident sequence evaluation of complex systems with multiple independent protective systems. Proc. Annual Reliability and Maintainability Symposium, Alexandria, VA, Jan. 24–27, 2005.
[11] AIChE CCPS, Layer of protection analysis, simplified process risk assessment, AIChE, 2001.
[12] INSAG, Defence in depth in nuclear safety. INSAG-10, IAEA, 1996.
[13] Henley EJ, Kumamoto H. Probabilistic risk assessment, reliability engineering, design and analysis. IEEE Press, New York, 1991.
[14] NASA, Fault tree handbook with aerospace applications, Ver. 1.1. NASA Publication, 2002.
[15] Vincent K.J. The human factor: Revolutionizing the way people live with technology. Routledge, New York, 2003.
[16] Railway Electrical Engineering Association of Japan, Block Devices (revised edition) (in Japanese). 2004; 66–81.
[17] Railway Electrical Engineering Association of Japan, ATS&ATC (in Japanese), 1993; 6–22.

43

Probabilistic Risk Assessment

Mohammad Modarres

Reliability Engineering Program, A.J. Clark School of Engineering, University of Maryland, College Park, Maryland, 20742, USA

Abstract: In this chapter, the key elements of the basic methodology of probabilistic risk assessment (PRA) are presented. Starting with the enumeration of some of the strengths of PRA, the detailed steps involved in a PRA will be discussed and subsequently a case study shall be provided to highlight the various steps involved.

43.1 Introduction

Probabilistic risk assessment (PRA) is a systematic procedure for investigating how complex systems are built and operated. PRA models how human, software and hardware elements of the system interact with each other. Also, it assesses the most significant contributors to the risks of the system, and determining the value of the risk. PRA involves estimation of the degree or probability of loss. A formal definition proposed by Kaplan and Garrick [1] provides a simple and useful description of the elements of risk assessment that involves addressing three basic questions:

1. What can go wrong that could lead to exposure of hazards?
2. How likely is this to happen?
3. If it happens, what consequences are expected?

The PRA procedure involves quantitative application of the above triplets in which probabilities (or frequencies) of scenarios of events leading to exposure of hazards are estimated, and the corresponding magnitude of health, safety, environmental and economic consequences for each scenario are predicted. The risk value (*i.e.*, expected loss) of each scenario is often measured as the product of the scenario frequency and its consequences. The main result of the PRA is not the actual value of the risk computed (the so-called bottom-line number); rather it is the determination of the system elements that substantially contribute to the risks of that system, uncertainties associated with such estimates, and effectiveness of various risk reduction strategies available. That is, the primary value of a PRA is to highlight the system design and operational deficiencies and optimize resources that can be invested on improving the design and operation of the system.

43.1.1 Strength of PRA

The most important strengths of PRA as the formal engineering approach to risk assessment are:

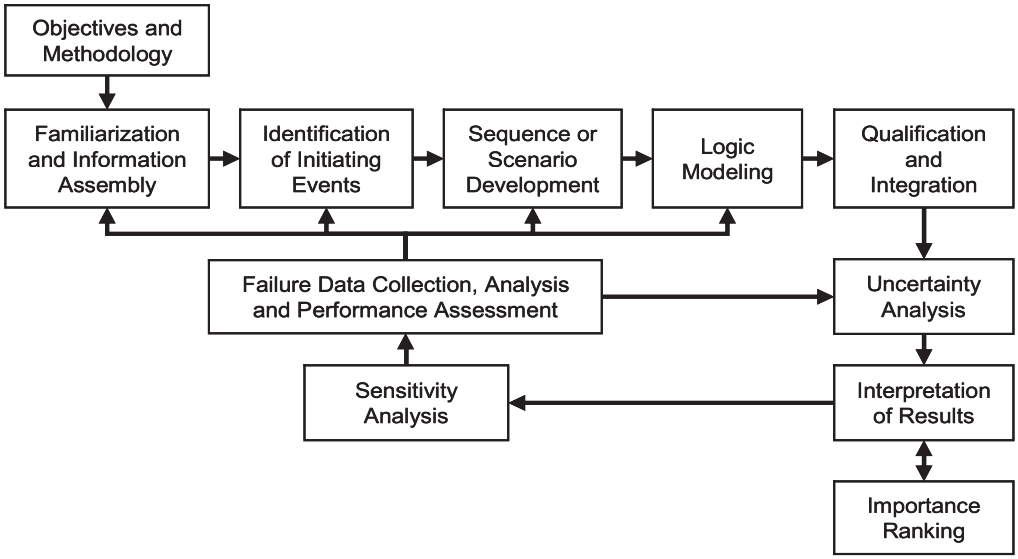


Figure 43.1. Components of the overall PRA process [2]

- PRA provides an integrated and systematic examination of a broad set of design and operational features of an engineered system,
- PRA incorporates the influence of system interactions and human-system interfaces,
- PRA provides a model for incorporating operating experience with the engineered system and updating risk estimates,
- PRA provides a process for the explicit consideration of uncertainties,
- PRA permits the analysis of competing risks (*e.g.*, of one system *vs.* another or of possible modifications to an existing system),
- PRA permits the analysis of (assumptions, data) issues via sensitivity studies,
- PRA provides a measure of the absolute or relative importance of systems, components to the calculated risk value, and
- PRA provides a quantitative measure of overall level of health and safety for the engineered system.

Major errors may results from weak or absent models, or associated data of potentially important factors in the risk of the system, including cases where

- initiating events with very low frequencies of occurrence,
- human performance models and interactions with the system are highly uncertain, and
- failures occurring from a common cause failure such as an extreme operating environment are difficult to identity and model.

43.2 Steps in Conducting a Probabilistic Risk Assessment

The following subsections provide a discussion of essential components of PRA as well as the steps that must be performed in a PRA analysis.

The NASA PRA Guide [2] describes the components of the PRA as shown in Figure 43.1. Each component of PRA will be discussed in more in the following.

43.2.1 Objectives and Methodology

Preparing for a PRA begins with a review of the objectives of the analysis. Among many objectives that are possible, the most common ones include design improvement, risk acceptability, decision support, regulatory and oversight support, and operations and life management. Once the objectives are clarified, an inventory of possible techniques for the desired analyses should be developed. The available techniques range from required computer codes to system experts and analytical experts. This, in essence, provides a road map for the analysis. The resources required for each analytical method should be evaluated, and the most effective option selected. The basis for the selection should be documented, and the selection process reviewed to ensure that the objectives of the analysis will be adequately met. See Hurtado [3] and Kumamoto and Henley [4] for the inventory of methodological approaches to PRA.

43.2.2 Familiarization and Information Assembly

A general knowledge of the physical layout of the overall system (*e.g.*, facility, design, process, aircraft or spacecraft), administrative controls, maintenance and test procedures, as well as barriers and subsystems, whose job is to protect, prevent or mitigate hazard exposure conditions, is necessary to begin the PRA. All subsystems, structures, locations, and activities expected to play a role in the initiation, propagation, or arrest of a hazard exposure condition must be understood in sufficient details to construct the models necessary to capture all possible scenarios. A detailed inspection of the overall system must be performed in the areas expected to be of interest and importance to the analysis. The following items should be performed in this step:

1. Major critical barriers, structures, emergency safety systems, and human interventions should be identified.
2. Physical interactions among all major subsystems (or parts of the system) should be identified and explicitly described. The result should be summarized in a dependency matrix.
3. Past major failures and abnormal events that have been observed in the facility should be noted and studied. Such inform ation would help ensure inclusion of important applicable scenarios.
4. Consistent documentation is critical to ensure the quality of the PRA. Therefore, a good filing system must be created at the outset, and maintained throughout the study.

With the help of the designers, operators, and owners, the analysts should determine the ground rules for the analysis, the scope of the analysis, and the configuration and phases of the operation of the overall system to be analyzed. One should also determine the faults and conditions to be included or excluded, the operating modes of concern and the hardware configuration on the design freeze date (*i.e.*, the date after which no additional changes in the overall system design and configuration will be modeled). Therefore, the results of the PRA are only applicable to the overall system at the freeze date.

43.2.3 Identification of Initiating Events

This task involves identifying those events (abnormal events or conditions) that could, if not correctly and timely responded to, result in hazard exposure. The first step involves identifying sources of hazard and barriers around these hazards. The next step involves identifying events that can lead to a direct threat to the integrity of the barriers.

A system may have one or more operational modes which produce its output. In each operational mode, specific functions are performed. Each function is directly realized by one or more systems by making certain actions and behaviors. These systems, in turn, are composed of more basic units (*e.g.*, subsystems, components, hardware) that accomplish the objective of the system. As long as a system is operating within its design parameter tolerances, there is little chance of challenging the system boundaries in such a way that hazards will escape those boundaries. These

operational modes are called normal operation modes.

During normal operation mode loss of certain functions or systems will cause the process to enter an off-normal (transient) state transition. Once in this transition, there are two possibilities. First, the state of the system could be such that no other function is required to maintain the process in a safe condition (safe refers to a mode where the chance of exposing hazards beyond the system boundaries is negligible.) The second possibility is a state wherein other functions (and thus systems) are required to prevent exposing hazards beyond the system boundaries. For this second possibility, the loss of the function or the system is considered an initiating event. Since such an event is related to the normally operating equipment, it is called an operational initiating event.

Operational initiating events can also apply to various modes of the system (if it exists). The terminology remains the same since, for each mode, certain equipment, people or software must be functioning. For example, an operational initiating event found during the PRA of a test nuclear reactor was low primary coolant system flow. Flow is required to transfer heat produced in the reactor to heat exchanges and ultimately to the cooling towers and the outside environment. If this coolant flow function is reduced to the point where an insufficient amount of heat is transferred, core damage could result (thus the possibility of exposing radioactive materials—the main source of hazard in this case). Therefore, another system must operate to remove the heat produced by the reactor (*i.e.*, a protective barrier). By definition, then, low primary coolant system flow is an operational initiating event.

One method for determining the operational initiating events begins with first drawing a functional block diagram of the system. From the functional block diagram, a hierarchical relationship is produced with the process objective being successful completion of the desired system. Each function can then be decomposed into its subsystems and components, and can be combined in a logical manner to represent operations needed for the success of that function.

Potential initiating events are events that result in failures of particular functions, subsystems, or components, the occurrence of which causes the overall system to fail. These potential initiating events are "grouped" such that members of a group require similar subsystem responses to cope with the initiating event. These groupings are the operational initiator categories.

An alternative to the use of functional hierarchy for identifying initiating events is the use of failure mode and event analysis (FMEA). (See Stamatis [5]) The difference between these two methods is noticeable; namely, the functional hierarchies are deductively and systematically constructed, whereas FMEA is an inductive and experiential technique. The use of FMEA for identifying initiating events consists of identifying failure events (modes of failures of equipment, software and human) whose effect is a threat to the integrity and availability of the hazard barriers of the system. In both of the above methods, one can always supplement the set of initiating events with generic initiating events (if known). For example, see Sattison, *et al*. [6] for these initiating events for nuclear reactors, and the NASA Guide [2] for space vehicles.

To simplify the process, after identifying all initiating events, it is necessary to combine those initiating events that pose the same threat to hazard barriers and require the same mitigating functions of the process to prevent hazard exposure.

The following inductive procedures should be followed when grouping initiating events:

1. Combine the initiating events that directly break all hazard barriers.
2. Combine the initiating events that break the same hazard barriers (not necessarily all the barriers).
3. Combine the initiating events that require the same group of mitigating human or automatic actions following their occurrence.
4. Combine the initiating events that simultaneously disable the normal operation as well as some of the available mitigating human, software or automatic actions.

Events that cause off-normal operation of the overall system and require other systems to operate so as to maintain hazards within their desired boundaries, but are not directly related to a hazard mitigation, protection or prevention function, are non-operational initiating events. Non-operational initiating events are identified with the same methods used to identify operational events. One class of such events of interest is those that are primarily external to the overall system or facility. These so called "external events" will be discussed later in more detail in this article. The following procedures should be followed in this step of the PRA:

- Select a method for identifying specific operational and non-operational initiating events. Two representative methods are functional hierarchy and FMEA. If a generic list of initiating events is available, it can be used as a supplement.
- Using the method selected, identify a set of initiating events.
- Group the initiating events having the same effect on the system, for example those requiring the same mitigating functions to prevent hazard exposure are grouped together.

43.2.4 Sequence or Scenario Development

The goal of scenario development is to derive a complete set of scenarios that encompasses all of the potential exposure propagation paths that can lead to loss of containment or confinement of the hazards following the occurrence of an initiating event. To describe the cause and effect relationship between initiating events and subsequent event progression, it is necessary to identify those functions (*e.g.*, safety functions) that must be maintained to prevent loss of hazard barriers. The scenarios that describe the functional response of the process to the initiating events are frequently displayed by event trees. The event tree development techniques are discussed in [2] and [4].

Event trees order and depict (in an approximately chronological manner) the success or failure of key mitigating actions (*e.g.*, human actions or mitigative hardware actions) that are required to act in response to an initiating event. In PRA, two types of event trees can be developed: functional and systemic. The functional event tree uses mitigating functions as its heading. The main purpose of the functional tree is to better understand the scenario of events at an abstract level, following the occurrence of an initiating event. The functional tree also guides the PRA analyst in the development of a more detailed systemic event tree. The systemic event tree reflects the scenarios of specific events (specific human actions, protective or mitigative subsystem operations or failures) that lead to a hazard exposure. That is, the functional event tree can be further decomposed to show failure of specific hardware, software or human actions that perform the functions described in the functional event tree. Therefore, a systemic event tree fully delineates the overall system response to an initiating event and serves as the main tool for further analyses in the PRA. For a detailed discussion on specific tools and techniques used for this purpose see Modarres [7].

There are two kinds of external events. First kind refers to events that originate from within the facility or the overall system (but outside of the physical boundary of the facility), which are called internal events external to the process of the system. Events that adversely affect the facility or overall system and occur external to its physical boundaries, but can still be considered as part of the system, are defined as internal events external to the system. Typical internal events external to the system are internal conditions such as fires from fuel stored within a facility or floods occurred due to rupture of tank which is part of the overall system. The effects of these events should be modeled with event trees to show all possible scenarios.

The second kind of external events are those that originate outside of the overall system, and are called external events. Examples of external events are fires and floods that originate from outside of the system. Examples include seismic events, extreme heat, extreme drought, transportation events, volcanic events, high-wind events, terrorism, and sabotage. Again, this classification

can be used in developing and grouping the event tree scenarios.

The following procedures should be followed in this step of the PRA:

- Identify the mitigating functions for each initiating event (or group of events).
- Identify the corresponding human actions, systems or hardware operations associated with each function, along with their necessary conditions for success.
- Develop a functional event tree for each initiating event (or group of events).
- Develop a systemic event tree for each initiating event, delineating the success conditions, initiating event progression phenomena, and end effect of each scenario.

For specific examples of scenario development see [2]–[4].

43.2.5 Logic Modeling

Event trees commonly involve branch points at which a given subsystem (or event) either works (or happens) or does not work (or does not happen). Sometimes, failure of these subsystems (or events) is rare and there may not be an adequate record of observed failure events to provide a historical basis for estimating frequency of their failure. In such cases, other logic-based analysis methods such as fault trees or master logic diagrams may be used, depending on the accuracy desired. The most common method used in PRA to calculate the probability of subsystem failure is fault tree analysis. This analysis involves developing a logic model in which the subsystem is broken down into its basic components or segments for which adequate data exist. For more details on how a fault tree can be developed to represent the event headings of an event tree, see Modarres *et al*. [8].

Different event tree modeling approaches imply variations in the complexity of the logic models that may be required. If only main functions or systems are included as event-tree headings, the fault trees become more complex and must accommodate all dependencies among the main and support functions (or subsystems) within the fault tree. If support functions (or systems) are explicitly included as event tree headings, more complex event trees and less complex fault trees will result. For more discussions on methods and techniques used for logic modeling see Modarres [7].

The following procedures should be followed as a part of developing the fault tree:

1. Develop a fault tree for each event in the event tree heading for which actual historical failure data does not exist.
2. Explicitly model dependencies of a subsystem on other subsystems and inter-component dependencies (*e.g.*, common cause failures). For common cause failures, see Mosleh *et al*. [9].
3. Include all potential reasonable and probabilistically quantifiable causes of failure, such as hardware, software, test and maintenance, and human errors, in the fault tree.

The following steps should be followed in the dependent failure analysis:

1. Identify the hardware, software and human elements that are similar and could cause dependent or common cause failures. For example, similar pumps, motor-operated valves, air-operated valves, human actions, software routine, diesel generators, and batteries are major components in process plants, and are considered important sources of common cause failures.
2. Items that are potentially susceptible to common cause failure should be explicitly incorporated into the corresponding fault trees and event trees of the PRA where applicable.
3. Functional dependencies should be identified and explicitly modeled in the fault trees and event trees.

43.2.6 Failure Data Collection, Analysis and Performance Assessment

A critical building block in assessing the reliability and availability of complex systems is the data on

the performance of its barriers to contain hazards. In particular, the best resources for predicting future availability are past field experiences and tests. Hardware, software and human reliability data are inputs to assess performance of hazard barriers, and the validity of the results depends highly on the quality of the input information. It must be recognized, however, that historical data have predictive value only to the extent that the conditions under which the data were generated remain applicable. Collection of the various failure data consists fundamentally of the following steps: collecting generic data, assessing generic data, statistically evaluating facility-specific or overall system-specific data, and developing failure probability distributions using test and/or facility-specific and system-specific data. Three types of events identified during the risk scenario definition and system modeling must be quantified for the event trees and fault trees to estimate the frequency of occurrence of sequences: initiating events, component failures, and human error.

The quantification of initiating events and hazard barriers and components failure probabilities involves two separate activities. First, the probabilistic failure model for each barrier or component failure event must be established; then the parameters of the model must be estimated. Typically the necessary data include time of failures, repair times, test frequencies, test downtimes, common-cause failure events. Further uncertainties associated with such data must also be characterized. Kapur and Lamberson [10], Modarres [8], and Nelson [11] discuss available methods for analyzing data to obtain the probability of failure or the probability of occurrence of equipment failure. Also, Crow [12], and Ascher and Feingold [13] discuss analysis of data relevant to repairable systems. Finally, Mosleh *et al*. [9] discusses analysis of data for dependent failures, Poucet [14] reviews human reliability issues, and Smidts [15] examines software reliability models. Establishment of the data base to be used will generally involve collection of some facility-specific or system-specific data combined with the use of generic performance data when specific data are absent or sparse. For example, References [16]–[18] describe generic data for electrical, electronic, and mechanical equipment.

To attain the very low levels of risk, the systems and hardware that comprise the barriers to hazard exposure must have very high levels of performance. This high performance is typically achieved through the use of well-designed systems with adequate margin of safety considering uncertainties, redundancy and/or diversity in hardware, which provides multiple success paths. The problem then becomes one of ensuring the independence of the paths, since there is always some degree of coupling between agents of failures such as those activated by failure mechanisms, either through the operating environment (events external to the system) or through functional and spatial dependencies. Treatment of dependencies should be carefully included in both event tree and fault tree development in the PRA. As the reliability of individual subsystems increases due to redundancy, the contribution from dependent failures becomes more important; in certain cases, dependent failures may dominate the value of overall reliability. Including the effects of dependent failures in the reliability models used in the PRA is a difficult process and requires some sophisticated, fully integrated models be developed and used to account for unique failure combinations that lead to failure of subsystems and ultimately exposure of hazards. The treatment of dependent failures is not a single step performed during the PRA; it must be considered throughout the analysis (*e.g.*, in event trees, fault trees, and human reliability analyses).

The following procedures should be followed as part of the data analysis task:

1. Determine generic values of material strength or endurance, load or damage agents, failure times, failure occurrence rate and failures on demand for each item (hardware, human action, or software) identified in the PRA models. This can be obtained either from facility-specific or system-specific experiences, from generic sources of data, or both.
2. Gather data on hazard barrier tests, repair, and maintenance data primarily from

experience, if available. Otherwise use generic performance data.
3. Assess the frequency of initiating events and other probability of failure events from experience, expert judgment, or generic sources.
4. Determine the dependent or common cause failure probability for similar items, primarily from generic values. However, when significant specific data are available, they should be primarily used.

43.2.7 Quantification and Integration

Fault trees and event trees are integrated and their events are quantified to determine the frequencies of scenarios and associated uncertainties in the calculation of the final risk values. This integration depends somewhat on the manner in which system dependencies have been handled. We will describe the more complex situation, in which the fault trees are dependent, *i.e.*, there are physical dependencies (*e.g.*, through support units of the main hazard barriers such as those providing motive, proper working environment and control functions).

Normally, the quantification will use a Boolean reduction process to arrive at a Boolean representation for each scenario. Starting with fault tree models for the various systems or event headings in the event trees, and using probabilistic estimates for each of the events modeled in the event trees and fault trees, the probability of each event tree heading (often representing failure of a hazard barrier) is calculated (if the heading is independent of other headings). The fault trees for the main subsystems, support units (*e.g.*, lubricating and cooling units, power units) are merged where needed, and the equivalent Boolean expression representing each event in the event tree model is calculated. The Boolean expressions are reduced to arrive at the smallest combination of basic failures events (the so-called minimal cut-sets) that lead to exposure of the hazards. These minimal cut sets for each of the main subsystems (barriers)—that are often identified as headings on the event trees—are also obtained. The minimal cut sets for the event tree event headings are then appropriately combined to determine the cut sets for the event-tree scenarios. If possible, all minimal cut sets must be generated and retained during this process; unfortunately in complex systems and facilities this leads to an unmanageably large collection of terms and a combinatorial outburst. Therefore, the collection of cut sets are often truncated (*i.e.*, probabilistically small and insignificant cut sets are discarded based on the number of terms in a cut set or on the probability of the cut set.). This is usually a practical necessity because of the overwhelming number of cut sets that can result from the combination of a large number of failures, even though the probability of any of these combinations may be vanishingly small. The truncation process does not disturb the effort to determine the dominant scenarios since we are discarding scenarios that are extremely unlikely.

Even though the individual cut sets discarded may be several orders of magnitude less probable than the average of those retained, the large number of them discarded may sum to a significant part of the risk. The actual risk might thus be larger than what the PRA results indicate. This can be discussed as part of the modeling uncertainty characterization. Detailed examination of a few PRA studies of very complex systems, for example nuclear power plants shows that cut set truncation will not introduce any significant error in the total risk assessment results (see Dezfuli and Modarres [19]).

Other methods for evaluating scenarios also exist that directly estimate the frequency of scenario without specifying cut sets. This is often done in highly dynamic systems whose configuration changes as a function of time leading to dynamic event tree and fault trees. For more discussion on these systems see Chang, Mosleh and Dang [20], NASA Procedures PRA Guide [2], Dugan *et al.* [21]. Employing advanced computer programming concepts, one may directly simulate the operation of parts to mimic the real system for reliability and risk analysis (see Azarkhail and Modarres [22].) The following procedures should be followed as part of the quantification and integration step in the PRA:

1. Merge corresponding fault trees associated with each failure or success event modeled in the event tree scenarios (*i.e.*, combine them in a Boolean form). Develop a reduced Boolean function for each scenario (*i.e.*, truncated minimal cut sets).
2. Calculate the total frequency of each sequence, using the frequency of initiating events, the probability of barrier failure including contributions from test and maintenance frequency (outage), common cause failure probability, and human error probability.
3. Use the minimal cut sets of each sequence for the quantification process. If needed, simplify the process by truncating based on the cut sets or probability.
4. Calculate the total frequency of each scenario.
5. Calculate the total frequency of all scenarios of all event trees.

43.2.8 Uncertainty Analysis

Uncertainties are part of any assessment, modeling, and estimation. In engineering calculations we routinely ignore the estimation of uncertainties associated with failure models and parameters, because the uncertainties are very small and more often analyses are done conservatively (*e.g.,* by using high safety factor, design margin). Since PRAs are primarily used for decision making and management of risk, it is critical to incorporate uncertainties in all facets of the PRA.

Also, risk management decisions that consider PRA results must consider estimated uncertainties. In PRAs uncertainties are primarily shown in form of probability distributions. For example, the probability of failure of a subsystem (*e.g.*, a hazard barrier) may be represented by a probability distribution showing the range and likelihood of risk values.

The process involves characterization of the uncertainties associated with frequency of initiating events, probability of failure of subsystems (or barriers), probability of all event tree headings, strength or endurance of barriers, applied load or incurred damage by the barriers, amount of hazard exposures, consequences of exposures to hazards, and sustained total amount of losses. Other sources of uncertainties are in the models used. For example, the fault tree and event tree models, stress-strength and damage-endurance models used to estimate failure or capability of some barriers, probabilistic failure models of hardware, software and human, correlation between amount of hazard exposure and the consequence, exposure models and pathways, and models to treat inter- and intra-barrier failure dependencies. Another important source of uncertainty is incompleteness of the risk models and other failure models used in the PRAs. For example, the level of detail used in decomposing subsystems using fault tree models, scope of the PRA, and lack of consideration of certain scenarios in the event tree just because they are not known or experienced before.

Once uncertainties associated with hazard barriers have been estimated and assigned to models and parameters, they must be "propagated" through the PRA model to find the uncertainties associated with the results of the PRA, primarily with the bottom-line risk calculations, and with the list of risk significant elements of the system. Propagation is done using one of several techniques, but the most popular method used is Monte Carlo simulation. The results are then shown and plotted in form of probability distributions. Steps in uncertainty analysis include:

1. Identify models and parameters that are uncertain and the method of uncertainty estimation to be used for each.
2. Describe the scope of the PRA and significance and contribution of elements that are not modeled or considered.
3. Estimate and assign probability distributions depicting model and parameter uncertainties in the PRA.
4. Propagate uncertainties associated with the hazard barrier models and parameters to find the uncertainty associated with the risk value.
5. Present the uncertainties associated with risks and contributors to risk in an easy way to understand and visually straightforward to grasp.

43.2.9 Sensitivity Analysis

Sensitivity analysis is the method of determining the significance of choice of a model or its parameters, assumptions for including or not including a barrier, phenomena or hazard, performance of specific barriers, intensity of hazards, and significance of any highly uncertain input parameter or variable to the final risk value calculated. The process of sensitivity analysis is straightforward. The effects of the input variables and assumptions in the PRA are measured by modifying them by several folds, factors or even one or more order of magnitudes one at a time, and measure relative changes observed in the PRA's risk results. Those models, variables and assumptions whose change leads to the highest change in the final risk values are determined as "sensitive". In such a case, revised assumptions, models, additional failure data and more mechanisms of failure may be needed to reduce the uncertainties associated with sensitive elements of the PRA.

Sensitivity analysis helps focus resources and attentions to those elements of the PRA that need better attention and characterization. A good sensitivity analysis strengthens the quality and validity of the PRA results. Usually elements of the PRA that could exhibit multiple impacts on the final results, such as certain phenomena (*e.g.*, pitting corrosion, fatigue cracking and common cause failure) and uncertain assumptions are usually good candidates for sensitivity analysis. The steps involved in the sensitivity analysis are:

1. Identify the elements of the PRA (including assumptions, failure probabilities, models and parameters) that analysts believe might be sensitive to the final risk results.
2. Change the contribution or value of each sensitive item in either direction by several factors in the range of 2–100. Note that certain changes in the assumptions may require multiple changes of the input variables. For example, a change in failure rate of similar equipment requires changing of the failure rates of all this equipment in the PRA model.
3. Calculate the impact of the changes in step 2 one-at-a-time and list the elements that are most sensitive.
4. Based on the results in step 3 propose additional data, any changes in the assumptions, use of alternative models, and modification of the scope of the PRA analysis.

43.2.10 Risk Ranking and Importance Analysis

Ranking the elements of the system with respect to their risk or safety significance is one of the most important outcomes of a PRA. Ranking is simply arranging the elements of the system based on their increasing or decreasing contribution to the final risk values. Importance measures rank hazard barrier, subsystems or more basic elements of them usually based on their contribution to the total risk of the system. The ranking process should be done with much care. In particular, during the interpretation of the results, since formal importance measures are context dependent and their meaning varies depending on the intended application of the risk results, the choice of the ranking method is important.

There are several unique importance measures in PRAs. For example, Fussell–Vesely [23], Risk Reduction Worth (RRW), and Risk Achievement Worth (RAW) [8] are identified as appropriate measures for use in PRAs, and all are representative of the level of contribution of various elements of the system as modeled in the PRA and enter in the calculation of the total risk of the system. For example, the Birnbaum importance measure [24] represents changes in total risk of the system as a function of changes in the basic event probability of one component at a time. If simultaneous changes in the basic event probabilities are being considered, a more complex representation would be needed.

Importance measures can be classified based on their mathematical definitions. Some measures have fractional type definitions and show changes (in the number of folds or factors) in system total risk under certain conditions with respect to the normal operating or use condition (*e.g.*, as is the case in risk reduction worth and risk achievement

worth measures). Some measures calculate the changes in system total risk as failure probability of hazard barriers and other elements of the system or conditions under which the system operates change. This difference can be normalized with respect to the total risk of the system or even expressed in a percentage change form. There are other types of measures, which account for the rate of changes in the system risk with respect to changes in the failure probability of the elements of the system. These measures can be interpreted mathematically as partial derivative of the risk as a function of failure probability of its elements (barriers, components, human actions, phenomena, *etc*.). For example, the Birnbaum measure falls under this category.

Another important set of importance measures focus on ranking the elements of the system with the most contribution to the total uncertainty of the risk results obtained from PRAs. This process is called "uncertainty ranking" and is different than component, subsystem, and barrier ranking. In this importance ranking, the analyst is only interested in knowing which of the system elements drive the final risk uncertainties, so that resources can be focused on reducing important uncertainties.

There is another classification for importance measures in which they can be divided into two major categories of absolute *vs.* relative. Absolute measures are representative of fixed importance of one element of the system, independent of the importance of other elements, while relative importance expresses significance of one element with respect to weight of importance of other elements. Absolute importance can be used to estimate the impact of component performance on the system regardless of how important other elements are, while relative importance estimates the significance of the risk-impact of the component in comparison to the effect or contribution of others.

Absolute measures are useful when we speculate on improving actions, since they directly show the impact on the total risk of the system. Relative measures are preferred when resources or actions to improve or prevent failures are taken in a global and distributed manner. For additional discussions on the risk ranking methods and their implications in failure and success domains see Azarkhail and Modarres [25]. Applications of importance measures may be categorized into the following areas:

1. (Re)Design: To support decisions of the system design or redesign by adding or removing elements (barriers, subsystems, human interactions, *etc*.)
2. Test and maintenance: To address questions related to the plant performance by changing the test and maintenance strategy for a given design.
3. Configuration and control: To measure the significance or the effect of failure of a component on risk or safety or temporarily taking a component out of service.
4. Reduce uncertainties in the input variables of the PRAs.

The following are the major steps of importance ranking:

1. Determine the purpose of the ranking and select appropriate ranking importance measure that has consistent interpretation for the use of the ranked results.
2. Perform risk ranking and uncertainty ranking, as needed.
3. Identify the most critical and important elements of the system with respect to the total risk values and total uncertainty associated with the calculated risk values.

43.2.11 Interpretation of Results

When the risk values are calculated, they must be interpreted to determine whether any revisions are necessary to refine the results and the conclusions. There are two main elements involved in the interpretation process. The first is to understand whether or not the final values and details of the scenarios are logically and quantitatively meaningful. This step verifies the adequacy of the PRA model and the scope of analysis. The second is to characterize the role of each element of the system in the final results. This step highlights additional analyses data and information gathering that would be considered necessary.

The interpretation process heavily relies on the details of the analysis to see whether the scenarios are logically meaningful (for example, by examining the minimal cut sets of the scenarios), whether certain assumptions are significant and greatly control the risk results (using the sensitivity analysis results), and whether the absolute risk values are consistent with any historical data or expert opinion available. Based on the results of the interpretation, the details of the PRA logic, its assumptions and scope may be modified to update the results into more realistic and dependable values.

The ranking and sensitivity analysis results may also be used to identify areas where gathering more information and performing better analysis (for example, by using more accurate models) is warranted. The primary aim of the process is to reduce uncertainties in the risk results.

The interpretation step is a continuous process with receiving information from the quantification, sensitivity, uncertainty, and importance analysis activities of the PRA. The process continues until the final results can be best interpreted and used in the subsequent risk management steps.

The basic steps of the PRA results interpretation are:

1. Determine accuracy of the logic models and scenario structures, assumptions, and scope of the PRA.
2. Identify system elements for which better information would be needed to reduce uncertainties in failure probabilities and models used to calculate performance.
3. Revise the PRA and reinterpret the results until attaining stable and accurate results.

43.3 Compressed Natural Gas (CNG) Powered Buses: A PRA Case Study

43.3.1 Primary CNG Fire Hazards

The fire safety hazards that should be considered in assessing the risks of using CNG fuel are:

- Fire potential from fuel leakage.
- Explosion potential from uncontrolled dispersion and mixing of CNG in the presence of an ignition source.
- Impacts and missile generated hazards due to fuel being stored at high pressure.
- Chemical hazards (gas toxicity, asphyxiation potential and higher hydrocarbons in CNG maybe considered neurotoxin even though CNG is relatively non-toxic.)
- Electrostatic discharge.

The issues of bulk transport and storage are completely different from most of the other fuel types that are typically transported to fleet storage via tanker trucks. For use as a fuel, natural gas is compressed and stored in high-pressure cylinders (tanks) on the vehicle at 2,400–3,000 psig. The containment of natural gas at such high pressures requires very strong storage tanks that are both heavy and costly. Furthermore, such tanks are subject to corrosion-fatigue, sustained load cracking, stress corrosion and fatigue failure. This distinguishing feature of CNG has the most impact on safety issues. Some important fire related incidents which include fatalities in CNG vehicles are summarized in [26].

There are two distinct categories of CNG fuel tank designs:

Metal tanks: These tanks are made of aluminum or 4130X steel. There have been some cases of fragmentation rupture in this type of cylinders. *Composite-wrapped:* These are tanks constructed with an aluminum/steel liner and E-glass wrap or carbon fiber insert with E-glass wrap. There have been several ruptures of this type of tank [27].

This PRA study only considers metal tank type.

43.3.2 The Probabilistic Risk Assessment Approach

The standard PRA approach may be applied. Fault tree and event tree modeling techniques [28] describe scenarios of events leading to fire and explosion fatalities. Frequency of occurrence of such scenarios was then quantified using the generic failure data for basic components gathered

from the process industry that experience similar components [29]. Engineering judgment and simple fire analysis methods were used to determine the likelihood of occurrence of particular fire scenarios. The main source of uncertainty is the data used in the risk model (parameter uncertainty). The uncertainty from the failure data was factored into the PRA results. Model uncertainty was not considered since the methods discussed in the literature are still evolving [30]. A universally acceptable methodology has yet to emerge. In the absence of such an approach, conservative modeling assumptions have been used in the PRA to minimize error due to model uncertainty.

Uncertainties due to failure and consequence data are propagated using a standard Monte Carlo simulation technique. The sensitivity of individual elements of the risk model (*e.g.* failure data and assumptions) was measured by varying them individually by many factors and determining the resulting change in fire fatality risk.

43.3.3 System Description

The typical CNG bus system shown in Figure 43.2 was considered for this risk study. It is comprised of the following major subsystems.

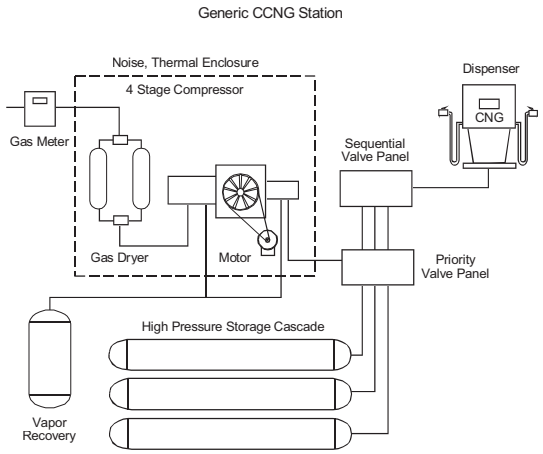


Figure 43.2. Components of a CNG station

43.3.3.1 Natural Gas Supply

Natural gas is supplied to the compressor station from a local distribution company through its pipeline system. Gas supply pressure in pipelines is typically around 25–60 psig.

43.3.3.2 The Compression and Storage Station

The compression and storage station provides CNG at different pressures to the dispenser, depending on the fueling procedure. The compression stations are designed with the flexibility to "fast fill" or regularly fill CNG bus tanks. Additionally refueling can take place directly from the compressor.

43.3.3.3 Storage Cascade

CNG is filtered after leaving the compressor and injected with methanol to reduce the moisture content. It is then sent through the priority and sequence valve panels to the low-pressure storage cascade bank, where it is stored at 1000 psig. Once the low-pressure storage bank is filled, medium (1500 psig) and high (3,600 psig) pressure banks are sequentially filled.

43.3.3.4 Dispensing Facility

The compressor and the storage tanks are connected to the dispenser through underground steel lines, which are subject to corrosion and the possibility of damage from excavation or earth movements. The dispensing equipment draws gas either from the storage cascades or from the compressor. A master shut-off valve isolates the compressor and storage cascades from the dispensing equipment for maintenance or emergency situations.

43.3.3.5 CNG Bus

The typical CNG Bus shown in Figure 43.3 is used in this study. This design is a 40 ft long bus which has six undercarriage CNG storage tanks. Only the parts of the bus relevant to the usage of CNG as a fuel and contributing to fire hazards are identified and used in this study.

The PRA develops fire scenarios and consequences due to occurrence of initiating events

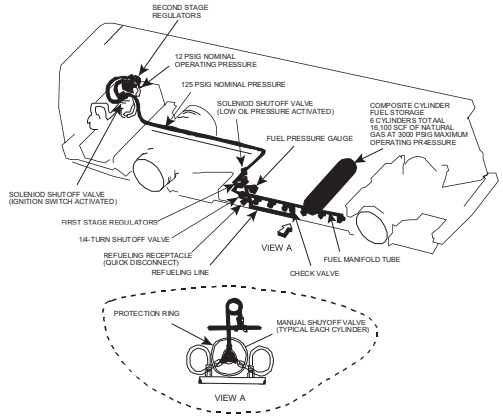


Figure 43.3. Fuel supply system of a CNG bus

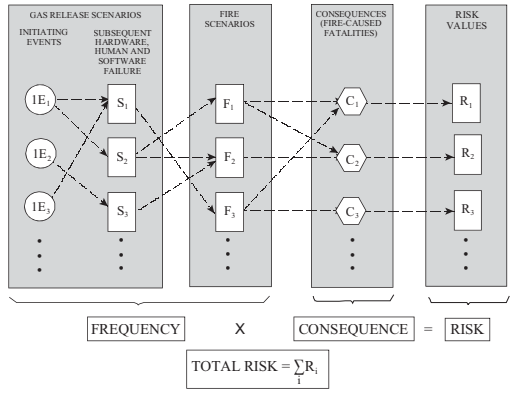


Figure 43.4. Summary of the overall PRA approach in this study

and subsequent hardware or human failures, identified as important in the qualitative risk analysis.

Generic and historical data obtained from various sources [29], [31] were used for quantifying the fault tree and event tree models, and were used to determine the frequency of occurrence of scenarios leading to fire-related fatalities. The risk was then computed from the frequency and consequence of each scenario. The steps are summarized in Figure 43.4.

43.3.4 Gas Release Scenarios

The failure modes may be grouped into six initiating event groups and subsequence hardware, human or software failures were identified to describe the scenarios of events leading to gas releases. Each scenario has an initiating event and subsequent failure events which can result in a fire or explosion with corresponding fatal consequences. The determination of the frequency of occurrence of each initiating event, the actual propagation of them into fires/explosions and consequences are part of the quantitative assessment. The classes of initiating events identified are:

1. Hardware catastrophic failures due to intrinsic failure mechanisms, leading to instantaneous release of CNG in the presence of an ignition source.
2. Hardware degraded failures resulting in gradual release, in the presence of an ignition source.
3. Hardware or human failures resulting in a CNG release with potential for electrostatic discharge ignition.
4. Accidental impact of hardware resulting in gas release in the presence of an ignition source.
5. Human error resulting in the release of CNG in the presence of an ignition source.
6. Non-CNG related fire (*e.g.*, fires due to oil or cargo burning) resulting in the release of CNG in the presence of an ignition source.

Fault Trees were used to identify and compute the probability of failure leading to a sustained gas release in the presence of an ignition source, given the occurrence of the initial failure events. A constant failure rate model was used to represent the events modeled in the fault trees. From the fault trees cut-sets were generated. Rare event approximation [29] was used to combine scenarios. Component failures were assumed independent and no common cause failure events were determined significant since very little redundancy in active components existed.

43.3.5 Fire Scenario Description

Factors that determine the kind of fire that results from gas release include:

- Type of initial gas release (leak *vs*. sudden release)
- Gas dispersion
- Gas ignition likelihood

43.3.5.1 Gas Release

The CNG release may be instantaneous or gradual. Adiabatic expansion of the gas occurs with an instantaneous release, for example from a ruptured gas tank cylinder. A gradual release occurs, as from a leaking joint or cracked fuel line. Component defects, with greater than 1/4" opening in the containment system, are determined to produce an instantaneous release of CNG. Conversely, a gradual release is produced by a crack or other defect with less than 1/4" opening.

Adiabatic expansion of CNG results in the formation of a flammable air/gas mixture with explosive potential. If the mixture is ignited immediately it results in a fireball [32]. The pressure and the volume of the CNG containment determine the extent of the fireball and explosion. Delayed ignition of the released gas results in continued mixing with a vapor cloud forming. Ignition would result in a vapor cloud explosion or flash fire. Gradual release of CNG results in a limited mixing of gas with air which, if ignited immediately, will result in a jet flame in the vicinity of the mixture. Delayed ignition leads to the accumulation of flammable air gas mixture which would produce a vapor cloud explosion or flash fire, if ignited.

43.3.5.2 Gas Dispersion

The extent of mixing of the released CNG that is not immediately ignited is best determined with computer models. In the absence of an elaborate model, the dispersion scenarios considered are dense cloud, and neutral or buoyant dispersion.

If there is an instantaneous release of CNG and the ignition is delayed, then the gas will be dispersed as a dense cloud, which will form a flash fire or would explode when ignition occurs. Gradual release of CNG in a jet, leads to buoyant dispersion and delayed ignition results in a flash fire. Following the dispersion of CNG in a dense cloud, even if delayed ignition does not occur, there are thermodynamic effects on the human body that present additional risks apart from fire or explosion hazards. This aspect of CNG dispersion is further discussed in [33].

43.3.5.3 Ignition Likelihood

If ignition can occur in less than 10 minutes of exposure then it can be considered immediate. Delayed ignition is generally considered to be greater than 10–15 minutes of exposure. Table 43.1 shows the reference values [26], [34] used for a qualitative judgment of the likelihood potential of ignition of a vapor cloud exposed to an ignition source.

Table 43.1. Qualitative ignition potential

Qualitative ranking	Quantitative likelihood range
Strong	0.25–1.00
Moderate	0.10–0.24
Weak	0.01–0.09

In this study immediate ignition of a flammable gas mixture (fireball and jet flame) is assumed to occur with a conditional probability of 0.8. Delayed ignition and dispersion (flash fire) is assumed to occur with a conditional probability of 0.95 [34]. Sensitivity of the risk results to these assumptions were assessed later in the study.

Table 43.2 summarizes the different gas release, ignition or dispersion and fire scenarios considered in this study.

Table 43.2. Summary of CNG release, ignition and fire scenario

CNG release mode	Ignition mode	Expected consequence
Instantaneous	Immediate	Fireball
	Delayed	Vapor cloud explosion or flash fire
Gradual	Immediate	Jet flame
	Delayed	Vapor cloud explosion or flash fire

43.3.6 Consequence Determination

An analytical assessment method was used to compute the number of fatalities due to the various

fire scenarios identified before. The method estimates the heat release rate and flame height, exposure temperature from fire plume modeling, and the time required to reach critical damage thresholds causing fatalities. The consequences for each event in this study are computed by assuming the following:

- Worst-case fire and explosive intensities associated with each scenario.
- Fatalities occurring when exposed to a fire heat flux of 25.0 kW/m^2 for one minute [26].

Fatalities occurring when persons are present within the distance from a point source where a radiant flux of 25.0 kW/m^2 or more is being received.

43.3.7 Fire Location

To determine the lethality of each fire event, location of the vehicle is of paramount importance. The five vehicle fire locations chosen represents normal usage. A probability factor, representing the relative frequency of a vehicle's location during normal use, is applied to the consequences. Number of people present at each location was different and was represented by distributions consistent from current experience ranging from 1–30 people exposed (no evacuation or other mitigation measures were allowed). This allows determination of the expected fatalities in each location given a fire scenario.

The locations and probability factors are based on the following assumptions:

- Garage or storage facility (0.5), (bus is parked 12 hours per day).
- Fueling station (0.06), (bus refueled maintained and repaired 1.5 hour /day).
- Urban roadway (0.21), (bus is in operation 5 hours on urban roadway).
- Rural roadway (0.21), (bus is in operation and near school, near homes and on rural roadway 5 hours).
- Tunnel, under bridges or other enclosed roadways (0.02), (bus goes through this type of roadways for 0.5 hour per day).

43.3.8 Risk Value Determination

Gas release and fire scenarios along with the consequences were combined for each initiating event to determine the risk associated with each event. The summation of each individual risk gave the total risk. Event Trees of the gas release and fire scenarios were used to combine the elements of the risk model. For this purpose, the software tool QRAS V1.6 [33] was used. This tool was used to calculate the sets of scenarios and corresponding risk values.

43.3.9 Summary of PRA Results

The PRA fire safety risk results of this study are summarized in Table 43.3. The mean total fire fatality risk for CNG buses is estimated as 0.23 per 100-million miles of operation. The study also estimates mean values of 0.16 fatalities per 100-million miles for passengers inside the CNG bus only. This would suggest that approximately 70% of the total fire related fatalities are expected to be due to the passengers of the bus.

43.3.10 Overall Risk Results

The projected mean fatalities from a typical bus due to catastrophic failures resulting in an uncontained fire are 2.7×10^{-6}/bus/year, and for all causes is 2.2×10^{-5}/bus/year. For the 8500 CNG school buses [35], [36]. in operation in the U.S. in year 2001, this would lead to a mean total risk value of approximately 0.19 deaths/year or a mean time to occurrence of 5.4 years/fatality for all existing buses in operation. If all the existing buses were to be replaced with CNG buses, then the projected fatality would be 9.9 deaths/year or a mean time to occurrence of 0.1 year/fatality.

It should be noted that some actual cases of CNG related explosions and fire from component failures have been recorded. One such incident was reported in Houston, Texas in 1998. In this case, gradual gas release and delayed ignition resulted in the explosion and a subsequent flash fire (no fatalities were reported). A CNG cylinder rupture as a result of accidental impact caused a fireball in Nassau County, NY [37] in 2001. Seven people

Table 43.3. PRA risk results

Scenarios groups leading to fire and fatality	Risk (mean fatalities/bus/year)	Risk (mean fatalities/ 100 M miles)	% of total risk
Catastrophic failure of bus or station hardware components	2.4×10^{-6}	2.5×10^{-2}	10.84
Degraded failure of bus or station hardware components	8.7×10^{-6}	9.0×10^{-2}	38.77
Electrostatic discharge of CNG	2.7×10^{-6}	2.8×10^{-2}	12.21
Accidental impacts mainly due to collision	4.9×10^{-6}	5.1×10^{-2}	21.70
Non-CNG related fires	3.4×10^{-6}	3.5×10^{-2}	14.94
Operator error	3.6×10^{-7}	3.7×10^{-3}	1.54
Total mean fire fatality risk	$\mathbf{2.2 \times 10^{-5}}$	$\mathbf{2.3 \times 10^{-1}}$	**100**

were killed in a CNG bus explosion/fire in Tajikistan and four in another accident in San Salvador [38] in 2001. As such, the evidences of some of the scenarios considered in this study have already been observed.

Analysis of the projected fatalities from all the initiating events has revealed that while the number of fatalities from CNG bus fires are low, or have not been reported to date in the U.S., this is only due to the small number of CNG buses in operation. Increasing the number of such buses will certainly increase the expected number of fatalities due to fires and explosions.

43.3.11 Uncertainty Analysis

The sources of uncertainty in the results of this study can be classified and characterized as follows:

- Generic bus system description and model used (model uncertainty)
- Major fire hazard scenarios considered (model/completeness uncertainty)
- Conservatism in fire scenario and consequence modeling techniques used (model/ assumption uncertainty)
- Failure data for hardware/human failures and estimated frequency of fires and their location (lack of sufficient data / parameter uncertainty)
- Integration of all scenarios to estimate total risk (model uncertainty).

While model uncertainties are important, due to lack of a sound model uncertainty estimation methodology, at this point only the source of uncertainty due to failure data used to quantify the PRA models are quantified. Uncertainties in the models themselves are not considered and as is the general practice in the PRA's, model uncertainties were reduced by independent peer reviews and conservatism in constructing the models. The uncertainty in failure data used in the PRA model was represented by probability distributions assigned to the component failure rate, probabilities for subsequent events and consequence of individual scenarios. Where appropriate, normal, lognormal and uniform distributions were used along with distribution parameters as suggested by the generic data sources and from engineering judgment to represent the uncertainties in failure data, parameters and assumptions.

Propagation and combination of the uncertainties in the risk analysis were performed using the QRAS V1.6, Risk Analysis software [39]. The

Table 43.4. Summary of uncertainty analysis results

CNG bus fire scenarios resulting from the following causes	Mean frequency of occurrence/bus/year	Mean risk (fatalities/bus/year)	5%	95%
Catastrophic failure of bus or station hardware components	1.4×10^{-3}	2.4×10^{-6}	2.7×10^{-7}	6.1×10^{-6}
Degraded failure of bus or station hardware components	3.7×10^{-3}	8.7×10^{-6}	5.6×10^{-7}	2.5×10^{-5}
Electrostatic discharge of CNG	1.4×10^{-5}	2.7×10^{-6}	4.1×10^{-7}	6.6×10^{-6}
Accidental impacts mainly due to collision	3.6×10^{-2}	4.9×10^{-6}	4.3×10^{-7}	1.2×10^{-5}
Non-CNG related fires	3.6×10^{-4}	3.4×10^{-6}	3.7×10^{-7}	8.5×10^{-6}
Operator error	4.0×10^{-2}	3.6×10^{-7}	2.4×10^{-8}	9.8×10^{-7}
Total fire fatality risk		**2.2×10^{-5}**	**9.1×10^{-6}**	**4.0×10^{-5}**

* Assuming 9598 miles of travel per bus per year [40]

propagation of the uncertainties relied on a Monte Carlo simulation with Latin hypercube sampling and regression analysis [40]. The results of the uncertainty analysis are summarized in Table 43.4. The mean value of the fire fatality risk computed is 2.2×10^{-5} fatalities/bus/year (see Table 43.4). The probability bounds at 5% and 95% levels are calculated as 9.1×10^{-6} and 4.0×10^{-5}, respectively.

43.3.12 Sensitivity and Importance Analysis

The sensitivity of the total risk to the input parameters was performed by changing the failure rates of important components by a factor of ten (10) and changing the outcomes of each fire by a factor of one half. Each change is done while the other parameters are kept constant. This approach allows identification of the components which contribute most to the uncertainty of the overall risk results. The sensitivity of the risk to the presence of certain ignition sources was performed by similarly varying the probability of occurrence of each ignition source and comparing the effect on the total risk result.

Sensitivity analysis shows that the total fire fatality risk is relatively insensitive to ignition sources except to the introduction of an ignition source by an operator from such activities as smoking. This result is very important and should be included in any selection and training process for operators of CNG powered equipment.

Fatality risk is sensitive to location of the fire. This study shows that the risk is highly sensitive to flash fires in urban and rural areas. The third most important fire events are fireballs in urban areas. More detailed modeling of fire scenarios would be required so that critical adiabatic flame temperatures, flame speed and burning rates can be determined analytically.

Birnbaum Importance measures [28] were also used to identify design weaknesses and component failures that are critical to the prevention of CNG release and fires. It is a good measure for identifying components and design features that contribute most to risk. Such importance measures provide insights into how one should focus risk reduction and management efforts. The components with the highest potential for risk

reduction are the CNG cylinders, pressure relief devices and bus fuel piping.

43.3.13 Case Study Conclusions

While CNG buses are more susceptible to major fires, the total average expected fire risk from CNG buses over diesel power-buses is expected to be higher by only a factor of about two. However, since most of the fire fatalities are expected to occur among the passengers of CNG school buses, the fire risk for CNG bus passengers is expected to be larger than that of diesel school bus by over two orders of magnitude. While on the average the total CNG fire safety risk is not much higher than the diesel buses, the worst possible fire scenarios may impose a far higher fatality risk in CNG buses than the worst case fire scenario from diesel powered buses.

The reliance of this study on generic models and failure data is a good approximation to screen safety risks of CNG buses. However, a more accurate physics of failure based model (such as fatigue and corrosion based life models) should be supplemented with this study to provide more accurate results. This is part of on-going research by the authors. Further, CNG-specific hardware failure data would also be needed.

Three components have been identified from the sensitivity and importance analysis to contribute most to fire fatality risk and to the uncertainty of the overall fire fatality risk. These are pressure relief valves on cylinders, CNG storage cylinders, and bus fuel piping. The failure mechanisms of these components should be modeled using a physics of failure based approach to analytically determine the failure rates.

To compare the results of CNG with diesel buses, the risk assessment should add risk of non-fatal injuries in addition to fatalities. For any policy decision making, the fire risk should be compensated for and properly characterized by integrating the safety risks of this study and the expected health and environmental benefits of using CNG powered school buses.

References

[1] Kaplan S, Garrick J. On the quantitative definition of risk, Risk Analysis 1981; 1 (1): 11–28.

[2] Stamatelatos M. *et al*., Probabilistic risk assessment procedures guide for NASA managers and practitioners, version 1.1, NASA, Washington DC, 2002.

[3] Hurtado JL, Jogler F, Modarres M. Generalized renewal process: Models, parameter estimation and applications to maintenance problems. International Journal of Performability Engineering 2005; 1(1): 37–50.

[4] Kumamoto H, Henley EJ. Probabilistic risk assessment for engineers and scientists. New York: IEEE Press, 1996.

[5] Stamatis DH. Failure mode and effect analysis: FMEA from theory to execution, 2nd edition. Wisconsin: ASQ Quality Press, 2003.

[6] Sattison MB. *et al.* Analysis of core damage frequency: Zion, unit 1 internal events. NUREG/CR-4550, 7, Rev. 1, 1990.

[7] Modarres M. Risk analysis in engineering, techniques, tools and trends. Boca Raton, FL: CRC Press, 2006.

[8] Modarres M., Kaminskiy M., Krivtsov V. Reliability engineering and risk analysis, a practical guide, New York: Marcel Dekker, 1999.

[9] Mosleh A., *et al*. Procedure for treating common cause failures in safety and reliability studies, U.S. Nuclear Regulatory Commission, NUREG/CR-4780, Washington, DC, 1988; I and II

[10] Kapur KC, Lamberson LR. Reliability in engineering design. New York: Wiley, 1977.

[11] Nelson W. Accelerated testing: statistical models, test plans and data analyses. New York: Wiley, 1990.

[12] Crow LH. Evaluating the reliability of repairable systems. Proc. Annual Reliability Maintainability Symposium, IEEE 1990.

[13] Ascher H, Feingold H. Repairable systems reliability: modeling and inference, misconception and their causes. New York: Marcel Dekker, 1984.

[14] Poucet A. Survey of methods used to assess human reliability in the human factors reliability benchmark exercise. Reliability Engineering and System Safety 1998; 22: 257–68.

[15] Smidts C. Software reliability. In: Whitaker JC, editor. The electronics handbook. Boca Raton, FL: CRC Press and IEEE Press, 1996.

[16] Guidelines for process equipment data. New York: Center for Chemical Process Safety, American Institute of Chemical Engineers 1989.

[17] Military handbook, reliability prediction of electronic equipment (MIL-HDBK-217F), Department of Defense, 1995.
[18] Guide to the collection and presentation of electrical, electronic, sensing component and mechanical equipment reliability data for nuclear power generating stations (IEEE Std.500), New York: IEEE Standards, 1984.
[19] Dezfuli H., Modarres M. A truncation methodology for evaluation of large fault trees. IEEE Transactions on Reliability 1984; R-33: 325–28.
[20] Chang YH, Mosleh A., Dang V. Dynamic probabilistic risk assessment: framework, tool, and application. Annual Meeting, Society for Risk Analysis, Baltimore, MD, Dec. 7–10, 2003.
[21] Dugan J, Bavuso S, Boyd M. Dynamic fault tree models for fault tolerant computer systems. IEEE Transactions on Reliability 1993; 40 (3): 363.
[22] Azarkhail M, Modarres M. An intelligent-agent-oriented approach to risk analysis of complex dynamic systems with applications in planetary missions. Proc. of the 8th International Conference on Probabilistic Safety Assessment and Management. ASME, New Orleans, USA 2006; May.
[23] Fussell J. How to hand calculate system reliability and safety characteristics. IEEE Transactions on Reliability 1975; R 24 (3).
[24] Birnbaum ZW. On the importance of different components in a multicomponent system. In: Krishnaiah PR, editor. Multivariate analysis II. New York: Academic Press, 1969.
[25] Azarkhail M., Modarres M. A study of implications of using importance measures in risk-informed decisions. PSAM-7, ESREL 04 Joint Conference, Berlin, Germany June 2004.
[26] Modarres M., Mowrer F, Chamberlain S. Compressed natural gas bus safety: a qualitative and quantitative risk assessment. CTRS-MCI-02; University of Maryland, 2001.
[27] Proper care and handling of compressed natural gas cylinders, Gas Research Bulletin, Chicago, IL: Gas Research Institute, 1996.
[28] Fault tree handbook with aerospace applications (Draft). NASA, 2002; June.
[29] Process equipment reliability data, center for chemical process safety. New York: American Institute of Chemical Engineers 1989.
[30] Droquette EL. Methodology for treatment of model uncertainty. PhD Dissertation, University of Maryland, College Park, MD, 1999.
[31] Watt GM. Natural gas vehicle transit bus fleet the current international experience. Australia: Gas Technology Services 2000.
[32] Guidelines for chemical process quantitative risk analysis, center for chemical process safety. New York: Am. Inst. of Chem. Eng. 1989.
[33] Mowrer FW. Preliminary fire safety analysis of CNG-fueled vehicles. Fire Protection Engineering, University of Maryland, 2001.
[34] Bulk storage of LPG – factors affecting offsite risk. The Assessment of Major Hazards, American Institute of Chemical Engineers, New York: Paragon Press, 1992.
[35] Natural gas transit buses world review. Int. Association for Natural Gas Vehicles (Inc.), 2000.
[36] Alternative fueled vehicle fleet survey. National Technical Information Service, 1999.
[37] Newsday. New York, Newsday Inc., 2001; August 26.
[38] ITAR News. ITAR-TASS News Agency, TASS, 2001; July 10.
[39] Vose D. Quantitative risk assessment system (QRAS). Version 1.6, NASA, Washington, DC.
[40] Vose D. Risk analysis: A quantitative guide. New York: Wiley, 2000.

44

Risk Management

Terje Aven

University of Stavanger, 4036 Stavanger, Norway

Abstract: This chapter reviews and discusses fundamental issues in risk management, related to concepts, principles and methods used. Some of the issues addressed include:

- How we should understand risk.
- How we should express risk.
- How we should deal with uncertainties in future performance.
- How we should balance project risk management and corporate portfolio perspectives.
- How we should use expected values in risk management.
- How we should deal with cautionary and precautionary principles, as well as the ALARP principle (risk should be reduced to a level that is as low as reasonably practicable).
- How we should formulate and use goals, criteria, and requirements to stimulate performance and ensure acceptable safety standards.

44.1 Introduction

In this chapter, we first present some of the basic issues of risk management and risk analysis, as described in the literature and standards, in particular ISO [1]. These relate in particular to different perspectives on risk and key features of risk analysis. A basic distinction is made between the classical approach to risk and probability, and the Bayesian approach or paradigm.

In Section 44.2 we present and discuss the key principles of risk management and decision making, related to economic theories and perspectives, such as cost-benefit analysis and cost-effectiveness analysis, as well as cautionary and precautionary principles. The "cautionary principle" says that in the face of uncertainty, caution should be the ruling principle. The precautionary principle is a special case of the cautionary principle and expresses that caution should be the ruling principle if there is a lack of scientific certainty that will become the consequences of the action.

Special attention is given to the use of expected values in risk management. Expected values as a basis for decision making are supported by the portfolio theory and are a ruling principle among economists. Also, many safety experts view expected values as the key performance measure while making decisions in the face of uncertainties. In this section, we also review and discuss the use of risk acceptance criteria and the ALARP principle.

In Section 44.3, we highlight the key principles that we believe should form the basis of risk management.

The terminology used in this chapter is in line with the ISO standard on risk management terminology [1]. Our definition of risk is, however, slightly adjusted compared to the ISO standard, as discussed in Section 44.1.2. Our main focus is the part of risk management that addresses HES (health, environment, and safety), and in particular major accidents. However, the concepts and principles are applicable also to other areas. The chapter is to a large extent based on [2].

44.1.1 The Basis of Risk Management

The purpose of risk management is to ensure that adequate measures are taken to protect people, the environment, and assets from harmful consequences of the activities being undertaken, as well as balancing different concerns, in particular risks and costs. Risk management includes measures both to avoid the occurrence of hazards and to reduce their potential harms. Traditionally, risk management was based on a prescriptive regulating regime, in which detailed requirements were set to the design and operation of the arrangements. This regime has gradually been replaced by a more goal oriented regime, putting emphasis on what to achieve rather than on the means of doing so.

Risk management is an integral aspect of a goal oriented regime. It is acknowledged that risk cannot be eliminated but must be managed. There is an enormous drive and enthusiasm in various industries and society as a whole nowadays to implement risk management in organizations. There are high expectations that risk management is the proper framework for obtaining high levels of performance.

To support decision making on design and operation, risk analyses are conducted. The analyses include identification of hazards and threats, cause analyses, consequence analyses, and risk description. The results of the analyses are then evaluated. The totality of the analyses and the evaluations are referred to as risk assessments. Risk assessment is followed by risk treatment, which is a process involving the development and implementation of measures to modify risk, including measures designed to avoid, reduce ("optimize"), transfer or retain risk. Risk transfer means sharing with another party the benefit or loss associated with a risk. It is typically affected through insurance. Risk management covers all coordinated activities to direct and control an organization with regard to risk. The risk management process is the systematic application of management policies, procedures and practices to the tasks of establishing the context, assessing, treating, monitoring, reviewing and communicating risks, see Figure 44.1.

Risk management involves achieving an appropriate balance between realizing opportunities for gains while minimizing losses. It is an integral part of good management practice and an essential element of good corporate governance. It is an iterative process consisting of steps that, when undertaken in sequence, enable continuous improvement in decision making and facilitate continuous improvement in performance.

"Establishing the context" (see Figure 44.1) defines the basic frame in which conditions within the risks must be managed and sets the scope for the

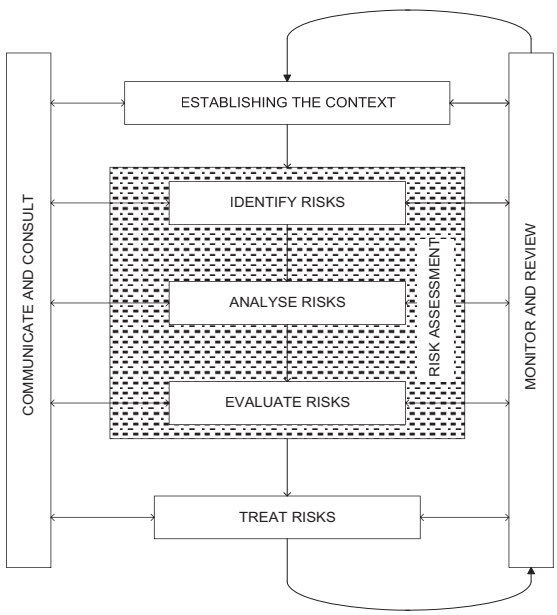


Figure 44.1. The risk management process (based on [3])

rest of the risk management process. The context includes an organization's external and internal environment, and the purpose of the risk management activity. This also includes consideration of the interface between the external and internal environments. The context means a definition of suitable decision criteria as well as structures for how to carry out the risk assessment process.

Risk analysis is often used in combination with risk acceptance criteria, as inputs to risk evaluation. Sometimes the term risk tolerability limits is used instead of risk acceptance criteria. The criteria state is what is deemed as an unacceptable risk level. The need for risk reducing measures is assessed with reference to these criteria. In some industries and countries, it is a requirement in regulations that such criteria be defined in advance of performing the analyses.

Figure 44.2 illustrates the use of risk analysis in a decision making context. The model shown in Figure 44.2 covers the following items:

1. *Stakeholders*. The stakeholders are here defined as people, groups, owners, authorities, *etc*., who have interests related to the decisions to be made. Internal stakeholders may be the owner of the installation, other shareholders, the safety manager, unions, the maintenance manager, *etc.*, whereas external stakeholders may be the safety authorities (the Norwegian Safety Petroleum Authority, the State Pollution Control Agency, *etc*.), environmental groups (Green Peace, *etc*.), research institutions, *etc*.
2. *Decision problem and decision alternatives*. The starting point for the decision process is a choice between various concepts, design configurations, sequence of safety critical activities, risk reducing measures, *etc*.
3. *Analysis and evaluation*. To evaluate the performance of the alternatives, different types of analyses are conducted, including risk analyses and cost-benefit (cost-effectiveness) analyses. These analyses may, given a set of assumptions and limitations, result in recommendations on which alternative to choose.
4. *Managerial review and judgment.* The decision support analyses need to be evaluated in the light of the premises, assumptions and limitations of these analyses. The analyses are based on a background information that must be reviewed together with the results of the analyses. Considerations should be given to factors such as:
   - The decision alternatives being analysed.
   - The performance measures analysed (to what extent do the performance measures used describe the performance of the alternatives?).
   - The fact that the results of the analyses represent judgments and not only facts.
   - The difficulty of assessing values for burdens and benefits.
   - The fact that the analysis results apply to models, *i.e.*, simplifications of the real world, and not the real world itself. The modelling entails the introduction of a number of assumptions, such as replacing continuous quantities with discrete quantities, extensive simplification of time sequences, *etc*.

In Figure 44.2 we have indicated that the stakeholders may also influence the final decision process in step (7) in addition to their stated criteria, preferences, and value tradeoffs providing input to the formal analyses in step (6).

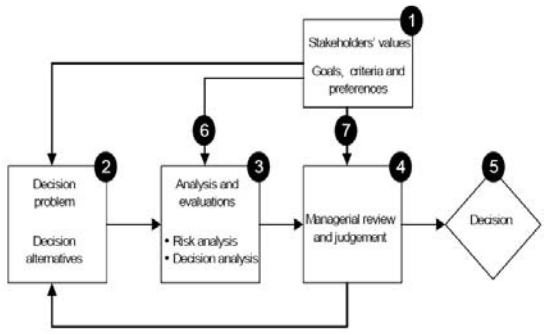


Figure 44.2. Model of the decision making process [2]

Safety management covers all coordinated activities designed to direct and control an organization with regard to safety. We use the term safety when we focus on risk related to accidents. Hence risk management includes safety management in our terminology. In the literature the terms risk and safety, as well as risk management and safety management are defined in many different ways, and often risk and risk management are used in a narrower sense than here, see, *e.g.* [4] and [5]. In safety management emphasis is often placed on aspects related to human and organizational factors, see *e.g.*, [6], [7] and [8], in contrast to risk management which has a tendency to concentrate on the more technical issues.

Similarly we define HES (health, environment, and safety) management. Safety management may be seen as a special part of uncertainty management. While uncertainty management considers all uncertainties regarding the project outcome, *i.e.*, events both with negative and positive consequences, safety management addresses only the uncertainties that can result in accidents. However, safety management is mainly concerned with low-probability and large-consequence events that normally are not considered in uncertainty management. Hence safety management goes beyond what is typically the scope of uncertainty management [9].

Following our terminology for risk, uncertainty management is a part of the risk management, although many aspects normally treated in uncertainty management is not covered by risk management.

44.1.2 Perspectives on Risk

A common definition of risk is that risk is the combination of probability and consequences, where the consequences relate to, for example, loss of lives and injuries. This definition is in line with that used in [1]. However, it is also common to refer to risk as probability multiplied by consequences (losses), *i.e.*, what is called the expected value in probability calculus. If the focus is the number of fatalities during a certain period of time, X, then the expected value is given by E[X], whereas risk defined as the combination of probability and consequence expresses probabilities for different outcomes of X, for example the probability that X does not exceed 10. Adopting the definition that risk is the combination of probability and consequence, the whole probability distribution of X is required, whereas the expected value refers only to the centre of gravity of this distribution. In the scientific risk discipline there is a broad consensus concluding that at risk cannot be restricted to expected values. We need to see beyond the expected values, for example, by expressing the probability of a major accident having a number of fatalities.

Hence risk is seen as the combination of probability and consequence. But what is a probability? There are different interpretations. Here are the two main alternatives:

a). A probability is interpreted in the classical statistical sense as the relative fraction of times the events occur if the situation analyzed were hypothetically "repeated" an infinite number of times. The underlying probability is unknown, and is estimated in the risk analysis.

b). Probability is a measure of expressing uncertainties as to the possible outcomes (consequences), seen through the eyes of the assessor and based on some background information and knowledge.

Following definition a) we produce estimates of the underlying true risk. This estimate is uncertain, as there could be large differences between the estimate and the correct risk value. As these correct values are unknown it is difficult to know how accurate the estimates are.

Following interpretation b), we assign a probability by performing uncertainty assessments, and there is no reference to a correct probability. There are no uncertainties related to the assigned probabilities, as they are expressions of uncertainties.

The implications of the different perspectives are important. If the starting point is a), there is a risk level that expresses the truth about risk, for example for an offshore installation at a given point in time. This risk level is unknown, true, but

in many cases it is difficult to see whether people are talking about the estimates of risk or the real risk.

If the starting point is b) the expert's position may be weakened, as it is acknowledged that the risk description is a judgment, and others may arrive at a different judgment. Also risk estimates represent judgments, but the mixture of estimates and real risk can often give the experts a stronger position in this case.

Depending on the risk perspective, there are different approaches to risk analysis and assessments, risk acceptance, *etc*. We will discuss this in more detail below.

Seeing risk as the combination of probability and consequence means a quantitative approach to risk. A probability is a number. Of course, a probability may also be interpreted in a qualitative way, using an interpretation such as the level of danger. We may, for example, refer to the danger of an accident occurring without reference to a specific interpretation of a probability, neither through a) nor through b). However, as soon as we address the meaning of such a statement and the issue of uncertainty, we must clarify whether we are adopting interpretation a) or b). If there is a real risk level, it is relevant to consider and discuss the uncertainties of the risk estimates compared to the real risk. If probability is a measure of the analyst's uncertainty, a risk assignment is a judgment and there is no reference to a correct and objective risk level.

In some cases we have references levels through historical records. These numbers do not, however, express risk, but they provide a basis for expressing risk. In principle, there is a huge step from historical data to risk that is a statement concerning the future. In practice, many analysts do not distinguish between the data and the risk derived from the data. This is unfortunate as the historical data may to varying degree be representative for the future, and the amount of data may often be very limited. A mechanical transformation from historical data to risk numbers should be avoided.

There are a number of other perspectives to risk than those mentioned above. Some of these are summarized below [10],[11]:

- In psychology there has been a long tradition of work that adopts the perspective to risk, that uncertainty can be represented as an objective probability. Here researchers have sought to identify and describe people's (lay-people's) ability to express the level of danger using probabilities and to understand which factors are influencing the probabilities. A main conclusion is that people are poor assessors if the reference is a real objective probability value, and that the probabilities are strongly affected by factors such as dread.
- Economists usually see probability as a way of expressing uncertainty about the outcome, and often seen in relation to the expected value. Variance is a common measure of risk. Both the interpretations a) and b) are applied, but in most cases without making it clear which interpretation being used. In economic applications a distinction has traditionally been made between risk and uncertainty, based on the availability of information. Under risk the probability distribution of the performance measures can be assigned objectively, whereas under uncertainty these probabilities must be assigned or estimated on a subjective basis [12]. This latter definition of risk is seldom used in practice.
- In decision analysis, risk is often defined as "minus expected utility", *i.e.*,− E[u(X)], where the utility function u expresses the assessor's preference function for different outcomes x.
- Social scientists often use a broader perspective on risk. Here risk refers to the full range of beliefs and feelings that people have about the nature of hazardous events, their qualitative characteristics and benefits, and most crucially their acceptability. This definition is considered useful if lay conceptions of risk are to be adequately described and investigated. The motivation is the fact that there is a wide range of multidimensional characteristics of hazards, rather than just an abstract

expression of uncertainty and loss, which people evaluate in performing perceptions - so that the risks are seen asfundamentally and conceptually distinct. Furthermore, such evaluations may vary with the social or cultural group to which a person belongs, the historical context in which a particular hazard arises, and may also reflect aspects of both the physical and human or organizational factors contributing to hazard, such as trustworthiness of existing or proposed risk management.

- Another perspective, often referred to as cultural relativism, expresses that risk is a social construction and it is therefore meaningless to speak about objective risk.

There also exist perspectives that intend to unify some of the perspectives above, see *e.g.* [13] and [14]. One such perspective, the predictive Bayesian approach [14], is based on the interpretation b), and makes a sharp distinction between historical data and experiences, future quantities of interest such as loss of lives, injuries, *etc.* (referred to as observables), and predictions and uncertainty assessments of these. The thinking is analogous to cost risk assessments, where the costs, the observables, are estimated or predicted, and the uncertainties of the costs are assessed using probabilistic terms. Risk is then viewed as the combination of possible consequences (outcomes) and associated uncertainties. This definition is in line with the definition adopted by the UK Government ([15], p. 7). The uncertainties are expressed or quantified using probabilities. Using such a perspective, with risk seen as the combination of consequences and associated uncertainties (probabilities), a distinction is made between risk as a concept and terms such as risk acceptance, risk perceptions, risk communication and risk management, in contrast to the broad definition used by some social scientists in which this distinction is not clear.

In this chapter we adopt this perspective on risk, viewing risk as the combination of possible consequences and associated uncertainties, acknowledging that risk cannot be distinguished from the context it is a part of, the aspects that are addressed, those who assess the risk, the methods and tools used, *etc*. Adopting such a perspective the risk management needs to reflect this, by

- focusing on analyses and assessments of risk by different analysts;
- addressing aspects of the uncertainties not reflected by the computed expected values;
- acknowledging that what is acceptable risk and the need for risk reduction cannot be determined simply by reference to the results of risk analyses;
- acknowledging that risk perception has a role to play to guide decision makers; professional risk analysts do not have the exclusive right to describe risk.

Such an approach to risk is in line with the recommended approach by the UK Government, see [15], and also the trend seen internationally in recent years. An example where this approach has been implemented is the Risk Level Norwegian sector project, see [16] and [14], p.122.

Let C denote the consequences or outcomes associated with an activity. Typically C would be expressed by some quantities C1, C2, on the real line, *e.g.*, economic loss, number of fatalities, number of attacks, *etc*. These quantities are examples of observable quantities, *i.e*., quantities that express states of the "world", quantities of physical reality or nature, that are unknown at the time of the analysis but will, if the system being analyzed is actually implemented, take some value in the future, and possibly become known.

A source is a situation or an event with a potential of a certain consequence. We distinguish between three categories of sources; threats, hazards, and opportunities. These terms are typically used in security, safety, and economic contexts, respectively. Here security relates to intentional situations and events, whereas safety relates to accidental situations and events. An example of an opportunity is a planned shutdown, which allows for preventive maintenance.

We define vulnerability as the combination of possible consequences and associated uncertainties given a source. Hence risk is the combination of sources (including associated uncertainties) and vulnerabilities.

Based on this definition, we refer to "vulnerability" as an aspect or feature of the system, when the combination of possible consequences and associated uncertainties is judged to give a high vulnerability, *i.e.*, is considered critical in some sense. For example, in a system without redundancy the failure of one unit may result in system failure, and consequently we may judge the lack of redundancy as vulnerability depending on the uncertainties.

44.1.3 Risk Analysis to Support Decisions

Two of the most common methods to identify hazards and risks are FMECA (failure mode and effect and criticality analysis) and HAZOP (hazard and operability studies). In FMECA categorises of the possible consequences and associated likelihoods are introduced, and the criticality is determined using a risk matrix approach. Using this approach different options may be assessed with respect to risk (criticality) and compared using the risk matrix. This is a crude risk analysis. The next level of sophistication of risk analysis is obtained when models are developed to represent cause and/or consequence scenarios. The standard tools used are FTA (fault tree analysis) and ETA (event tree analysis), and the combination of the two, CCA (cause consequence analysis). These models are important elements in a qualitative risk analysis, and provide the basis for a quantitative risk analysis. These are all standard risk analysis methods and the interested reader is referred to textbooks for their description and discussion, see *e.g.*, [5]. For further descriptions and discussions of risk analysis the reader is referred to the chapter in this book on probabilistic risk assessment.

44.1.4 Challenges

Given the above fundamentals of risk management, the next step is to develop principles and methodology that can be used in practical decision making. This is, however, not straightforward. There exist a number of challenges and some of these are addressed here:

i. Establishing an informative risk picture for the various decision alternatives.
ii. The use of this risk picture in a decision making context.

Establishing an informative risk picture means identifying appropriate risk indices, and assessments of uncertainties. Using the risk picture in a decision making context means definition and application of risk acceptance criteria, cost-benefit analyses and the ALARP principle (risk should be reduced to a level that is as low as reasonably practicable).

Risk management involves decision making in situations involving high risks and large uncertainties, and such decision making is difficult as it is hard to predict what would be the consequences (outcomes) of the decisions. A number of tools are available to support decision making in such situations, such as risk and uncertainty analyses, risk acceptance criteria (tolerability limits), cost-benefit analyses (expected net present value calculations) and cost-effectiveness analyses (addressing, *e.g.*, expected costs *per* statistical saved lives). However, these tools do not provide clear answers. They have limitations and are based on a number of assumptions and presumptions, and their uses are based not only on scientific knowledge, but also on value judgments involving ethical, strategic and political concerns. Some of the challenges related to these tools are: the assessment of uncertainties and assignment of probabilities, determination of appropriate values for quantities such as a statistical life and the discount rate, to distinguish between objective knowledge and subjective judgments, treatment of uncertainties and the way of dealing with intangibles.

Risk analyses, cost-benefit analyses and related type of analyses provide support for decision making, leaving the decision makers to apply decision processes outside the direct applications of the analyses. We speak about managerial review and judgment, see. Figure 44.2. It is not desirable to develop tools that prescribe or dictate the decision. That would mean a too mechanical approach to decision making and would fail to recognize the important role of management to

perform difficult value judgments involving uncertainty.

Nonetheless, there is a need to provide guidance and a structure for decision making in situations involving high risks and large uncertainties. The aim must be to obtain a certain level of consistency in decision making and confidence in obtaining desirable outcomes. Such guidance and structure exist to some degree, and the challenge is to find the right level. This will be discussed in more detail in the following sections.

44.2 Risk Management Principles

44.2.1 Economic and Decision Analysis Principles

This section gives a brief introduction to decision analysis theory, emphasizing expected utility theory, cost-benefit analysis, the use of expected values to support decision making, and risk aversion. The purpose of the section is not to give a comprehensive and all-including review of the field, but to highlight important issues important for risk management.

44.2.1.1 Expected Utility Theory

We consider a decision situation involving possible consequences (outcomes) that are subject to uncertainties. The problem is to make a "good" decision in such a situation. We may, for example, think of a choice between a number of different investment alternatives or development projects for an offshore installation. In theory, the optimization of the expected utility is the ruling paradigm among economists and decision analysts in such a situation, see, *e.g.*, [17],[18],[19]. The expected utility is in mathematical terms written like Eu(X), where u is the utility function and X is the outcome expressing a vector of different attributes, for example, costs and the number of fatalities. The expected utility approach is theoretically attractive, as it provides recommendations based on a logical basis. If a person is coherent both in his preferences amongst consequences and in his assessments about uncertain quantities, it can be proved that the only sensible way for him to proceed is by maximizing expected utility. For a person to be coherent when speaking about the assessment of uncertainties of events, the requirement is that he follows the rules of probability. When it comes to consequences, coherence means adherence to a set of axioms including the transitive axiom: If b is preferred to c, which is in turn preferred to d, then b is preferred to d. What we are doing is making an inference according to a principle of logic, namely that implication should be transitive. Given the framework in which such maximization is conducted, this approach provides a strong tool for guiding decision makers.

In practice it is difficult to work out a utility function. The proper specification of the utility function means the application of a lottery process, as explained in, *e.g.*, [18]. This lottery process is not straightforward to carry out in practice, and simplification procedures are presented to ease the specifications. One possible approach is to define a parametric function for the utility function, which is determined up to a certain parameter, and the value specification is reduced to assigning a number to this parameter. Examples of such procedures are found in [14]. This approach simplifies the specification process significantly, but it can be questioned whether the process imposes a too strong requirement on the specification of the utilities. Is the parametric function actually reflecting the decision maker's preferences? The decision maker should be skeptical to let his preferences be specified more or less automatically without a careful reflection of what his preferences are. Complicated value judgments are not easily transformed to a mathematical formula.

The specification of the utility function is particularly difficult when there are several attributes, and in most cases this is so. For multi-attribute utility functions simplifications can be performed by using weighted averages of the individual utility functions, see, *e.g.*, [20]. Again it is a question whether the simplification can be justified [14].

Hence methods exist that makes the specification process more feasible in practice. Nonetheless, the author of the chapter still see the expected utility theory as difficult to use in many

situations, in particular in the situations of main interest for this premise, is characterized by a potential of large consequences and relatively large uncertainties as to what the consequences will be? It is also acknowledged that even if it were possible to establish practical procedures for specifying utilities for all possible outcomes, decision makers would be skeptical to reveal these, as it would mean reduced flexibility to adapt to new situations and circumstances. In situations with many parties, as in political decision making, this aspect is of great importance.

Although the expected utility theory is the ruling paradigm for decision making under uncertainty among economists and decision analysts, experimental studies on decision making under uncertainty have revealed that individuals tend to systematically violate the independence axiom of the expected utility theory. Several alternative frameworks and theories have been established, and the rank-dependent utility theory is one of the most popular [21],[22]. The rank-dependent utility theory has been developed to better reflect how people act in real life.

The problems mentioned above in applying the expected utility theory also apply for the rank-dependent theory. However, a discussion of the suitability of the rank dependent theory compared to the expected utility theory is beyond the scope of this chapter.

There also exist other analysis approaches, and the most used in practice are cost-benefit analysis and cost-effectiveness analysis. Before we review these analyses we will briefly look into the rationale for using expected values to support decision making under uncertainty.

44.2.1.2 The Use of Expected Values to Support Decision Making. Risk Aversion

In situations with a number of independent activities, the use of expected values can provide strong guidance on how to make decisions. The justification is the law of large number saying that the average of a number of random quantities can be accurately approximated by the expected value when the number of quantities is high. In economic theory, the so-called portfolio theory plays a similar role: it justifies the use of expected values to support decision making when considering a large number of projects.

The portfolio theory expresses that the value of a portfolio of projects is equal to the expected value of the portfolio plus unsystematic and systematic risks (interpreted here as uncertainties) [23]. The systematic risk relates to general market movements, for example caused by political events, and the unsystematic risk relates to specific project uncertainties, for example, accident risks. When the number of projects is large, the unsystematic economic risk can be ignored. By diversification of the risks into many projects, the unsystematic risks are removed. A company's total cash flow (all projects are included) is approximately equal to the expected cash flow of all the projects, when ignoring the systematic risk. The difference between the portfolio's actual value and its calculated statistical expected value lies in from the portfolio theory being just dependent on the systematic risk.

However, the portfolio theory is just a theory; it has limitations. Some of these limitations and their effects are [2],[24] as follows:

1. Expected values should be used with care when an activity involves the possibility of a large accident, as large accidents have a minor effect on expected values, due to their small probabilities, but if they occur they can result in consequences that are not outweighed by other projects in the portfolio.
2. Assessments of uncertainties are difficult and the probability assignments are based on a number of assumptions and suppositions and will depend on the assessors' judgments. The expected values computed are not objective numbers.
3. Large accidents most often involve consequences that are difficult to transform to monetary values, and the expected NPV can give limited information about the consequences exceeding the strict economic values. What is the value of a life and the environment? How should the company reflect, for example, that a life has a value in itself?

Hence, uncertainty needs to be considered beyond the expected values. The important question then is how the uncertainties should be reflected in the decision making process.

When evaluating the risks, the decision maker's attitude towards risk can affect the outcome of the evaluation process. It is common to divide the decision makers into three categories: risk seeking, risk neutral and risk averse, where risk averse is the standard behavioral assumption, see [17]. The risk aversion principle is defined in decision analysis and the economic literature, see *e.g.*, [25], and reflects that we dislike negative consequences so much that these are given more weight than what is justified by reference to the expected value. Mathematically these terms are defined as follows; we call the decision maker's behavior risk averse if $E_u(X) < u(EX)$. The behavior is risk neutral if $E_u(X) = u(EX)$ and risk seeking if $E_u(X) > u(EX)$. These concepts can also be rephrased using the so-called certainty equivalent. The certainty equivalent C(X) is the value replacing the uncertain situation with C with certainty. Hence in a situation of risk aversion, the certainty equivalent is less than the expected value EC.

In the safety community, risk aversion is often referred to as an attitude to risks and uncertainties, expressing that we dislike or has antipathy against the risks and uncertainties [26]. Such an interpretation is in line with the standard dictionary definition of the word "aversion".

There seems to be a gap between the theory developed in the economic and decision analysis literature and the practical use in safety contexts. Safety people often seem to lack a basic understanding of what risk aversion means, as defined by the economic literature [27]. Following the economist interpretation, risk aversion is not a way of justifying decisions, but a way of characterizing behavioral attitudes and decisions. Two persons may both be risk averse in a specific case, but conclude in different ways on how to handle the risk.

44.2.1.3 Cost-benefit Analysis and Cost-effectiveness Analysis

A traditional cost-benefit analysis is an approach to measure benefits and costs of a project. The common scale used to measure benefits and costs is the country's currency. The main principle in transformation of goods into monetary values is to find out what the maximum amount the society is willing to pay for the project. Market goods are easy to transform to monetary values since the prices on the market goods reflect the willingness to pay. The willingness to pay for non-market goods is on the other hand more difficult to determine, and different methods such as contingent valuation and hedonic price techniques are used. The reader is referred to [28].

After transformation of all attributes to monetary values, the total performance is summarized by computing the expected net present value, the E[NPV], see, *e.g.*, [17]. To measure the NPV of a project, the relevant project cash flows (the movement of money into and out of your business) are specified, and the time value of money is taken into account by discounting future cash flows by the appropriate rate of return. The formula used to calculate NPV is:

$$\mathrm{NPV} = \sum_{t=0}^{T} \frac{X_t}{(1+r_t)^t},$$

where, X_t is equal to the cash flow at year t, T is the time period considered (in years) and r is the required rate of return, or the discount rate, at year t. The terms capital cost and alternative cost are also used for r. As these terms imply, r represents the investor's cost related to not employing the capital in alternative investments. When considering projects where the cash flows are known in advance, the rate of return associated with other risk-free investments, like bank deposits, makes the basis for the discount rate to be used in the NPV calculations. When the cash flows are uncertain, which is usually the case, they are normally represented by their expected values $E[X_t]$, and the rate of return is increased on the basis of the capital asset pricing model (CAPM) in order to outweigh the possibilities for unfavorable outcomes. The risk adjustment is based on the systematic risk only. The reader is referred to [29].

The cost-benefit analysis is based on a risk neutral behavior. However, several methods have been developed to reflect risk aversion in the

analysis. A review is given in [30]. See also Section 44.3.

We distinguish between a cost-benefit analysis and a cost-effectiveness analysis. The latter analysis is an analysis where indices of the form expected cost *per* expected saved lives (statistical life) are calculated. The analysis method does not explicitly put a value to the benefit, say a statistical life, as is required in the cost-benefit analysis.

44.2.1.4 Multi-attribute Analysis

A multi-attribute analysis is a decision support tool analysing the consequences of the various measures separately for the various attributes. Thus there is no attempt made to transform all the different attributes in a comparable unit.

As a part of the multi-attribute analysis, expected net-present values for economic measurable attributes may be reported as well as cost-effectiveness ratios.

44.2.2 The Cautionary and Precautionary Principles

The cautionary principle is a basic principle in safety management, expressing the idea that, in the face of uncertainty, caution should be a ruling principle [31]. This principle is being implemented in all industries through safety regulations and requirements. For example, in the Norwegian petroleum industry it is a regulatory requirement that in the living quarters, the walls facing process and drilling areas be protected by fireproof panels of a certain quality. This is a standard adopted to obtain a minimum safety level. This is based on established practice of many years of operation of process plants. A fire may occur, it represents a hazard for the personnel, and in the case of such an event, the personnel in the living quarters should be protected. The assigned probability for the living quarter on a specific installation being exposed to fire may be judged as low, but we know that fires occur from time to time in such plants. It does not matter whether we calculate a fire probability of x or y, as long as we consider the risks to be significant; and this type of risk has been judged to be significant by the authorities. The justification is experience from similar plants and sound judgments. A fire may occur, since it is not an unlikely event, and we should then be prepared. We need no references to cost-benefit analysis. The requirement is based on a cautionary thinking.

Risk analyses, cost-benefit analyses and similar types of analyses are tools providing insights into risks and the trade-offs involved. But they are just tools, with strong limitations. Their results are conditioned on a number of assumptions and suppositions. The analyses do not express objective results. Being cautious also means reflecting this fact. We should not put more emphasis on the predictions and assessments of the analyses than what can be justified by the methods being used.

In the face of uncertainties related to the possible occurrences of hazardous situations and accidents, we are cautious and adopt principles of safety management, such as

- robust design solutions, such that deviations from normal conditions do not leading to hazardous situations and accidents;
- design for flexibility, meaning that it is possible to utilize a new situation and adapt to changes in the frame conditions;
- implementation of safety barriers, to reduce the negative consequences of hazardous situations if they should occur, for example a fire;
- improvement of the performance of barriers by using redundancy, maintenance/testing, *etc*.;
- quality control/quality assurance;
- the precautionary principle, meaning that in the case of lack of scientific certainty on the possible consequences of an activity, we should not carry out the activity;
- the ALARP principle, meaning that the risk should be reduced to a level that is as low as reasonably practicable.

The level of caution adopted will, of course, have to be balanced against other concerns such as costs. However, all industries would introduce some minimum requirements to protect people and the environment, and these requirements can be

considered justified by the reference to the cautionary principle.

In this section we will draw special attention to the precautionary principle, whereas the ALARP principle will be discussed in Section 44.3.

There are many definitions of the precautionary principle, see *e.g.*, [32] and [33]. The most commonly used definition is probably the 1992 Rio Declaration:

> *In order to protect the environment, the precautionary approach shall be widely applied by states according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation.*

Seeing beyond environmental protection, a definition such as the following reflects what we believe is a typical way of understanding this principle:

> *The precautionary principle is the ethical principle that if the consequences of an action, especially the use of technology, are subject to scientific uncertainty, then it is better not to carry out the action rather than risk the uncertain, but possibly very negative, consequences.*

The key aspect is that if there is a lack of scientific certainty as to the consequences of an action, then that action should not be carried out.

The problem with this statement is that the meaning of the term "scientific certainty" is not at all clear. As the focus is on the future consequences of the action, there would be no (or at least very few) cases with known outcomes. Hence scientific uncertainty must mean something else. Three natural candidates are:

i. knowing which type of consequences could occur,
ii. being able to predict the consequences with sufficient accuracy, and
iii. having accurate descriptions or estimates of the real risks, interpreting the real risk as the consequences of the action.

If we adopt one of these interpretations, the precautionary principle may be applied either when we do not know the type of consequences that may occur, or we have poor predictions of the consequences, risk descriptions or estimates. As an example, let us think of the issue about starting year-round petroleum activities in the Barents Sea. In December 2003 the Norwegian government considered whether year-round activities should be allowed for the areas of Lofoten and the Barents Sea, both ecologically vulnerable areas. Then following i) and using broad categories of consequences we cannot apply the precautionary principle, as we know the type of consequences of this activity. As a result of these operations, some people may be killed, some may get injured, or an oil spill may occur causing damage to the environment, *etc*. Different categories of this damage can be defined. Hence by grouping of categories and types of consequences, the possible lack of scientific certainty is "eliminated".

However, in this case, many biologists would say that there is some lack of knowledge as to what the consequences for the environment will be, given an oil spill. This lack of scientific certainty could be classified as fairly small, but that would be a value statement and people and parties could judge this differently. The point is that there is some scientific uncertainty about the consequences of an oil spill. But is this lack of scientific certainty of a different kind than uncertainty related to what will be the outcome of the oil spill? Consider the consequences of an oil spill on fish species, and let X denote the recovery time for the population of concern, with X being infinity if the population does not recover. Then there is scientific certainty according to criterion ii) if there is scientific consensus about a function (model) f such that X equals $f(Z_1, Z_2\ldots)$ with high confidence, where Z_1, $Z_2\ldots$ are some underlying factors influencing X. Such factors could relate to the possible occurrence of a blow-out, the amount and distribution of the oil spilled on the sea surface, the mechanisms of dispersion and degradation of oil components, and the exposure and effect on the fish species. For selected values of the Z_s, we can use f to predict the consequences X. The precautionary principle applies when it is difficult to establish such a

function f; the scientific discipline does not have sufficient knowledge for obtaining "scientific certainty" on how the high level performance, in this case measured by X, is influenced by the underlying factors. Models may exist, but they are not broadly accepted in the scientific community.

Scientific consensus in this sense does not mean that the consequences (X) can be predicted with accuracy, when not conditioned on the Zs. Unconditionally, the consequences (X) are uncertain, and this uncertainty is defined by the uncertainties of the factors Z.

To study the criterion iii), suppose that p represents the "real" risk, quantified by the probability distribution of X, and let p* be an estimate of p derived from a detailed risk analysis of the activity. Since the uncertainties in this estimate are considered large, relative to the real p, the precautionary principle may be applied following criterion iii). We see that using i), ii) or iii), we may obtain different conclusions.

44.2.2.1 Discussion

Among most economists and decision analysts, the theoretical framework for obtaining good decisions is the expected utility theory, based on the use of subjective probabilities. Attention should be on Eu(X), where u is the utility function and X is the outcome. In this framework there is no place for the application of the precautionary principle, as the expected utility is the appropriate guidance for the decision maker. Uncertainties and the weights put on these uncertainties are properly taken into account using this theory.

However, this is a theory, and it is difficult to prove in practice. People do not behave according to this theory. This is well known, and different alternative frameworks have been suggested. Many economists would refer to the cost-benefit analyses, as the adequate practical tool to guide the decision makers. By transforming all values to monetary values and calculating expected net present values, E[NPV]s, a consistent procedure is obtained for making decisions, which is believed to provide good decisions seen from a societal point of view.

Again, in this framework there is no place for the application of the precautionary principle, as the cost-benefit analysis is the appropriate tool for the decision maker. However, few people would conclude that the cost-benefit analyses and related tools provide clear answers. They have limitations and are based on a number of assumptions and presumptions, and their use is based not only on scientific knowledge, but also on value judgments involving ethical, strategic and political concerns. The analyses provide support for decision making, leaving the decision makers to apply decision processes outside the direct applications of the analyses. It is necessary to see beyond the expected values.

The important question then is how the uncertainties should be taken into account in the decision making process. The precautionary principle is a way of dealing with the uncertainties. The above discussion has demonstrated that the precautionary concept is difficult to understand and use, and depends on the perspective on risk applied.

To us the most meaningful definition of the precautionary principle relates to the lack of understanding of how the consequences of the activity are influenced by the underlying factors, *i.e.*, a version of criterion ii). If there is a lack of such knowledge, we may decide not to carry out the activity with references to the use of the precautionary principle. Any reference to being able to accurately measure probabilities should be avoided, as that leads to a meaningless discussion of accuracy in probability estimates. We have to acknowledge that it is not possible to establish science-based criteria for when the precautionary principle should apply. Judging when there is a lack of scientific certainty is a value judgment. In the face of uncertainty, analysts and scientists need to do a good job of expressing the uncertainties, enabling the decision maker to obtain an informative basis for his or her decision. Based on our experience, there is a large potential for improvement on risk and uncertainty descriptions and communications. Many analysts and scientists have severe problems in dealing with uncertainties, as do many statisticians. Being aware of the different perspectives on risk, and using these in the descriptions and communications, we see as a key element in improving the present situation.

Is there then a need for the concept precautionary principle? Could we not just refer to the possible consequences, the uncertainties and the probabilities, *i.e.* the risks? Well, we need a term for saying that we will not start an activity in the face of large uncertainties and risks, and we will not postpone the implementation of measures because of uncertainties. We may refer to this as a cautionary principle [34], but it would be too broad a definition for the precautionary principle. Unfortunately, this kind of broad interpretation of the precautionary principle is often seen in practice. We prefer to restrict the precautionary principle to situations where there is a lack of understanding of how the consequences (outcomes) of the activity are influenced by the underlying factors, and use the concept of caution as the broader principle saying that caution should be the ruling principle in the face of risk. Hence we adopt the cautionary principle when the criterion ii) is not met, *i.e.*, risk is present, and the precautionary principle in the special case described above.

This thinking seems to be consistent with the meaning and the use of this principle adopted by HSE [34] in the UK adheres to the following policy for using the precautionary principle.

Our policy is that the precautionary principle should be invoked where:

- there is good reason, based on empirical evidence or plausible causal hypothesis, to believe that serious harm might occur, even if the likelihood of harm is remote; and
- the scientific information gathered at this stage of consequences and likelihood reveals such uncertainty that it is impossible to evaluate the conjectured outcomes with sufficient confidence to move to the next stages of the risk assessment process.

An essential point here is that the precautionary principle is linked to outcomes and not risks.

44.2.2.2 An Example from the Offshore Oil and Gas Industry

A riser platform is installed with a bridge connection to a gas production platform. On the riser platform, there are two incoming gas pipelines and one outgoing gas pipeline. The pipelines are all large in diameter, 36 inches and above. The decision problem is whether or not to install a sub-sea isolation valve (SSIV) on the export pipeline.

We assume that the analyst has specified an annual frequency of $1x10^{-4}$ *per* year for ignited pipeline or riser failures, *i.e.*, the computed expected number of failures for a one year period is $1x10^{-4}$, which is the same as saying that there is a probability of $1x10^{-4}$ for a failure event to occur during one year. In the case of an accident, the SSIV will dramatically reduce the duration of the fire, and hence damages to equipment and exposure of personnel.

Let us assume that the computed expected number of fatalities without SSIV is 5, given pipeline/riser failure, and 0.5 with SSIV installed. Let us further assume that the expected damage cost without SSIV is 800 MNOK (million Norwegian Krones), given pipeline/riser failure, and 200 MNOK with SSIV installed. When there is no SSIV installed, the riser platform will have to be rebuilt completely, which is estimated to take two years, during which time there is no gas delivery at all. This corresponds to an expected loss of income of 40000 MNOK. With SSIV installed, the expected loss of income is 8000 MNOK.

The expected investment cost is taken as 75 MNOK, and the annual expected cost for inspection and maintenance is 2 MNOK. In the calculations of the expected net present value, 10% interest is used. All monetary values are calculated without taking inflation into account.

The total expected net present value of costs related to the valve is 93.9 MNOK, with annual maintenance costs over 30 years. The annual expected saving (*i.e.* reduced expected damage cost and reduced expected lost income) is 3.26 MNOK, and the expected net present value over 30 years is 30.7 MNOK. This implies that the expected net present value of the valve installation is a cost of 63.2 MNOK.

The expected number of averted fatalities *per* year is $4.5x10^{-4}$ fatalities. Summed over 30 years

(without depreciation of lives), this gives an expected value of averted fatalities equal to 0.0135.

Thus, the expected net present value of the costs *per* averted statistical life is 4675 MNOK, and a cursory evaluation of such a value would conclude that the cost is in gross disproportion to the benefit.

But let us examine the results more closely. It should be noted that if the frequency of ignited failure is 10 times higher, 10^{-3} *per* year, the expected net present value of the reduced costs becomes 307 MNOK (instead of 30.7 MNOK). This implies that the valve actually means an expected cost saving. In this case, the conclusion based on expected values, should clearly be to install the valve.

If we return to the base case values, the probability of experiencing a pipeline or riser failure near the platform is 0.3%, *i.e.*, the scenario is very unlikely. There is a 99.7% probability that there will never any need for the SSIV, and its installation is just a loss, without any possibility of covering any costs.

But with a small probability, 0.3 %, a highly positive scenario will occur. An ignited leak occurs, but the duration of the fire is limited to a few minutes, due to the valve cutting off the gas supply. There are still some consequences; the expected number of fatalities is 0.5, expected damage cost of 200 MNOK, and expected lost income of some months, equivalent to 8000 MNOK. These are quite serious consequences, but they would be so if an SSIV were not installed. The expected saving in this case are 4.5 fatalities, 600 MNOK damage cost, and 32000 MNOK in lost income. Note that we in the above calculations have disregarded the probability that the SSIV will not work when needed (the error introduced by this simplification is small as the assigned probability of a SSIV failure is small).

If we focus on the economy, there is a probability of 99.7% of a 63 MNOK loss (in expected net present value), and a probability of 0.3% of 32 600 MNOK reduced damage cost (in expected net present value) in a year with a pipeline/riser failure. The expected NPV, based on these conditions, becomes 63.1 MNOK. For the installation in question, the expected net present value of 63.1 MNOK is not very informative, either the scenario occurs, with an enormous cost saving (and reduced fatalities) or it does not occur, and there are only costs involved.

From the portfolio theory, and a corporate risk point of view, it is still a reasonable approach to use statistical expected values as a tool for evaluating the performance of this project. But as discussed above, we should not perform a mechanical decision making based on the expected value calculations. We need to take into account the above factors. The conclusion then becomes an overall strategic and political one, rather than one determined by the safety discipline.

44.2.3 Risk Acceptance and Decision Making

The safety regulation in industries nowadays is to large extent goal-oriented, *i.e.*, high level performance measures need to be specified and various type of analyses have to be conducted to identify the best possible arrangements and measures according to these performance measures. There has been a significant trend internationally in this direction for more than ten years. On the other hand, there are different approaches taken in order to implement this common objective, if worldwide regulatory regimes are considered.

Whereas the objective may seem simple as a principle, there are certainly some challenges to be faced in the implementation of the principle. One of the main challenges is related to the use of predetermined quantitative risk acceptance criteria, expressed as upper limits of acceptable risk.

Some examples of risk acceptance criteria used for an offshore installation, are as follows:

- The FAR value should be less than 10 for all personnel on the installation, where the FAR value is defined as the expected number of fatalities *per* 100 million exposed hours
- The individual probability that a person is killed in an accident during one year should not exceed 0.1%.

Note that in the following, when using the term "risk acceptance criteria", we always have in mind such upper limits. Now, should we use such

criteria before any analysis of the systems is conducted? The traditional textbook answer is yes. First comes the criteria, then the analysis to see if these criteria are met, and according to the assessment results, the need for risk reducing measures is determined. Such an approach is intuitively appealing, but a closer look reveals several problems, of which the following two are the most important:

1. The introduction of pre-determined criteria may give the wrong focus, meeting these criteria rather than obtaining overall good and cost-effective solutions and measures.
2. The risk analyses, the tools used to check whether the criteria are met, are not generally sufficiently accurate to permit such a mechanical use of criteria.

Item 1 is the main point. The adherence to a mechanistic use of risk acceptance criteria does not provide a good structure for management of risk to personnel, environment or assets. This is clearly demonstrated for environmental risk. Acceptability of operations with respect to environmental risk is typically decided on the results of a political process and following this process, risk acceptance is not an issue and risk acceptance criteria do not have an important role to play. Risk acceptance criteria have been required by Norwegian authorities for more than 10 years, but almost never have such criteria lead to improvement from an environmental point of view. The reader is referred to the discussion in [35].

The point here is that there are good reasons for looking at other regimes and discuss these against the one based on risk acceptance criteria. The ALARP principle as adopted in the UK represents such an alternative. This principle means that the risk should be reduced to a level which is as low as reasonably practicable. Identified improvements (risk reducing measures) should be implemented as a base case, unless it can be demonstrated that the benefits are grossly disproportionate to the costs and operational restrictions. This principle is normally applied together with a limit for intolerable risk and a limit for negligible risk. The interval between these two limits is often called the ALARP region.

In most cases, in practice risk is found to be in the ALARP region and the ALARP principle is adopted, and an ALARP assessment process is required. This will include a dedicated search for possible risk reducing measures and a subsequent assessment of these in order to determine which to be implemented.

In the UK, the ALARP principle applies in such a way that the higher a risk is, the more employers are expected to spend to reduce it. At high risks, close to the level of intolerability, they are expected to spend up to the point where further expenditure would be grossly disproportionate to the risk; *i.e.* that costs and/or operational disturbances are excessive in relation to the risk reduction. This is generally considered to be a reasonable approach as higher risks call for greater spending. More money should be spent to save a statistical life if the risk is just below the intolerability level than if the risk is far below this level.

The ALARP principle implies what could be referred to as the principle of "reversed onus of proof". This means that the base case is that all identified risk reduction measures should be implemented, unless it can be demonstrated that there is gross disproportion between costs and benefits. To verify ALARP, procedures mainly based on engineering judgments and codes are used, but also traditional cost-benefit analyses and cost effectiveness analyses. When using such analyses, guidance values as indicated above are often used, to specify what values define "gross disproportion". Such values may vary from substantially less than 1 million NOK, up to more than 100 million NOK.

A typical number for a value of statistical life used in cost-benefit analysis is 1–2 million £ [35, 36]. This number applies to the transport sector. For other areas the numbers are much higher, for example in the offshore UK industry it is common to use 6 million £ [36]. This increased number accounts of the potential for multiple fatalities and uncertainty.

The practice of using traditional cost-benefit analyses and cost effectiveness analyses to verify ALARP has been questioned [37]. The ALARP principle is an example of application of the cautionary principle. Uncertainty should be given

strong weight, and the grossly disproportionate criterion is a way of making the principle operational. However, cost-benefit analyses calculating expected net present values ignore the unsystematic risks (uncertainties) and the use of this approach to weight the unsystematic risk is therefore meaningless.

Modifications of the traditional cost-benefit analysis are suggested to solve this problem, see *e.g.,* [30]. In these methods, adjustments are made to either the discount rate or the contribution from cash flows. This latter case could be based on the use of certainty equivalents for uncertain cash flows. Although arguments are provided to support these methods, their rationale can be questioned. There is a significant element of arbitrariness associated with the methods, in particular when seen in relation to the standard given by the expected utility theory.

To explain this in more detail, say that the net present value relates to two years only, and the cash flows are X_0 and X_1. Then an approach based on certainty equivalents means an expected utility approach for the cash flows seen in isolation. The uncertain cash flows are replaced by their certainty equivalents c_0 and c_1, respectively, which means that the uncertain cash flow X_i is compared to having the money c_i with certainty, $i = 0,1$. The specification of such certainty equivalents is not straightforward, ref. the review of the expected utility theory in Section 44.2.1. However, the important point here is not this specification problem, but the fact that this procedure does not necessarily reflecting the decision maker's preferences. If we ignore the discounting for a second, the utility function of the cash flows X_0 and X_1 is not in general given by the sum of the individual utility functions. By introducing certainty equivalents on a yearly basis, we take uncertainties into account, but the way we do it has not been justified.

The alternative approach of adjusting the discount rate seems plausible as the systematic risk is incorporated in the net present value calculations through this procedure. But how large should the adjustment be? There is a rationale for the systematic risk adjustment, the CAPM model, but there is no such a rationale for the unsystematic risk. It will be impossible to find such a rationale, in fact, as the calculations are based on expected cash flows, which ignores the uncertainties. Hence we have to conclude that such an adjustment cannot be justified.

The common procedures for verifying the grossly disproportionate criterion using cost-benefit analysis therefore fail, even if we try to adjust the traditional approach. We should be careful in using an approach which is based on a conflicting perspective, ignoring unsystematic uncertainties.

So what alternative would we then suggest? In our view we have to acknowledge that there is no simple and mechanistic method or procedure for balancing different concerns. When it comes to the use of analyses and theories we have to adopt a pragmatic perspective. We have to acknowledge the limitations of the tools, and use them in a broader process where the results of the analyses are seen as just one part of the information supporting the decision making. Moreover, the results need to be subject to an extensive degree of sensitivity analyses.

44.2.3.1 Discussion

Above we have argued for the need to consider risk as a basis for making decisions under uncertainty. Such considerations however, must be seen in relation to other burdens and benefits. Care should be shown when using pre-determined risk acceptance criteria in order to obtain good arrangements, plans and measures. Pre-defined criteria driving the decisions should in general be replaced by a risk management approach highlighting risk characterization and evaluation, and a drive for risk reductions and a proper balance between burdens and benefits.

Risk analyses support decision making on choice of specific concepts, arrangements, measures, procedures, *etc*., as well as decision criteria. Such decision criteria may have the form of a requirement, for example, the system should have a probability of failure of maximum 1/1000 for a period of one year. Further detailing of this system in a later development phase, could involve risk/reliability/performance analyses to support decision making, and 1/1000 would be a boundary

condition for system performance. Some people may also refer to 1/1000 as a pre-determined risk acceptance criterion. This example illustrates the different levels of criteria that are used for supporting decision making, and the need to view the development of criteria and requirements in a time perspective. Above we have mainly focused on the high level criteria, used for the total system and not its many subsystems and components. For the latter it may be more appropriate to apply specific acceptance limits, to facilitate the design and development process, but even for such situations our main line of approach could be used. Generating alternatives and predicting their burdens and benefits, should always, in our view, be the ruling paradigm.

We see that there is a hierarchy of goals, criteria, and requirements. These can schematically be divided into four categories;

1. Overall ideal goals, for example "our goal is to have no accident".
2. Risk acceptance criteria (defined as upper limits of acceptable risk) or tolerability limits, managing the accident risk, for example, "the individual probability of being killed in an accident shall not exceed 0.1%".
3. Requirements related to the performance of safety systems and barriers, such as a reliability requirement for a safety system.
4. Requirements related to the specific design and operation of a component or subsystem, for example, the gas detection system.

Our main message can be summarized as follows:

- Focus should be on meeting defined overall objectives; which should be formulated using quantities that are observable (such as the number of fatalities, the number of injuries, the occurrence of a specific accidental event, *etc*.). Probabilistic quantities should not be used to express such objectives.
  - Safety management is a tool for obtaining confidence in meeting these objectives.
  - Emphasis should be placed on generating alternatives, to be compared with projected performance.
  - Risk acceptance criteria (level 2 above) should not be used.
- To ease the planning process for optimizing arrangements and measures, requirements related to safety systems and barriers may be useful (level 3 above).
- What is acceptable from a safety point of view and what constitutes a defensible safety level, cannot in principle be determined without incorporating all the pros and cons of the alternative, and the decision needs to be taken by personnel with formal responsibility at a sufficiently high level.

44.3 Recommendations

We recommend a risk assessment process following a structure as summarized in the following:

For a specified alternative, say A, we assess the consequences or effects of this alternative seen in relation to the defined attributes (safety, costs, reputation, *etc*.). Hence we first need to identify the relevant attributes (X_1, X_2, …), and then assess the consequences of the alternative for these attributes. These assessments could involve qualitative or quantitative analysis. Regardless of the level of quantification, the assessments need to consider both what the expected consequences are, as well as uncertainties related to the possible consequences. Often the uncertainties could be large. In line with the adopted perspective on risk, we recommend a structure for the assessment according to the following scheme:

1. Identify the relevant attributes (safety, costs, reputation, alignment with main concerns, *etc*.) .
2. What are the assigned expected consequences, *i.e.*, $E[X_i]$ given the available knowledge and assumptions?
3. Are there special features of the possible consequences? In addition to assessing the consequences on the quantities X_i, some

aspects of the possible consequences might need special attention. Examples are presented below based on the scheme developed in [38].

4. Are the large uncertainties related to the underlying phenomena, and do experts have different views on critical aspects? The aim is to identify factors that may lead to consequences Xi far from the expected consequences $E[X_i]$. A system for describing and characterizing the associated uncertainties is outlined below (based on [9]).
5. The level of manageability during project execution. To what extent is it possible to control and reduce the uncertainties, and obtain desired outcomes? The expected values and the probabilistic assessments performed in the risk analyses provide predictions for the future, but some risks are more manageable than others, meaning that the potential for reducing the risk is larger for some risks compared to others. By proper uncertainty and safety management, we seek to obtain desirable consequences. This leads to considerations on, for example, how to run processes reducing risks (uncertainties) and how to deal with human and organizational factors and obtain a good safety culture.

The structure in [38], which has been modified in [39], consists of eight consequence characteristics:

a) Potential consequences (outcomes), represented by representative performance measures (future observable quantities) such as costs, income, production volumes, deliveries, number of fatalities, *etc*.
b) Ubiquity, which describes the geographical dispersion of potential damage,
c) Persistency, which describes the temporal extension of the potential damage,
d) Delay effect, which describes the time of latency between the initial event and the actual impact of damage. The time of latency could be of physical, chemical or biological nature.
e) Reversibility, which describes the possibility to restore the situation to the state before damage occurred.
f) Violation of equity. which describes the discrepancy between those who enjoy the benefits and those who bear the risk.
g) Potential of mobilization. which is to be understood as violation of individual, social and cultural interests. and values generating social conflicts and psychological reactions by individuals and groups who feel inflicted by the risk consequences. The potential of mobilization could also result from perceived inequities in the distribution of risk and benefits.
h) The difficulty in establishing appropriate (representative) performance measures (observable quantities on a high system level).

For the uncertainties various types of uncertainty analyses can be used. The risk analysis is to be seen as an uncertainty analysis of future observable quantities and events. The analysis structures the analysts' knowledge on the risks and vulnerabilities; on what the consequences of a hazard could be. Normally a number of scenarios could possibly develop from a specific hazard. There are uncertainties present, and these uncertainties need to be assessed and described. To assess the uncertainties about the possible consequences we may adopt a classification system as follows, in addition to using probabilities to express the uncertainties related to what will be the outcomes of the various observables ([9]:

a) Insight into phenomena and systems, which describes the current knowledge and understanding about the underlying phenomena and the systems being studied.
b) Complexity of technology, which describes the level of complexity of the technology being used, reflecting, for example, that new technology will be utilized.
c) The ability to describe system performance based on its components.
d) The level of predictability, from changes in input to changes in output.

e) Experts' competence. which describes the level of competence of the experts' being used, seen in relation to for example the best available knowledge.
f) Experience data, which describes the quality of the data being used in the analysis.
g) Time frame, which describes the time frame of the project and how it influences the uncertainties.
h) Vulnerability of system, which describes the vulnerability of the system to, *e.g.*, weather conditions and human error. A more robust technical system is more likely to withstand strains and this can reduce the likelihood of negative consequences.
i) Flexibility, which describes the flexibility of the project and how this affects the uncertainty, *e.g.,* a high flexibility allows adjustments to the project plan as more information becomes available and this can reduce the potential for negative outcomes.
j) Level of detail, which describes the need for more detailed analysis to reduce the uncertainty about the potential consequences.

The uncertainty aspects a)–j) can be assessed qualitatively, and discussed, or assessed by some type of categorizations and scoring system, describing the analysts' and the experts' knowledge and judgments.

These assessments provide a basis for comparing alternatives and making a decision.

Compared to standard ways of presenting risk results, this basis is much more comprehensive. In addition, sensitivity analyses are to be performed. Of course, the depth of the analysis will be a function of the decision situation, the risks involved and the resources to be used. The full risk descriptions as outlined above would be used only in special situations, requiring a comprehensive decision support basis.

Various kinds of risk matrices can be informative. The traditional risk matrix showing combinations of possible consequences (with some defined categories) and associated probabilities is applicable in many cases.

The starting point for risk characterizations would normally be the expected value, as the expected value would give accurate predictions when considering a large population of activities. We take a portfolio perspective. We must, however, distinguish between different attributes (lives, economic quantities, *etc*.); it is not straightforward to transform all attributes to one common scale.

Let C_i be the consequence (outcome) of an activity for a given period of time, for example next year, for a specific attribute i. We may as an example let C_i denote the outage time. In the analysis we relate Ci to relevant initiating events (sources), and we may then write

$$C_i = \Sigma_j C_i \, I(A_j),$$

where, A_j denotes the source j and $I(A_j)$ is the indicator function which equals 1 if the event A_j occurs and 0 otherwise. We see that $C_i \, I(A_j)$ expresses the outage time as a result of the source j.

Hence by probability calculus, it follows that the total expected number of fatalities equals [40]

$$EC_i = \Sigma_j E[C_i \, I(A_j)] = \Sigma_j E[C_i \,|A_j] \, P(A_j),$$

i.e., the expected outage time equals the probability of event j multiplied by the expected outage time given this event, summed over all events j.

This gives a starting point for evaluating the risks. We determine $P(A_j)$ and $E[C_i \,|A_j]$ and multiply these together. We may do this by using crude categories of probability and expected values, for example consequence categories as presented in Step 1.

The consequence categories can also be based on features such as ubiquity and persistence, see list above.

This analysis is carried out for all relevant attributes, and a summarizing index can be defined based on the scores assigned for each attribute. One possible way of doing this is simply to sum the various contributions (or take an average), assuming that corresponding categories have been defined for all relevant attributes.

The derived expected values constitute a basis for the risk evaluation. However, we need to see beyond the expected values. The reason is that the actual outcomes could deviate strongly from the

expected values. The analyses are based on judgments, made by some experts, a number of assumptions and suppositions are made, and there could be large uncertainties associated with the phenomena being studied. The fact that such deviations may occur, should also be taken into account. A way of doing this is to use the approach presented in [41].

The basis is the expected value of the form EC, and we develop a matrix with components EC and U, where U are factors that could give significant deviations between the expected value and the outcomes. Such factors include the following (see. Steps 4 and 5 above)

- Vulnerabilities
- Complexity in technology
- Complexity in organizations
- Available information
- Time horizon
- Level of manageability. To what extent is it possible to control and reduce the uncertainties, and obtain desired outcomes? Some risks are more manageable than others, meaning that the potential for reducing the risk is larger for some risks compared to others. By proper uncertainty management, we seek to obtain desirable consequences.
- The thoroughness, *etc*., of the analysis. What are the experts' competences, seen in relation to the best available knowledge? Do we have available relevant experience data? To what extent would further analysis reduce the uncertainties about the potential consequences?

For each factor we give a score and based on this an index could be established.

An alternative approach for summarizing the risk picture is to use a classification scheme in line with the one used by [39] (see also [14]), and based on the system developed in [38]. The scheme is based on seven categories to represent the various combinations of the characteristics included in the scheme. The categories are based on the two main characteristics of risk; possible consequences and uncertainty about the consequences. The seven categories show a tendency of increased risk, as well as increased level of authority involvement, stakeholders' implications and treatment of societal values. The arrow in Table 44.1 is to be read as a tendency, not as a strict increasing value.

Table 44.1. Risk context classification scheme

	Category		Level of risk
	Potential consequences	**Uncertainty of consequences**	
1	Small	S/M/L	Low
2	Moderate	Small	
3	Moderate	Moderate	
4	Moderate	Large	⇓
5	Large	Small	
6	Large	Moderate	
7	Large	Large	High

Following our definition of risk, a low degree of uncertainty does not necessarily mean a low risk, and a high degree of uncertainty does not necessarily mean a high level of risk. This is important. As risk is defined as the combination of possible consequences and the associated uncertainties (quantified by probabilities), any judgment about the level of risk, needs to consider both dimensions. For example, consider a case where only two outcomes are possible, 0 and 1, corresponding to 0 and 1 fatality, and the decision alternatives are A and B, having uncertainty (probability) distributions (0.5,0.5), and (0.0, 1.0), respectively. Hence for alternative A there is a higher degree of uncertainty than for alternative B. However, considering both dimensions, we would, of course, judge alternative B to have the highest risk as the negative outcome 1 is certain to occur.

The intention of the classification scheme is to make a basis for characterization, discussion and management of risk. By this we mean that the scheme should be considered as a starting point or a basis for further handling of risk, and not as a "tool" that provide decisions of its own.

44.3.1 Research Challenges

We see the need for research in many areas, in particular related to the development of theories and methodologies for

a) structuring risk decision problems and processes,
b) analyzing vulnerabilities and risks, and
c) managing risks and making decisions under uncertainty.

Different types of classification systems for characterizing decision situations and risks are presented in the literature, see *e.g.*, [9], [38],[39] [41] and [42]. Such classification systems are designed for structuring decision problems and guide decision makers on how to deal with the problems, reflecting different stakeholder perspectives, risk assessments results, *etc*. Classification as such is not the aim, but classification can be a point of departure for clarification of relationships and behavioral patterns, *etc*. We have applied aspects of these classification systems in our framework, but further research is needed to determine the most suitable schemes.

We believe that the Bayesian approach using subjective probabilities to express uncertainties provides a sound basis for risk analyses. With limited and partially relevant data, Bayesian inference is needed. However, Bayesian analysis is not straightforward for complex problems, see, *e.g.*, [14], and further research is required. Underlying this issue is the possible use of the "rational consensus" perspective [43] on uncertainties in risk management. Is it possible to obtain a "neutral" view of uncertainties that is acceptable for all stakeholders and thereby confine stakeholder discourse to questions to preference only? To what extent is it possible to balance such a "neutral" view and the pure subjectivist position, that probability is a subjective, personal construction?

Another issue is the need for development of appropriate problem decomposition methods for risk and vulnerability identification and analysis (including extending the logic modeling techniques such as fault trees and event trees to include influence diagrams), essential for capturing different dimensions of complex risk issues. The work must be seen in relation to existing approaches such as the I-Risk [44], ARAMIS [45], the BORA projects [31], the SAM approach [47], and the HCL method [48], which develop methodology for operational risk analysis including analysis of the performance of safety barriers, with respect to technical systems as well as human [45], operational, and organizational factors.

To support the development of suitable theories and methods, there is a need for further research exploring the inter-relationships between economic theory, decision analysis, and safety science:

- How and to what extent factors other than the economic performance measures are and should be given weight, and how these factors can be measured and/or handled. Special focus should be on factors not directly related to a firms' core activity such as social responsibility and potential loss of goodwill.
- To what extent risk reducing measures are external effects for agents (firms and organizations), in the sense that they are beneficial for society but not necessarily for the agent in question.
- How these issues are influenced by public regulations and actions.

Some of the areas that need to be addressed relate to portfolio theory and safety management, the use of the cautionary and precautionary principles, the interactions between government and firms, and incentives in decision processes.

In such a context one also needs to be aware of the link between productivity growth and risk. Good risk management is generally claimed to be productivity enhancing, while the opposite is true of poorly designed schemes. If this is so, why is not risk management a higher priority both in theory and practice?

References

[1] ISO Risk management vocabulary. ISO/IEC Guide 73, 2002.
[2] Aven T, Vinnem JE. Risk management, with applications from the offshore oil and gas industry. Springer, New York, 2007.
[3] ISO Risk management – General guidelines for principles and implementation of risk management. N 5. Preliminary version, 2005.

[4] Henley EJ, Kumamoto H. Reliability engineering and risk assessment. Prentice Hall, New York, 1981.
[5] Modarres M. What every engineer should know about reliability and risk analysis. Marcel Dekker, New York, 1993.
[6] Mol T. Productive safety management. Elsevier, London, 2003.
[7] Thomen, JR. Leadership in safety management. Wiley, New York, 1991.
[8] OHSAS Occupational health and safety management systems – Guidelines for the implementation of OHSAS 18001. ISBN:0580331237, 2000.
[9] Sandøy M, Aven T, Ford D. On integrating risk perspectives in project management. Risk Management: An International Journal 2005; 7:7–21.
[10] Pidgeon NF, Beattie J. The psychology of risk and uncertainty. In: Calow P, editor. Handbook of environmental risk assessment and management. Blackwell Science, London, 1998: 289–318.
[11] Okrent D, Pidgeon N. Special issue on risk perception versus risk analysis. Reliability Engineering and System Safety 1998; 59.
[12] Douglas, E.J. Managerial economics: Theory, practice and problems, 2nd ed. Prentice Hall, Englewood Cliffs, NJ, 1983.
[13] Rosa EA. Metatheoretical foundations for post-normal risk. Journal of Risk Research 1998; 1: 15–44.
[14] Aven T. Foundations of risk analysis: A knowledge and decision-oriented perspective. Wiley, New Yrok, 2003.
[15] Cabinet office risk: Improving government's capability to handle risk and uncertainty. Strategy Unit Report, UK, 2002; 7.
[16] Vinnem JE, Aven T, Husebø T, Seljelid J, Tveit O. Major hazard risk indicators for monitoring of trends in the Norwegian offshore petroleum sector. Reliability Engineering and System Safety 2006; 91:778–791.
[17] Levy H, Sarnat M. Capital investment and financial decisions. Fourth edition. Prentice Hall, New York, 1990.
[18] Lindley DV. Making decisions. Second edition. Wiley, New York, 1985.
[19] Watson SR, Buede DM. Decision synthesis. Cambridge University Press, Cambridge, 1987.
[20] Clemen RT, Reilly T. Making hard decisions with decision tools. Imprint Pacific Grove, Duxbury/ Thomson Learning, 2001
[21] Gonzalez R, Wu G. On the shape of the probability weighting function. Cognitive Psychology 1999; 38:129–166.
[22] Tversky A, Kahneman D. Advances in prospect theory: Cumulative representation of uncertainty. Journal of Risk and Uncertainty 1992; 5: 297–323.
[23] Brealey R, Myers S. Principles of corporate finance. McGraw-Hill, New York, 1996.
[24] Abrahamsen EB, Aven T, Vinnem JE, Wiencke HS. Safety management and the use of expected values. Risk, Decision and Policy 2005; 9:347–358.
[25] Bodie Z, Kane A, Marcus AJ. Investments. Fifth edition. Irwin McGraw-Hill, Chicago, 2002.
[26] Vinnem JE. Offshore risk assessment. Kluwer, London, 1999.
[27] Abrahamsen EB, Aven T, Sandøy M. A note on the concept of risk aversion in safety management. Journal of Risk and Reliability 2006; 220:69–71.
[28] Hanley N, Spash CL. Cost-benefit analysis and the environment. Edward Elgar, Cheltenham, 1993.
[29] Copeland TE, Weston JF. Financial theory and corporate policy. Addison-Wesley, Reading, MA, 1988.
[30] EAI. Risk and uncertainty in cost benefit analysis. A toolbox paper for the Environmental Assessment Institute. http://www.imv.dk., 2006.
[31] Aven, T. On the precautionary principle, in the context of different perspectives on risk. Risk Management: An International Journal 2006; 8:192–205.
[32] Lofstedt RE. The precautionary principle: Risk, regulation and politics. Transactions IchemE 2003; 81:36–43.
[33] Sandin P. Dimensions of the precautionary principle. Human and Ecological Risk Assessment 1999; 5:889–907.
[34] HSE. Reducing risks, protecting people: HSE's decision-making. HSE Books, London, 2001.
[35] Aven T, Vinnem JE. On the use of risk acceptance criteria in the offshore oil and gas industry. Reliability Engineering and System Safety 2005; 90:15–24.
[36] HSE. Offshore installations (safety case) regulations 2005 regulation 12 demonstrating compliance with the relevant statutory provisions. Offshore Information Sheet No. 2/2006.
[37] Aven T, Abrahamsen EB. On the use of cost-benefit analysis ALARP processes. International Journal of Performability Engineering. 2007; 3(3):345–353.
[38] Renn O, Klinke A. A New approach to risk evaluation and management: Risk-based precaution-based and discourse-based strategies. Risk Analysis 2002; 22(6):1071–1094.
[39] Kristensen V, Aven T, Ford D. A new perspective on Renn & Klinke's approach to risk evaluation

and risk management. Reliability Engineering and System Safety 2006; 91:421–432.
[40] Aven T. A unified framework for risk and vulnerability analysis and management covering both safety and security. Reliability Engineering and System Safety. 2007; 92:745–754.
[41] Aven T, Vinnem JE, Wiencke HS. A decision framework for risk management. Reliability Engineering and System Safety. 2006; 92:433–448.
[42] Rasmussen J. Risk management in a dynamic society. Safety Science 1997; 27:183–213.
[43] Cooke R. Experts in uncertainty. Oxford University Press, New York, 1991.
[44] Papazoglou IA, Bellamy LJ, Hale AR, Aneziris ON, Post JG, Oh JIH. I-Risk: Development of an integrated technical and Management risk methodology for chemical installations. Journal of Loss Prevention in the Process Industries 2003; 16:575–591.
[45] Duijm NJ, Goossens L. Quantifying the influence of safety management on the reliability of safety barriers. Journal of Hazardous Materials 2006; 130(3): 284–292.
[46] Aven T, Hauge S, Sklet S, Vinnem JE. Methodology for incorporating human and organizational factors in risk analyses for offshore installations. International Journal of Materials and Structural Reliability 2006; 4:1–14.
[47] Paté-Cornell EM, Murphy DM. Human and management factors in probabilistic risk analysis: The SAM approach and observations from recent applications. Reliability Engineering and System Safety 1996; 53:115–126.
[48] Røed W, Mosleh A, Vinnem JE, Aven T. On the use of hybrid causal logic method in offshore risk analysis. Reliability and System Safety; to appear in 2008.

45

Risk Governance: An Application of Analytic-deliberative Policy Making

Ortwin Renn

University of Stuttgart and Dialogik gGmbH
Seidenstr. 36, 70174 Stuttgart
Germany

Abstract: This chapter introduces an integrated analytic framework for risk governance which provides guidance for the development of comprehensive assessment and management strategies to cope with risks, in particular at the global level. The framework integrates scientific, economic, social and cultural aspects and includes the effective engagement of stakeholders. The concept of risk governance comprises a broad picture of risk: not only does it include what has been termed "risk management" or "risk analysis", it also looks at how risk-related decision-making unfolds when a range of actors is involved, requiring co-ordination and possibly reconciliation between a profusion of roles, perspectives, goals, and activities.

45.1 Introduction

The framework's risk process breaks down into three main phases: "pre-assessment", "appraisal", and "management." A further phase, comprising the "characterization" and "evaluation" of risk, is placed between the appraisal and management phases and, depending on whether those charged with the assessment or those responsible for management are better equipped to perform the associated tasks, can be assigned to either of them—thus concluding the appraisal phase or marking the start of the management phase. The risk process has "communication" as a companion to all phases of addressing and handling risk and is itself of a cyclical nature. However, the clear sequence of phases and steps offered by this process is primarily a logical and functional one and will not always correspond to reality. The chapter will address in particular the role of public participation and stakeholder involvement.

45.2 Main Features of the IRGC Framework

The framework offers a conceptual framework to guide decisions about risks that we shall accept or refuse. This framework has been developed under the direction of the International Risk Governance Council (IRGC) and published as IRGC White Paper [1]. The concept of risk governance comprises a broad picture of risk: not only does it include what has been termed "risk management" or "risk analysis", it also looks at how risk-related decision-making unfolds when a range of actors is

involved, requiring co-ordination and possibly reconciliation between a profusion of roles, perspectives, goals and activities. Indeed, the problem-solving capacities of individual actors, be they government, the scientific community, business players, NGOs, or civil society as a whole, are limited and often unequal to the major challenges facing society today. Risks such as those related to increasingly violent natural disasters, food safety, or critical infrastructures call for co-ordinated effort amongst a variety of players beyond the frontiers of countries, sectors, hierarchical levels, disciplines and risk fields. Finally, risk governance also illuminates a risk's context by taking account of such factors as the historical and legal background, guiding principles, value systems, and perceptions as well as organizational imperatives.

The framework offers two major innovations to the risk field: the inclusion of societal context and a new categorization of risk-related knowledge.

- *Inclusion of societal context:* Besides the generic elements of risk assessment, risk management and risk communication, the framework gives equal importance to contextual aspects which are either directly integrated in a model risk process consisting of the above as well as additional elements or else form the basic conditions for making any risk-related decision. Contextual aspects of the first category include the structure and interplay of the different actors dealing with risks, how these actors may differently perceive those risks, and what concerns they have regarding their likely consequences. Examples of the second category include policy-making or regulatory style, as well as the socio-political impacts prevalent within the entities and institutions having a role in the risk process, their organizational imperatives, and the capacity needed for effective risk governance. Linking context with risk governance, the framework reflects the important role of risk-benefit evaluation and the need for resolving risk-risk tradeoffs.
- *Categorization of risk-related knowledge:* The framework also proposes a categorization of risk which is based on the different states of knowledge about each particular risk, distinguishing between "simple", "complex", "uncertain" and "ambiguous" risk problems. The characterization of a particular risk depends on the degree of difficulty of establishing the cause-effect relationship between a risk agent and its potential consequences, the reliability of this relationship, and the degree of controversy with regard to both what a risk actually means for those affected and the values to be applied when judging whether or not something needs to be done about it. Examples of each risk category include, respectively, known health risks such as those related to smoking, the failure risk of interconnected technical systems such as the electricity transmission grid, atrocities such as those resulting from the changed nature and scale of international terrorism, and the long-term effects and ethical acceptability of controversial technologies such as nanotechnologies. For each category, a strategy is then derived for risk assessment, and risk management, as well as the level and form of stakeholder participation, supported by proposals for appropriate methods and tools.

Beyond these component parts the framework includes three major value-based premises and assumptions:

- First, the framework is inspired by the conviction that both the "factual" and the "socio-cultural" dimensions of risk need to be considered if risk governance is to produce adequate decisions and results. While the factual dimension comprises physically measurable outcomes and discusses risk in terms of a combination of potential, both positive and negative, consequences and the probability of their occurrence, the socio-cultural dimension

emphasises how a particular risk is viewed when values and emotions come into play.

- The second major premise concerns the inclusiveness of the governance process, which is seen as a necessary, although not sufficient, prerequisite for tackling risks in both a sustainable and acceptable manner and consequently imposes an obligation to ensure the early and meaningful involvement of all stakeholders and, in particular, civil society.
- A third major premise involving values is reflected in the framework's implementation of the principles of "good" governance: beyond the crucial commitment to participation, these principles include transparency, effectiveness and efficiency, accountability, strategic focus, sustainability, equity and fairness, respect for the rule of law, and the need for the chosen solution to be politically and legally realizable as well as ethically and publicly acceptable.

45.3 The Core of the Framework: Risk Governance Phases

The framework's risk process, or risk handling chain is illustrated in Figure 45.1. It breaks down into three main phases: "pre-assessment", "appraisal", and "management". A further phase, comprising the "characterization" and "evaluation" of risk, is placed between the appraisal and management phases and, depending on whether those charged with the assessment or those responsible for management are better equipped to perform the associated tasks, can be assigned to either of them—thus concluding the appraisal phase or marking the start of the management

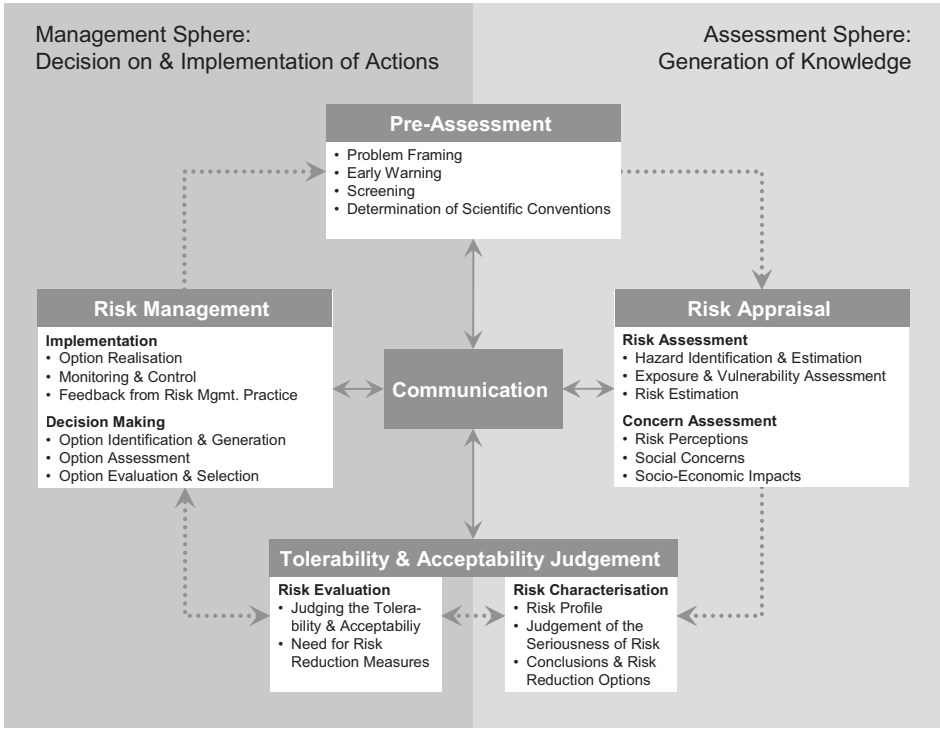


Figure 45.1. IRGC risk governance framework

phase. The risk process has "communication" as a companion to all phases of addressing and handling risk and is itself of a cyclical nature. However, the clear sequence of phases and steps offered by this process is primarily a logical and functional one and will not always correspond to reality.

The purpose of the *pre-assessment* phase is to capture both the variety of issues that stakeholders and society may associate with a certain risk and also existing indicators, routines, and conventions that may prematurely narrow down, or act as a filter for, what is going to be addressed as risk. What counts as a risk may be different for different groups of actors. The first step of pre-assessment, risk framing, therefore places particular importance on the need for all interested parties to share a common understanding of the risk issue(s) being addressed or, otherwise, to raise awareness amongst those parties of the differences in what is perceived as a risk. For a common understanding to be achieved, actors need both to agree with the underlying goal of the activity or event generating the risk and to be willing to accept the risk's foreseeable implications on that very goal. A second step of the pre-assessment phase, early warning and monitoring, establishes whether signals of the risk exist that would indicate its realization. This step also investigates the institutional means in place for monitoring the environment for such early warning signals.

The third step, pre-screening, takes up and looks into the widespread practice of conducting preliminary probes into hazards or risks and, based on prioritization schemes and existing models for dealing with risk, of assigning a risk to pre-defined assessment and management "routes", The fourth and final step of pre-assessment selects major assumptions, conventions and procedural rules for assessing the risk as well as the emotions associated with it.

The objective of the *risk appraisal* phase is to provide a knowledge base for the societal decision on whether or not a risk should be taken and, if so, how the risk can possibly be reduced or contained. Risk appraisal thus comprises a scientific assessment of both the risk and of questions that stakeholders may have concerning its social and economic implications.

The first component of risk appraisal, risk assessment, seeks to link a potential source of harm, a hazard, with likely consequences, specifying probabilities of occurrence for the latter. Depending on the source of a risk and the organizational culture of the community dealing with it, many different ways exist for structuring risk assessment. Despite such diversity, three core steps can be identified. These are: the identification and, if possible, estimation of the hazard; an assessment of related exposure and/or vulnerability; and an estimation of the consequent risk. The latter step, risk estimation, aggregates the results of the first two steps and states, for each conceivable degree of severity of the consequence(s), a probability of occurrence. Confirming the results of risk assessments can be extremely difficult, in particular when cause-effect relationships are hard to establish, when they are instable due to variations in both causes and effects and when effects are both scarce and difficult to understand.

Depending on the achievable state and quality of knowledge, risk assessment is thus confronted with three major challenges that can best be summarized using the risk categories outlined above—"complexity", "uncertainty", and "ambiguity". For a successful outcome to the risk process and, indeed, to overall risk governance, it is crucial that the implications of these challenges are made transparent at the conclusion of risk assessment and throughout all subsequent phases. Equally important to understanding the physical attributes of the risk is detailed knowledge of stakeholders' concerns and questions—emotions, hopes, fears, apprehensions—about the risk as well as likely social consequences, economic implications, and political responses. The second component of risk appraisal, concern assessment, thus complements the results from risk assessment with insights from risk perception studies and interdisciplinary analyses of the risk's (secondary) social and economic implications.

The most controversial phase of handling risk, *risk characterization and evaluation,* aims at judging a risk's acceptability and/or tolerability. A risk deemed "acceptable" is usually limited in terms of negative consequences so that it is taken

on without risk reduction or mitigation measures being envisaged. A risk deemed "tolerable" links undertaking an activity which is considered worthwhile for the value-added or benefit it provides with specific measures to diminish and limit the likely adverse consequences. This judgment is informed by two distinct but closely related efforts to gather and compile the necessary knowledge which, in the case of tolerability, must additionally support an initial understanding of required risk reduction and mitigation measures. While risk characterization compiles scientific evidence based on the results of the risk appraisal phase, risk evaluation assesses broader value-based issues that also influence the judgment. Such issues, which include questions such as the choice of technology, societal needs requiring a given risk agent to be present, and the potential for substitution as well as for compensation, reach beyond the risk itself and into the realm of policy-making and societal balancing of risks and benefits.

The *risk management* phase designs and implements the actions and remedies required to tackle risks with an aim to avoid, reduce, transfer, or retain them. Risk management thereby relies on a sequence of six steps which facilitates systematic decision-making. To start with, and based on a reconsideration of the knowledge gained in the risk appraisal phase and while judging the acceptability and/or tolerability of a given risk, a range of potential risk management options is identified. The options are then assessed with regard to such criteria as effectiveness, efficiency, minimization of external side effects, sustainability, *etc*. These assessment results are next complemented by a value judgment on the relative weight of each of the assessment criteria, allowing an evaluation of the risk management options. This evaluation supports the next step in which one (or more) of the of risk management options is selected, normally after consideration of possible trade-offs that need to be made between a number of second-best options. The final two steps include the implementation of the selected options and the periodic monitoring and review of their performance.

Based on the dominant characteristic of each of the four risk categories ("simple", "complex", "uncertain", "ambiguous") it is possible to identify specific safety principles and, consequently, design a targeted risk management strategy (*see* Table 45.1). "Simple" risk problems can be managed using a "routine-based" strategy which draws on traditional decision-making instruments and best practice, as well as time-tested trial-and-error. For "complex" and "uncertain" risk problems, it is helpful to distinguish the strategies required to deal with a risk agent from those directed at the risk-absorbing system: complex risks are thus usefully addressed on the basis of "risk-informed" and "robustness-focused" strategies, while uncertain risks are better managed using "precaution-based" and "resilience-focused" strategies. Whereas the former strategies aim at accessing and acting on the best available scientific expertise and at reducing a system's vulnerability to known hazards and threats by improving its buffer capacity, the latter strategies pursue the goal of applying a precautionary approach in order to ensure the reversibility of critical decisions and of increasing a system's coping capacity to the point where it can withstand surprises. Finally, for "ambiguous" risk problems the appropriate strategy consists of a "discourse-based" strategy which seeks to create tolerance and mutual understanding of conflicting views and values with a view to eventually reconciling them.

The remaining element of the risk process is *risk communication*, which is of major importance throughout the entire risk handling chain. Not only should risk communication enable stakeholders and civil society to understand the rationale of the results and decisions from the risk appraisal and risk management phases when they are not formally part of the process, but it should also help them to make informed choices about risk, balancing factual knowledge about risk with personal interests, concerns, beliefs, and resources, when they are themselves involved in risk-related decision-making. Effective risk communication consequently fosters tolerance for conflicting viewpoints and provides the basis for their means for assessing and managing risk and related concerns. Eventually, risk communication can have a major impact on how well society is

Table 45.1. Risk characteristics and their implications for risk management

Knowledge Characterization	Management Strategy	Appropriate Instruments	Stakeholder Participation
1 "Simple" risk problems	*Routine-based:* (tolerability/ acceptability judgment)	→ Applying "traditional" decision-making – Risk-benefit analysis – Risk-risk trade-offs	Instrumental discourse
	(risk reduction)	– Trial and error – Technical standards – Economic incentives – Education, labeling, information – Voluntary agreements	
2 Complexity-induced risk problems	*Risk-informed:* (risk agent and causal chain)	→ Characterizing the available evidence – Expert consensus seeking tools: - Delphi or consensus conferencing - Meta analyses - Scenario construction, *etc*. – Results fed into routine operation	Epistemological discourse
	Robustness-focused: (risk absorbing system)	→ Improving buffer capacity of risk target through: – Additional safety factors – Redundancy and diversity in designing safety devices – Improving coping capacity – Establishing high reliability organisations	
3 Uncertainty-induced risk problems	*Precaution-based:* (risk agent)	→ Using hazard characteristics such as persistence, ubiquity, *etc*., as proxies for risk estimates Tools include: – Containment – ALARA (as low as reasonably achievable) and ALARP (as low as reasonably possible) – BACT (best available control technology), *etc*.	Reflective discourse
	Resilience-focused: (risk absorbing system)	→ Improving capability to cope with surprises 1. Diversity of means to accomplish desired benefits 2. Avoiding high vulnerability 3. Allowing for flexible responses 4. Preparedness for adaptation	

prepared to cope with risk and to react to crises and disasters. Risk communication has to perform these functions both for the experts involved in the overall risk process—requiring the exchange of information between risk assessors and managers, between scientists and policy makers, between academic disciplines, and across institutional barriers—and for the "outside world" of those affected by the process.

45.4 Stakeholder Involvement and Participation

The classification of risk knowledge into four risk classes, *i.e.*, simple, complex, uncertain, and ambiguous, suggests some generic suggestions for participation:

- *Simple risk problems:* For making judgments about simple risk problems, a sophisticated approach to involve all potentially affected parties is not necessary. Most actors would not even seek to participate, since the expected results are more or less obvious. In terms of cooperative strategies, an "*instrumental discourse"* among agency staff and directly affected groups (such as product or activity providers and immediately exposed individuals), along with enforcement personnel is advisable. One should be aware, however, that often risks that appear simple turn out to be more complex, uncertain or ambiguous than originally assessed. It is therefore essential to revisit these risks regularly and monitor the outcomes carefully.
- *Complex risk problems:* The proper handling of complexity in risk appraisal and risk management requires transparency over the subjective judgments and the inclusion of knowledge elements that have shaped the parameters on both sides of the cost-benefit equation. Resolving complexity necessitates a discursive procedure during the appraisal phase, with a direct link to the tolerability and acceptability judgment and risk management. Input for handling complexity could be provided by an "*epistemological discourse"* aimed at finding the best estimates for characterising the risks under consideration. This discourse should be inspired by different science camps and on the participation of experts and knowledge carriers. They may come from academia, government, industry, or civil society, but their legitimacy to participate is their claim to bring new or additional knowledge to the negotiating table. The goal is to resolve cognitive conflicts. Exercises such as Delphi, Group Delphi, and consensus workshops would be most advisable to serve the goals of an epistemological discourse.
- *Risk problems due to high unresolved uncertainty:* Characterising risks, evaluating risks, and designing options for risk reduction pose special challenges in situations of high uncertainty about the risk estimates. How can one judge the severity of a situation when the potential damage and its probability are unknown or highly uncertain? In this dilemma, risk managers are well advised to include the main stakeholders in the evaluation process and ask them to find a consensus on the extra margin of safety in which they would be willing to invest in exchange for avoiding potentially catastrophic consequences. This type of deliberation, called *reflective discourse* relies on a collective reflection about balancing the possibilities for over- and under-protection. If too much protection is sought, innovations may be prevented or stalled; if we go for too little protection, society may experience unpleasant surprises. The classic question of "how safe is safe enough" is replaced by the question of "how much uncertainty and ignorance are the main actors willing to accept in exchange for some given benefit". It is recommended that policy-makers, representatives of major stakeholder groups, and scientists take part in this type of discourse. The reflective discourse can take different forms: round tables, open space forums, negotiated rule-making exercises, mediation, or mixed advisory committees including scientists and stakeholders.
- *Risk problems due to high ambiguity:* If major ambiguities are associated with a risk problem, it is not enough to

demonstrate that risk regulators are open to public concerns and address the issues that many people wish them to address. In these cases the process of risk evaluation needs to be open to public input and new forms of deliberation. This starts with revisiting the question of proper framing. Is the issue really a risk problem or is it in fact an issue of lifestyle and future vision? The aim is to find consensus on the dimensions of ambiguity that need to be addressed in comparing risks and benefits and on balancing the pros and cons. High ambiguities require the most inclusive strategy for participation, since not only directly affected groups but also those indirectly affected have something to contribute to this debate. Resolving ambiguities in risk debates requires a "participative discourse", a platform where competing arguments, beliefs, and values are openly discussed.

The opportunity for resolving these conflicting expectations lies in the process of identifying common values, defining options that allow people to live their own vision of a "good life" without compromising the vision of others, finding equitable and just distribution rules when it comes to common resources, and activating institutional means for reaching common welfare so all can reap the collective benefits instead of a few (coping with the classic commoners' dilemma). Available sets of deliberative processes include citizen panels, citizen juries, consensus conferences, ombudspersons, citizen advisory commissions, and similar participatory instruments.

Categorizing risks according to the quality and nature of available information on risk may, of course, be contested among the stakeholders. Who decides whether a risk issue can be categorized as simple, complex, uncertain or ambiguous? It seems prudent to have a screening board perform this challenging task. This board should consist of members of the risk and concern assessment team, of risk managers and key stakeholders (such as industry, NGOs, and representatives of related regulatory or governmental agencies). The type of discourse required for this task is called design discourse. It is aimed at selecting the appropriate risk and concern assessment policy, defining priorities in handling risks, organising the appropriate involvement procedures, and specifying the conditions under which the further steps of the risk handling process will be conducted.

Figure 45.2 provides an overview of the different requirements for participation and stakeholder involvement for the four classes of risk problems and the design discourse. As is the case with all classifications, this scheme shows an extremely simplified picture of the involvement process. In addition to the generic distinctions shown in the graph below, it may for instance be wise to distinguish between participatory processes based on risk agent or risk absorbing issues. To conclude these caveats, the purpose of this scheme is to provide general orientation and explain a generic distinction between ideal cases rather than to offer a strict recipe for participation.

45.5 Wider Governance Issues: Organizational Capacity and Regulatory Styles

The white paper also addresses wider governance issues pertinent to the context of a risk and the overall risk process, thus acknowledging the many different pathways that different countries—or, indeed, risk communities—may pursue for dealing with risk. The discussion of these wider issues begins with an assessment of the very notion of "risk governance" which builds on the observation that collective decisions about risks are the outcome of a "mosaic" of interactions between governmental or administrative actors, science communities, corporate actors, and actors from civil society at large, many of the interactions taking place in and relevant to only individual parts of the overall process. The interplay of these actors has various dimensions, including public participation, stakeholder involvement, and the formal (horizontal and vertical) structures within which it occurs. The white paper additionally investigates organizational prerequisites for

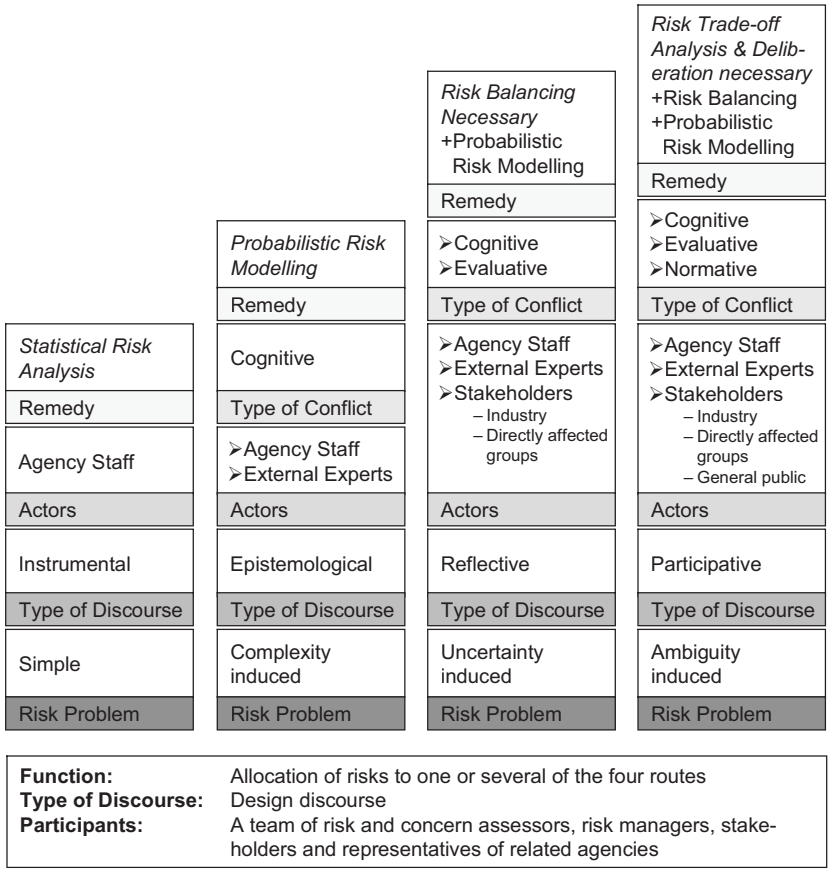


Figure 45.2. The risk management escalator and stakeholder involvement (from simple *via* complex uncertain to ambiguous phenomena)

effective risk governance, which are at the crossroads of the formal responsibilities of actors and their capability and authority to successfully fulfill their roles, and makes a very short case for risk education. The organizational prerequisites are summarized under the term "institutional and organizational capacity" and include both intellectual and material "assets", "skills", and also the framework of relations, or "capabilities", required to make use of the former two.

Risk management depends, however, not only on scientific input. It rather rests on three components: *systematic knowledge, legally prescribed procedures, and social values.* Even if the same knowledge is processed by different risk management authorities, the prescriptions for managing risk may differ in many aspects (*e.g.*, with regard to inclusion and selection rules, interpretative frames, action plans for dealing with evidence, and others). National culture, political traditions, and social norms furthermore influence the mechanisms and institutions for integrating knowledge and expertise in the policy arenas. Policy analysts have developed a classification of governmental styles that address these aspects and mechanisms. While these styles have been labeled inconsistently in the literature, they refer to common procedures in different settings. They are summarized in Table 45.2.

Table 45.2. Characteristics of policy making styles

Style	Characteristics	Risk Management
1 *Adversarial approach*	• open to professional and public scrutiny • need for scientific justification of policy selection • precise procedural rules • oriented towards producing informed decisions by plural actors	• main emphasis on mutual agreements on scientific evidence and pragmatic knowledge • integration of adversarial positions through formal rules (due process) • little emphasis on personal judgment and reflection on the side of the risk managers • stakeholder involvement essential for reaching communication objectives
2 *Fiduciary approach (patronage)*	• closed circle of ”patrons” • no public control, but public input • hardly any procedural rules • oriented towards producing faith in the system	• main emphasis on enlightenment and background knowledge through experts • strong reliance on institutional in-house “expertise” • emphasis on demonstrating trustworthiness • communication focused on institutional performance and “good record”
3 *Consensual approach*	• open to members of the “club” • negotiations behind closed doors • flexible procedural rules • oriented towards producing solidarity with the club	• reputation most important attribute • strong reliance on key social actors (also non-scientific experts) • emphasis on demonstrating social consensus • communication focused on support by key actors
4 *Corporatist approach*	• open to interest groups and experts • limited public control, but high visibility • strict procedural rules outside of negotiating table • oriented towards sustaining trust to the decision making body	• main emphasis on expert judgment and demonstrating political prudence • strong reliance on impartiality of risk information and evaluation • integration by bargaining within scientifically determined limits • communication focused on fair representation of major societal interests

- The *adversarial approach* is characterized by an open forum in which different actors compete for social and political influence in the respective policy arena. The actors in such an arena use and need scientific evidence to support their position. Policy-makers pay specific attention to formal proofs of evidence because their decisions can be challenged by social groups on the basis of insufficient use or negligence of scientific knowledge. Risk management and communication is essential for risk regulation in an adversarial setting because stakeholders demand to be informed and consulted. Within this socio-political context, stakeholder involvement is mandatory.

- In the *fiduciary approach*, the decision-making process is confined to a group of patrons who are obliged to make the "common good" the guiding principle of their actions. Public scrutiny and involvement of the affected public are alien to this approach. The public can provide input to and arguments for the patrons but is not allowed to be part of the negotiation or policy formulation process. The system relies on producing faith in the competence and the fairness of the patrons involved in the decision making process. Advisors are selected according to national prestige or personal affiliations. In this political context, stakeholder involvement may even be regarded as a sign of weakness or a diffusion of personal accountability.
- The *consensual approach* is based on a closed circle of influential actors who negotiate behind closed doors. Social groups and scientists work together to reach a predefined goal. Controversy is not present and conflicts are reconciled on a one-to-one basis before formal negotiations take place. Risk communication in this context serves two major goals: it is supposed to reassure the public that the "club" acts in the best interest of the public good and to convey the feeling that the relevant voices have been heard and adequately considered. Stakeholder participation is only required to the extent that the club needs further insights from the affected groups or that the composition of the club is challenged.
- The *corporatist approach* is similar to the consensual approach but is far more formalized. Well-known experts are invited to join a group of carefully selected policy-makers representing the major forces in society (such as employers, unions, churches, professional associations, and environmentalists). Similar to the consensual approach, risk communication is mainly addressed to the outsiders: they should gain the impression that the club is open to all "reasonable" public demands and that it tries to find a fair compromise between public protection and innovation. Often the groups represented within the club are asked to organize their own risk management and communication programs as a means of enhancing the credibility of the whole management process.

Although these four styles cannot be found in pure form in any country they form the backdrop of socio-political context variables against which specific risk governance structures are formed and operated. These structures, along with the individual actors' goals and the institutional perspectives they represent, would need more specific attention and, for the time being, are difficult to classify further.

45.6 Conclusions

The IRGC risk governance framework described in this chapter has been designed, on one hand, to include enough flexibility to allow its users to do justice to the wide diversity of risk governance structures and, on the other hand, to provide sufficient clarity, consistency, and unambiguous orientation across a range of different risk issues and countries.

The framework includes a comprehensive risk handling chain, breaking down its various components into three main phases: "pre-assessment", "appraisal", and "management". The two intermediate and closely linked stages of risk characterization and evaluation have been placed between the appraisal and management phases and can be assigned to either of them, depending on the circumstances: if the interpretation of evidence is the guiding principle for characterising risks, then risk and concern assessors are probably the most appropriate people to handle this task; if the interpretation of underlying values and the selection of yardsticks for judging acceptability are the key problems, then risk managers should be responsible. In an ideal setting, however, this task of determining a risk's acceptability should

be performed in a joint effort by both assessors and managers.

At any rate, a comprehensive, informed, and value-sensitive risk management process requires a systematic compilation of results from risk assessment, risk perception studies and other context-related aspects as recommended and subsumed under the category of risk appraisal. Risk managers are thus well advised to include all the information related to the risk appraisal in evaluating the tolerability of risks and in designing and evaluating risk reduction options. The crucial task of risk communication runs parallel to all phases of handling risk: it assures transparency, public oversight, and mutual understanding of the risks and their governance.

Reference

[1] International Risk Governance Council: White Paper on Risk Governance: Towards an integrative framework. IRGC: Geneva: Further references are listed in this document, 2005.

46

Maintenance Engineering and Maintainability: An Introduction

Krishna B. Misra

RAMS Consultants, Jaipur, India

Abstract: Maintenance is another important aspect of system performance after reliability. There are several facets of maintenace management, and in this introductory chapter we would like to have these surveyed. Broadly speaking, maintenance is the process of maintaining equipment in its operational state either by preventing its transition to a failed state or by restoring it to an operational state following a failure. This leads to various types of maintenace activities that can be planned to realize the objective of maitenance, such as preventive, predictive, or corrective. Recent developments in maintenance engineering and management are also discussed in this chapter.

46.1 Introduction

The Oxford dictionary meaning of "to maintain" is to "cause something to continue" or "to keep something in existence at the same level". Therefore, maintenance does extend the useful life of a product or system. Also the necessity of "upkeep" arises to oppose the forces of degradation. Degradation can be due to deterioration caused by the environment to which the equipment is exposed or due to deterioration of equipment arising from its actual use. From British Standard BS4778-3.1:1991 or BS3811:1993 (or MIL-STD-721B), one settles for the definition of maintenance as: "Maintenance is the process of maintaining an item in an operational state by either preventing a transition to a failed state or by restoring it to an operational state following failure". Therefore the primary aim of a maintenance system is to prolong the state of functioning of equipment or a system by not allowing it to deteriorate in condition.

There is an interesting philosophical paper by Rao [25], who postulates 14 laws for the subject of universal theory of failures. But more interesting and of concern to maintenance engineers is the section on the anatomy of failures in this article, which makes it an interesting reading, particularly in relation to fault and failure and the warning time to failures, as catastrophic failures do not occur instantaneously without a warning time. This allows us to take proactive measures to avoid them.

46.1.1 Maintenance System

An effective maintenance system involves three separate entities of work, *viz.*, maintenance, inspection, and verification, which can be done by different groups in the same company or different companies specifically subcontracted for the purpose.

Maintenance task: Maintenance tasks [12, 13, 15] are generally of two types, *viz.*, *planned* and

unplanned. *Planned maintenance* can be *preventive* or *corrective* (including deferred maintenance), whereas *unplanned maintenance* is mainly *corrective,* which includes any *emergency maintenance*. Again the preventive maintenance can be *scheduled maintenance*, and the other can be based on the condition of the equipment—known as *condition-based maintenance*. Therefore, the form of the maintenance can be:

1. *Pre-planned maintenance:* This includes early maintenance tasks such as cleaning, greasing, lubricating, zero-setting, and recording key measurements. This is often conducted by non-maintenance staff and observed equipment deterioration that cannot be corrected will be reported to regular maintenance staff. This is also called first-line maintenance.
2. *Planned maintenance:* This is also known as scheduled maintenance, and its timing and scope are both known in advance.
3. *Shutdown maintenance:* It is a planned maintenance but is carried out when production or plant is shut down.
4. *Breakdown maintenance:* This is carried out when equipment fails to meet its desired function. This may involve repairs, replacements, or adjustments as considered necessary.
5. *Emergency maintenance:* This is carried out only when either inspection or breakdown maintenance has identified its necessity.

Inspection: All plant machines, equipment, and structures are subjected to regular inspection scheduled to detect performance or safety problems and to ensure that all items receive necessary maintenance.

Verification: Verification is a process, not a measurement, and it has two primary objectives:

- To check that the maintenance work is being done, and
- To confirm that maintenance standards have not been compromised.

Verification is usually performed by or supplemented by (in addition to in-house verification) a third party (to be completely impartial or fair). One of the key parameters to verify if the maintenance was up to standard is to determine the availability of the system, since the maintenance is result dependent and the test lies in *effectiveness* rather than *efficiency*.

46.1.2 Maintenance Philosophy

Based on the timing and the work contents involved in the maintenance task, different maintenance philosophies [13, 15] can be put in the following categories, *viz.:*

1. *Timing known, content known:* preplanned maintenance (PPM), planned shutdowns, routine inspections, and scheduled change-outs fall in this category;
2. *Timing known, content unknown:* statutory surveys, third party inspections, and condition-based maintenance;
3. *Timing unknown, content known:* anticipated maintenance work, contingency work awaiting shutdown, and run to destruction; and
4. *Timing unknown, content unknown:* breakdown maintenance, immediate repairs arising from inspection, and run to failure.

From the point of view of work management, activities falling in category 1 are most welcome and those in category 4 are least welcome. It is always advantageous to shift work to a more manageable category. By using an effective maintenance regime, the intention should be to keep category 4 as empty as possible. It is worthwhile to observe that in "run to failure" in which equipment is run until it fails and then is repaired, work content is unknown. However, in the "run to destruct" category, in which equipment is run till it fails and then is discarded, a replacement is required; thus work content is known. Also, by careful evaluation of maintenance histories and shutdown programs, the timing uncertainty in category 3 can be minimized. Such work followed by full job preparation can provide a fast response when a situation finally requires it. Also, the requirements in category 2 can be anticipated with care once operations are routinely established.

Out of all maintenance work, preplanned maintenance (category 1) is most widely used, but it is often argued that this method requires work to be done that is not necessary since it is done on the basis of calendar irrespective of machine condition.

In run to destruct (category 3), the equipment is usually used until it fails and is discarded or replaced. The work requires switching off the machinery or isolating it, then removing or replacing the old unit and connecting the new unit. Work management is straightforward, as technical content is all known.

Breakdown maintenance (category 4) is simple and can be applied quickly with limited resources and information, but work arising from an unexpected breakdown is difficult to manage and may involve high costs. Breakdown maintenance is not safe and may sometimes involve danger to life.

46.1.3 Maintenance Scope Changed with Time

Over the past several decades starting from the pre-World War II period, the concept and scope of maintenance has changed considerably—more than any other management discipline. These changes can basically be attributed to the advent of more complex designs of systems requiring new maintenance techniques.

This is resulting in change in the concept of maintenance organization and responsibilities. There is a tremendous increase in the number, size and variety of physical assets (plants, equipment, and buildings) which have maintained.

There is a rapidly growing awareness of product quality affecting maintenance activities and of the extent to which equipment failure can affect safety and the environment, coupled with the requirement of achieving high plant availability at reduced costs. With the increase in complexity and sophistication, along with organizational changes, the maintenance work carried out today itself is undergoing changes. These changes are testing the attitudes and skills to their limits in all sectors of industry. Management and engineers [7, 11] are beginning to adopt completely new ways of thinking and strategies towards maintenance, so that they can evaluate them sensibly and apply those likely to be useful to them and their companies. In fact, the changes that have taken place during this period are well documented by Moubray [14], who split this period into three distinct periods (which Moubray [14] calls *generations I, II and III*) and are summarized in Table 46.1.

During the period 1930 to 1950 (first generation), industry was not so mechanized, so downtime did not matter much to them. Maintenance was conducted only when equipment actually failed. The work was more "fix-it" than maintenance. Moreover, most equipment was simple and was usually over-designed, which made

Table 46.1. Changing Maintenance Requirement over Time

Characterized by	Period		
	From 1930 to 1950	From 1950 to 1975	From 1975 to present
Expectations of maintenance	Failure-based maintenance	Higher plant availability Longer equipment life Lower costs	Higher plant availability and reliability Greater safety and better quality Environmentally friendly Longer life Greater cost effectiveness
Pattern of failure	Old age failures	Infant mortality and old age	Various patterns of hazard rates
Maintenance techniques	Reactive maintenance Fix it when it broke	Calendar-based maintenance Scheduled overhauls Systems for planning and controlling work -Big but slow computers	Condition monitoring Design for reliability and maintainability Hazard studies Small but fast computers Expert systems Multi-skilling and teamwork

it reliable and easy to repair. This meant that the prevention of equipment failure was not considered a priority by the management. Therefore there was no need for systematic maintenance [2, 14] of any sort beyond occasional cleaning, servicing, and lubrication. Obviously, the skill requirement was also lower than it is today.

But things changed dramatically during and after World War II. Wartime pressure accelerated mechanization, and by the 1950s machines had become more complex and numerous. As industry became more and more dependent on them, the concern for the uptime of these machines became the priority of the industry, and the management considered it advantageous and in their interest to prevent equipment failures. This became the rallying point for the concept of preventive maintenance with the realization that performing regular maintenance and refurbishment could keep equipment operating longer between failures. This came to be known as *periodic maintenance* or *calendar based maintenance* or *preventive maintenance* (PM). The goal was to have most of the equipment able to operate most of the time until the next scheduled maintenance outage. This approach provided more control over the maintenance schedule; however, the system was still susceptible to failure between maintenance cycles.

However, even by the 1960s, this concern was mainly confined to overhauls of equipment done at fixed intervals. Then as the cost of maintenance increased, the necessity of maintenance planning and control systems was felt. In fact, the amount of capital tied up in fixed assets increased enormously, and the necessity of maximizing the life of these assets was felt more acutely.

As downtime reduced output, it affected the productive capability of physical assets by increasing operating costs and interfering with customer service, and by the 1970s this was further aggravated by the worldwide move towards just-in-time systems—where reduced stocks of work-in-progress meant that quite small breakdowns could stop the whole plant. Instead of waiting for a machine to fail before working on it, or performing maintenance on a machine regardless of its condition (PM), the idea of performing maintenance on equipment only when it indicates impending faults—*predictive maintenance* (PdM)—took hold, and the idea of using PdM to perform maintenance on machines only when they exhibit signs of mechanical failure had come to be known as *condition-based maintenance* (CBM). This process of maintenance has become more *proactive* than *reactive* in maintenance tasking.

In recent times, however, with extensive automation, reliability, availability, and safety of production processes have become serious issues, since failures can affect our ability to sustain satisfactory quality standards and may have severe environmental consequences. This necessitates the integrity of our physical assets, which goes beyond cost and becomes a matter of survival for the organization. Today, as the dependence on physical assets is growing, in order to secure maximum return on their investment they must be kept in efficiently working condition for as long as possible.

Moreover, the cost of maintenance is also rising, in absolute terms and as a proportion of total expenditure. In some industries, it is the highest or the second highest element of operating costs. Consequently, in the last thirty years it has moved from almost nowhere to the top of the cost control priority. Also it is becoming apparent that there is less and less connection between the operating age of assets and how likely they are to fail.

In recent times, there has been tremendous growth in maintenance concepts and techniques. The change in emphasis includes:

- Decision support tools, such as hazard studies, failure modes and effects analyses, and expert systems.
- New maintenance techniques such as condition monitoring or CMMS.
- Designing equipment with emphasis on reliability and maintainability.
- A major shift in organizational thinking towards participation, teamwork and flexibility.

A major challenge facing maintenance people nowadays is not only to learn what these techniques are, but to decide which are worthwhile and which are not in their own organizations. If we

make the right choices, it is possible to improve asset performance and at the same time contain and even reduce the cost of maintenance. If we make the wrong choices, new problems are created while existing problems only get worse.

In fact, RCM provides a framework which enables users to respond to these challenges quickly and easily. Since every physical asset is put into service because someone wants it to do something, they expect it to fulfill a specific function or functions. When an asset is maintained, obviously the state we wish to preserve is the one in which it continues to do whatever its users want it to do.

Of late, emphasis is being placed on *core business* by several major companies of the world, and under this thinking companies are transferring previously in-house functions to external specialist companies. Use of experts or specialists, as well as choosing *in-house* teams *on-site*, accommodated teams, or *manned-up* technicians brought from outside for the completion of a job, is becoming routinely common these days. Subcontracting for maintenance jobs is also becoming quite common in the globalizing world of trade these days, and the number and size of companies engaged in maintenance work is growing very fast.

46.2 Approaches to Maintenance

There are several approaches to maintenance, and different approaches are applicable based on the expected use and maintenance schedule of an item. Economic considerations are tightly related to maintenance and the system lifecycle; it is clear that failure to consider a design's effects on maintenance, and *vice versa*, can have adverse effects on profit. Therefore, design and maintenance must be simultaneously planned in order to ensure an efficient and cost-effective operation over the life of a product.

Maintenance has been categorized based on the nature and purpose of the maintenance work and on its frequency. Generally, there are four types of maintenances in use, *viz.*, preventative, corrective, predictive, and fault-finding.

Maintenance can also be classified according to the degree to which the maintenance work is carried out to restore the equipment relative to its original state. This leads to the following categorization:

Perfect maintenance is maintenance which restores the equipment to *as good as new* condition.

Minimal maintenance results in equipment having the same failure rate as it had before the maintenance action was initiated. This is also called the *as bad as old* state.

Imperfect maintenance is maintenance in which the equipment is not restored to *as good as new*, but to a relatively *younger* state (a state in between *as good as new* and *as bad as old*).

Worse maintenance: This type of maintenance results (unintentionally) in an increase of the equipment's failure rate or actual age but does not result in breakdown.

Worst maintenance: This type of maintenance results (unintentionally) in the equipment's breakdown.

In the foregoing classification, maintenance can be preventive (PM) or corrective (CM), and accordingly the PM or CM would be belong to one of the above categories. These have been discussed nicely in several texts [20, 22, 24].

In this handbook, we have included Chapters 47 and 48 on some aspects of maintenance modeling and optimization as well as on the trends on maintenance technology and management.

46.2.1 Preventive Maintenance

Preventative maintenance, as the name itself indicates*,* is a schedule of planned maintenance aimed to prevent future breakdowns and failures of a system that is functioning properly. In fact, preventive maintenance is performed to prevent equipment failure before it actually occurs and to keep the equipment working and/or extend the life of the equipment. Usually, it is performed on equipment on a regular basis based on the expected life of the equipment, and the frequency of the maintenance is generally constant. Preventive maintenance is a schedule of planned maintenance actions aimed at the prevention of breakdowns and failures, since the primary objective of preventive maintenance is to prevent the failure of equipment before it actually occurs. For example, lubrication of mechanical systems is done after a certain

number of operating hours, or replacement of lightning arresters in jet engines after a certain number of lightning strikes. It is designed to enhance equipment reliability by replacing worn components before they actually fail. Preventive maintenance activities include equipment checks, partial or complete overhauls at specified periods, oil changes, lubrication, and so on. In addition, workers can record equipment deterioration, so they know which worn out parts to replace or repair before they can cause system failure. Technological advances in tools for inspection and diagnosis have enabled even more accurate and effective equipment maintenance. The ideal preventive maintenance program would prevent *all* equipment failures before they occur.

Preventive maintenance [17] is a logical alternative if the following two conditions are satisfied:

- The equipment in question has an increasing hazard rate. In other words, the hazard rate of the equipment increases with time, implying a wear-out situation. Preventive maintenance of a component that is assumed to have an exponential distribution (which implies a constant failure rate) does not make sense!
- The overall cost of the preventive maintenance action must be less than the overall cost of a corrective action. The overall cost for a corrective action includes ancillary tangible and/or intangible costs such as downtime costs, loss of production costs, lawsuits over the failure of a safety-critical item, loss of goodwill, *etc*.

As stated earlier, if the unit has an increasing failure rate, then a carefully designed preventive maintenance program may improve system availability. Otherwise, the costs of preventive maintenance might actually outweigh the benefits. It is important to make it explicitly clear that if a component has a constant failure rate (*i.e*., defined by an exponential distribution), then preventive maintenance of the component will have no effect on the component's failure occurrences.

In fact, the objective of a good preventive maintenance program is to either minimize the overall costs (or downtime, *etc*.) or to meet reliability-availability goals. In order to achieve this, an appropriate interval of time must be determined for the scheduled maintenance. One way to do that is to use the optimum age replacement model, where the model satisfies the conditions mentioned previously, *viz.*:

- The unit is exhibiting behavior associated with a wear-out mode. That is, the failure rate of the unit is increasing with time, and
- The cost for planned replacements is significantly less than the cost for unplanned replacements.

Long-term benefits of preventive maintenance include:

- Improved system reliability.
- Decreased cost of replacement.
- Decreased system downtime.
- Better spares inventory management.

Thus long-term effects and cost comparisons usually favor preventive maintenance over performing maintenance actions only when the system fails.

Maintenance Policies

The literature is full of numerous maintenance models [22] that have been presented by researchers using various assumptions and cost structures, but all of them can be broadly categorized under certain maintenance policies. These policies, however, are with regard to a single piece of equipment.

Age-dependent PM policy: Under this policy, PM is carried out at some predetermined age or repaired (CM) upon failure. PM or CM can be perfect, minimal or imperfect.

Periodic PM policy: Under this policy, the equipment's PM is carried out at fixed time intervals regardless of its failure history.

Failure limit policy: Under this policy, the PM is performed only when the failure rate (or some index of performance) reaches a predetermined level, and the intervening failures are repaired when they occur.

Sequential PM policy: Under this policy, the equipment's PM is carried out at unequal time intervals, which become shorter with age.

Repair limit policy: Under this policy, two cases arise, *viz.*, *repair cost limit policy* and *repair time limit policy*. Under the former, the repair cost is assessed when the equipment fails and repair is performed only if the repair cost is less than a predetermined limit. Otherwise the equipment is replaced. Under the repair time limit policy, the limit is set on the repair time instead of cost.

Repair number counting policy: Under this policy, the equipment is replaced at kth failure and the first $(k-1)$ failures are removed by minimal repair. Upon replacement the process repeats.

As said before, the foregoing maintenance policies were applicable to a single piece of equipment with an increasing failure rate. Recently, there has been increasing interest in multi-equipment maintenance models. In fact, maintenance of a multi-equipment system differs from that of single equipment in that there exists *economic* or *failure* dependence. Due to the former, the PM of non-failed subsystems can be performed at reduced cost while the failed subsystems are being repaired. In case of failure dependence or *correlated failures*, failure of one of the subsystems may affect the functioning of other subsystems. In case of a system with a number of subsystems or equipment, the following maintenance policies are applicable.

Group maintenance policy: Under this policy, there are three different cases:

- *T-age group replacement policy:* The units or equipment are replaced when the system is of age T.
- *m-failure group policy:* This calls for a system inspection after m failures have occurred.
- *m-failure* and *T-age policy*: This policy combines the advantages of the *m*-failure and *T-age* policies and calls for a group replacement when the system is of age T or when m failures have occurred, whichever comes first. This policy requires inspection at either the fixed age T or the time when m failures have occurred, whichever comes first. At inspection, all failed equipment are replaced with new ones and all functioning equipment are serviced so that they become as good as new.

Opportunistic maintenance policies: Under this policy in multi-component systems, it is possible to do PM of non-failed equipment at a reduced additional cost while failed equipment is being repaired. There are many variations in strategy under this category.

Warranty models: Maintenance needs to be incorporated in the warranty models so that if warranted equipment fails, the failed components that caused the equipment failure will be replaced, and in addition PM can be carried out to reduce the chances of failure in the future. Therefore, warranty policies [23] with integrated PM should be preferable.

It can easily be shown that corrective replacement costs increase as the replacement interval increases. In other words, the less often we perform PM, the higher will be the corrective costs. Obviously, the longer we let a piece of equipment operate, its failure rate increases to a point where it is more likely to fail, thus requiring corrective action. However, just the opposite is true for the preventive replacement costs. The longer we wait to perform PM, less shall be the costs. On the other hand, if we do PM too frequently, the cost would go up. If we combine both costs, it is easy to realize that there is an optimum point that minimizes the costs. In other words, one must strike a balance between the risk (costs) associated with a failure, while maximizing the PM interval analysis.

Generally, preventive maintenance (PM) is considered beneficial, but it must be mentioned that there are risks of equipment failure and human errors committed while performing PM, just as in any other maintenance operation. This logic dictates that it would cost more for regularly scheduled downtime and maintenance than it would normally cost to operate equipment until repair is absolutely necessary. This may be true for some components; however, one should compare not only the costs but the long-term benefits and savings associated with preventive maintenance. Without preventive maintenance, for example, costs for lost production time from unscheduled equipment breakdown will be incurred. Also, preventive maintenance results in savings due to an increase of effective system service life.

There are several excellent references available for preventive maintenance modeling and analysis, but the books by Nakagawa [20], Wang and Pham [22], and Jardine and Tsang [24] stand out distinctly. The book by Jardine and Tsang [24] presents different optimal replacement policies and models and spare parts provisioning, besides discussing optimal inspection policies under various conditions. Additionally, capital equipment replacement decisions and maintenance resource requirements are also presented. Nakagawa and Wang and Pham [20, 22] describe perfect and imperfect preventive maintenance models and several optimum preventive maintenance policies: inspection models, with different types of units such as standby and storage, and different types of failures such as extended failures (catastrophic, partial or degraded) and intermittent failures. Faults revealed or unrevealed are also considered. In fact, both these books present an up-to-date status of various models that have been available so far.

In this handbook, we have included Chapter 49 by Nakagawa on replacement and preventive maintenance models.

46.2.2 Predictive Maintenance

Predictive maintenance (PdM) or condition-based maintenance (CBM) is carried out only after collecting and evaluating enough physical data on performance or condition of equipment, such as temperature, vibration, particulate matter in oil, *etc.*, by performing periodic or continuous (on-line) equipment monitoring. Analysis is then performed on the collected data to prepare an appropriate maintenance plan. PdM technologies used to collect information of equipment conditions can include infrared, acoustic (partial discharge and airborne ultrasonic), corona detection, vibration analysis, sound level measurements, oil analysis, and other specific online tests.

The basic aim in PdM [18] is to perform maintenance at a scheduled point in time when the maintenance activity is most cost effective but before the equipment fails in service. Most PdM inspections are performed while equipment is in service, thereby minimizing disruption of normal system operations. This type of maintenance is generally carried out on mechanical systems where historical data is available for validating the performance and maintenance models for the systems and the failure modes are known. Predictive maintenance (PdM) helps determine the condition of in-service equipment in order to predict when maintenance should be performed. The *predictive* component of the term predictive maintenance comes from the goal of predicting the future trend of the equipment's condition. This approach uses principles of statistical process control to determine at what point in the future maintenance activities will be appropriate.

In fact, for condition monitoring or predictive techniques, any relevant means is acceptable to determine equipment conditions and to predict potential failure. This may even include the use of the human senses (appearance, sound, feel, smell, *etc.*), machine performance monitoring, and statistical process control techniques. Other sophisticated technologies used in monitoring include:

- Vibration measurement and analysis,
- Acoustic emission (ultrasonics),
- Oil analysis,
- Infrared thermography, and
- Motor current analysis.

These will be explained in some detail in the following paragraphs.

46.2.2.1 Vibration Measurement and Analysis

This technology owes its popularity to the fast Fourier transform (FFT) technique developed in 1964, when spectrum analyzers became available that could be used with special transducers to measure machine vibrations. When portable FFT-based data collectors became available around 1980, the use of vibration as a tool for machinery fault diagnosis underwent a sea of change and found applications in the petrochemical, electrical power, paper, and other process industries. Today, the *on-line vibration analysis system* (rather than portable analyzers) is widely used for monitoring vibrations with piezoelectric accelerometers as vibration probes and computer-based specialized

data acquisition systems for collecting, storing, and archiving FFT data. The on-line dynamic vibration monitoring system enables mechanical fault detection at the earliest detectable time. But the system installation costs are usually high because of the capital cost of the hardware as well as the installation labor. However, vibration analysis is the most appropriate solution on high speed rotating machines and can be the most expensive part of a PdM program. It still remains the most widely used method for detecting rubbing in rotating machines such as electrical power generating turbines through changes in amplitude and phase of the 1X (rotating frequency) vibration component.

46.2.2.2 Acoustic Emission

Acoustic emission (AE), particularly for bearing diagnosis, is becoming quite indispensable. Sometimes acoustical analysis may also be done at sonic or ultrasonic levels. Sonic technology is useful for mechanical equipment, whereas ultrasonic equipment is useful for detecting electrical problems. Ultrasonic testing is a relatively new predictive technology. It is capable of detecting sounds that lie outside the human hearing range and are indicators of failing mechanical conditions. As a result, ultrasonic testing has become an essential part of a predictive maintenance program. Ultrasonic inspections can help detect leaking gases or fluids in heat exchangers, compressors, and valves. This technique not only locates leaks in steam traps and valves, but can also be helpful in detecting certain electrical faults, such as arching and corona.

46.2.2.3 Oil Analysis

Oil analysis in relevant cases can be a more reliable technique in predictive maintenance. The early use of oil analysis dates back to the early 1940s by the railway companies in the western United States, where technicians used simple spectrographic equipment and physical tests to monitor locomotive engines. When diesel locomotives came in use, oil analysis practices by railways became very frequent. By the 1980s, oil analysis formed the basis of condition-based maintenance (CBM) in most railways in North America.

Lubricating oil contains a good deal of information about the envelope in which it circulates. Wear of metallic parts, for example, produces a lot of minute particles which are carried by the lubricant. Wear means the loss of solid material due to the effects of friction of contacting surfaces. These small metal particles can give information about the machine parts that are wearing, and they can be detected by various methods such as atomic emission spectrometry. Determination of larger particles can be done using optical or electronic microscopy, or ferrography. The acidity of oil can indicate whether the oil has been oxidized as a result of operation at high temperature, if there is a high percentage of moisture, or due to oil having been in service for a long period.

The viscosity of the oil is also an important parameter and must conform to the requirements of the machine. The loss of alkalinity of the oil indicates whether the oil is in contact with some inorganic acids such as sulfuric or nitric acid. Oil undergoes destructive changes in property when it is subjected to oxygen, combustion gasses, and high temperatures. Viscosity change, as well as additive depletion and oxidation, occur to degrade the oil.

Several methods are used to analyze oil condition and contamination. These analyses may include spectrometry, viscosity analysis, dilution analysis, water detection, acid number assessment, base number assessment, particle counting, and microscopy. Oil and wear particle analysis is a combination of spectrometric, ferrographic, and filter analysis. Oil and wear particle analysis can detect abnormal wear modes, particularly in aviation systems, long before the wear can cause any serious damage.

Oil data modeling and analysis can be of great help in fault detection procedures, and we have included Chapter 50 in this handbook on this aspect.

46.2.2.4 Infrared (IR) Thermography

Infrared (IR) thermography is used to detect temperature changes in bearings and shafts. IR thermographic analysis detects abnormal temperatures

that may signify corrosion, damaged wiring, loose connections, and/or insulation breakdown and hot spots. Infrared monitoring and analysis help reduce unexpected failures in electrical and mechanical equipment (from high to low speed equipment). This vital information can alert in advance of the catastrophic failures and is considered a cost-effective technique of monitoring.

46.2.2.5 Motor Current Analysis

Motor diagnostic technologies have become more prevalent through the 1990s to recent times. The technologies include: motor circuit analysis (MCA) and motor current signature analysis (MCSA) applied to both energized and de-energized electric motor systems. Motor current analysis techniques are non-intrusive methods of detecting mechanical and electrical problems in motor driven rotating equipment. Motor current monitor (MCM) uses the electric motor of the equipment as a sensor, and the information about the equipment is extracted from the line current of the motor. The MCM first learns the motor-based system for a certain period of time and acquires and processes the motor data. These data are stored in an internal database, and a reference model, which consists of parameters and their means and standard deviations, is established. Now during actual monitoring, the data being acquired is compared with the results stored in the internal database. If the acquired data is significantly different from the reference model, it indicates a fault level that is determined by the magnitude and the time duration of the difference. This approach is used for diagnostics of electrical equipment, especially those with rotating components. The main advantages lie in its being a noninvasive methodology for diagnosing health and operations of motor-actuated valves, generators, electric motors, and other types of electric equipment.

With new, inexpensive RF components and integration techniques, along with advances in microprocessor technology, it is possible to provide an economic solution for wirelessly monitoring motor operating parameters – such as temperature, vibration, current, *etc*. – for all classes of motors. The generic technology will find applications in areas where motors, pumps, gearboxes or drive chains need to be monitored on a continuous basis, such as fluids processes in chemical industries, motor generator systems, serial trunk conveyor systems, and general line production in manufacturing industries.

Motor current signature analysis (MCSA) is a technique used to determine the operating condition of AC induction motors without interrupting production. MCSA techniques can be used in conjunction with vibration and thermal analysis to confirm key machinery diagnostic decisions.

MCSA works on the principle that induction motor circuits can actually be viewed as a transducer. By clamping a Hall Effect current sensor on either the primary or the secondary circuit, fluctuations in motor current can be observed. It has been observed that if a high resistance exists, (for example due to broken rotor bars) harmonic fluxes are produced in the air gap. These fluxes induce current components in the stator winding that can cause modulation of the supply current at ± the number of motor poles times slip. Available signal processing techniques can help extract the modulating frequency and represent the amplitude relationship of modulating frequency to line frequency. This relationship allows one to estimate the presence and severity of the defect.

46.2.2.6 Problems in Condition Monitoring

Although many organizations use sophisticated techniques for condition monitoring these days, there are still many problems that remain unresolved. For example, it is known that the main determinant of the frequency of condition monitoring is the lead time to failure (or PF interval), which is from the time at which an incipient failure can first be detected until functional failure occurs. For example, in the case of a bearing, the PF interval is the time interval from when overall bearing vibration levels reach an alarming limit until the bearing seizes completely. In order to be sure that the failure is detected prior to functional failure; the bearing must be monitored at a frequency less than the PF Interval. But the PF interval can hardly be determined accurately. For instance, in the case of a bearing, the PF Interval may vary depending on the type of bearing

installed, the severity of its operating cycle, the type of lubrication applied, ambient temperature conditions, the type of failure detected, and many other factors.

Even today, the PF Interval can only be approximately estimated. Any error tends to be on the conservative *(i.e.,* too frequent) side. However, there are cases of bearing failures that have occurred undetected, despite these bearings being monitored at these conservative frequencies. However, the situation is not that bad, as smart sensor technology will greatly reduce the complexity of linking the outputs of these sensors to current process control systems, and thereby more and more equipment can be monitored continuously, -on-line, -and the control room operators will be able to assess quickly and easily, the current condition of the bearings, or alignment, or balance, or gears on a particular machine. Several expert systems for fault diagnosis are available today. However, at present these expert systems are still essentially rule-based systems, and like all rule-based systems, the results are only as good as the rules that have been established within the system.

Several articles have been published on the performance monitoring of steam turbines, using measurements of temperature, pressure, and power output and along with other techniques to determine the turbine condition, and the specific faults that may require attention. In the future, it is likely that this type of monitoring will be used on large diesel engines, pumps, and other sophisticated equipment. It is expected that sophisticated techniques such as ultrasonic flow measurement will be used to assist with the cost-effective application of performance monitoring techniques to a wider range of equipment.

The major trends one may expect to see in the future are:

- The development of smart sensors and other low-cost on-line monitoring systems that will permit the cost-effective continuous monitoring of important equipment.
- The increasing provision of built-in vibration sensors as standard features in large motors, pumps, turbines and other large equipment items.
- Increasingly sophisticated condition monitoring software, with rapidly developing *expert* diagnosis capabilities.
- Increasing integration and acceptance for interfacing condition monitoring software with CMMS and process control software.
- More focus on the applications of condition monitoring technologies to improve equipment reliability and performance, rather than just to predict component failure.
- A reduction in the cost of applying condition monitoring technologies.

In any case, adoption of PdM in the maintenance of equipment can result in substantial cost savings and higher system reliability. This approach offers cost savings over routine or time-based preventive maintenance because tasks are performed only when considered necessary, in contrast to time and/or operation count based maintenance where a piece of equipment gets maintained whether it needs it or not. Time based maintenance is labor intensive and ineffective in identifying problems that develop between scheduled inspections, and it is not cost effective.

46.2.3 Failure-finding Maintenance

Failure-finding maintenance involves checking a (quiescent) part of a system to see if it is still working. This is often performed on subsystems of a system dedicated to safety—protective devices. This is an important type of maintenance check because failures in safety systems can have more catastrophic effects if other parts of the system fail. Inspections are usually carried out in order to uncover hidden failures (also called dormant failures). In general, no maintenance action is performed on the component during an inspection unless the component is found failed, in which case a corrective maintenance action can be initiated.

46.2.4 Corrective Maintenance

Corrective maintenance consists of the actions taken to restore a failed piece of equipment or system to an operational state. This maintenance usually involves replacing or repairing the

component that caused the failure of the overall system. Corrective maintenance is performed at unpredictable intervals because a component's failure time is not known *a priori*. The equipment becomes operational after corrective maintenance or repairs have been performed. Corrective maintenance is actually carried out in three steps:

1. *Diagnosis of the fault*: The repairmen must take time to locate the fault or failed parts or otherwise satisfactorily assess the cause of the equipment or system failure.
2. *Repair or replacement of faulty components:* Once the cause of equipment failure has been established, action is taken to remove the cause, usually by replacing or repairing the components that caused the equipment to fail.
3. *Verification of the repair action:* After the faulty components have been repaired or replaced, the repair crew must verify that the system is again successfully operating.

The total time taken to repair the equipment is called *downtime,* as during this period the equipment is not available or operating. By the same logic, the *uptime* of an equipment or system is the time during which it is available or operating. Further, *cycle time* is the sum of *uptime* and *downtime*. In fact a repairable or maintainable equipment or system undergoes several such cycles of *operating state* and *down state* during its entire *lifetime* before it is discarded or decommissioned.

Actually, downtime is the sum of the *administrative time*, the *logistic time* and the *actual repair time*. The *administrative time* is the time spent in organizing repairs and is the time lost between the occurrence of a fault and the instant repairmen initiate repair action. This should exclude the *logistic time,* which is the portion of down time during which the repair activity is suspended or delayed on account of non-availability of spare parts or replacements.

The *actual repair time* or *active repair time* is the time during which the repairmen are working on the equipment to effect the repairs. This time is in fact the sum of the time to locate the fault or faults and for identification of the fault, fault correction time, and finally the time taken for testing and recommissioning the equipment. It is apparent that *repairability*, which is the probability that the equipment or system will be restored to operable state within a specified *active repair time*, depends on the training and skill of the repair crew as well as on the design of the equipment. For example, the ease of accessibility of components in equipment has a direct effect on the active repair time. However, human factors (covered in Chapter 40 of this handbook) to a large extent govern the duration of active repair time.

46.2.4.1 Maintainability

In contrast with repairability [4, 13, 19], *maintainability* is defined as the probability that the equipment or a unit will be restored to operable state within a specified downtime and depends on all the elements of downtime, *viz., administrative*, *logistic*, and *active repair* times. The downtime is a random variable and has its own distribution, called the repair distribution. If the repair distribution is exponentially distributed and we denote maintainability by $M(t)$, it will be given by

$$M(t) = 1 - e^{-\mu t} \quad ,$$

where μ is the repair rate and t denotes the time to repair (or rather downtime). One can also compute the mean of the repair distribution (MTTR) as:

$$MTTR = 1/\mu \, .$$

If we change the repair distribution to lognormal, Weibull, or gamma, *etc*, the expression for maintainability and mean time to repair would also change. One can find a discussion of repair time distributions in texts like [4, 8, 9, 10].

From the point of view of assessing the performance of such repairable equipment which undergoes several cycles of uptimes and downtimes, a question that naturally arises is what percentage of time on an average (over its entire life) the equipment is available or operating. Thus averaging over a long period of time, one can assess the performance of a repairable or maintained equipment or system, and this average characteristic is called *steady state availability* or *inherent availability* or just *mean uptime ratio*.

46.2.4.2 Availability

Statistically speaking, the uptimes and downtimes are random variables and will have their distributions. Based on these distributions, one can compute *mean uptime* and *mean downtime.* Actually mean uptime reflects how good the inherent design or built-in reliability is, and mean downtime reflects how good the maintainability is. If the steady state availability (SSA) is to be kept high, one should try to design for a high value of mean uptime (MUT) and mean down time (MDT) to be as low as possible, since SSA is the ratio of mean uptime to *mean cycle time* which is the sum of mean uptime and mean downtime. There can be several combinations of MUT and MDT which can offer the same value of availability. Thus availability is dependent on reliability and maintainability, and by clever manipulation one can get the desired value of availability. But the life cycle costs must not be lost sight of while designing a maintained equipment or system.

There are other measures of performance of the maintained equipment, such as *point availability* and *interval availability*.

Point availability is defined as the probability that the equipment or system is available at a given point of time, and *interval availability* is defined as the expected fraction of an interval of specified length that the equipment or system is in an up state. Naturally if the interval becomes very large, the interval availability would approach steady state availability. There are other measures, such as *frequency of failures* and *mean duration of failure*, of interest in the case of maintained systems. The frequency of failures can also be further classified as interval frequency and steady state frequency. The interval frequency of failure is defined as the expected number of times a failure state is encountered in a specified interval, whereas the steady state frequency of failure, or simply the frequency of failure, is defined as the expected number of times a failure state is encountered over a long period of time.

46.2.4.3 Assessment Techniques

For quantitative analysis of performance measures like reliability, availability, or any other measure mentioned in earlier sections, it is necessary to have the following information about the equipment or system:

- *System configuration:* the number of units (identical or non-identical), series, parallel, standby, nature of redundancy (such as warm, cold, or active, *etc*.);
- *Failure and repair data:* failure modes, failure and repair distributions; and
- *Repair strategy:* number of repair crews, independent repair facilities inspection or overhaul schedules, *etc*.

Once the above information is available, one can proceed using any of the following techniques:

- State space approach or Markov method,
- Block diagram approach,
- Conditional probability approach, or
- Monte Carlo approach

Detailed information on these approaches can be found in the references quoted above or in [4]. The Markov method appears to be a more popular technique to analyze maintained systems, although it suffers the disadvantage of the dimensionality of the formulation even for a moderately sized system. However, with fast computing facilities having large memories available, this should not be considered a disadvantage any more. In any case, one can always decompose a large problem into manageably sized problems and also use a combination of solution techniques, rather than using just one technique.

46.2.4.4 Availability Trade-offs

In designing repairable systems, it is generally desired to optimize system availability subject to some cost constraints. Alternatively, a designer may be specified a value of availability to achieve and must determine the optimal pair of mean time between failures (MTBF) and the mean time to repair (MTTR), while minimizing the cost of the system. These formulations are discussed in Chapter 32 of this handbook and the several models are discussed in texts like [1, 8]. However, it is necessary to have some relationship between the variables MTBF and cost and MTTR *versus* cost before any tradeoff can take place. Also, the lower and upper limits on MTBF and MTTR

should be established from practical considerations as well as the state-of-the-art of the available technology. This will help establish the feasibility pairs for MTBF and MTTR.

46.3 Reliability Centered Maintenance

Reliability centered maintenance (RCM) is an approach that helps in deciding what maintenance tasks must be performed at any given point of time. RCM methodology [3, 5 ,6, 16, 21] was initially used in the aviation industry during the 1960s to reduce maintenance costs and to increase safety and reliability. Today it is used in a variety of industries and has benefits applicable to dependable embedded systems. In fact RCM covers a wide range of steps, starting from the product design phase to the deployment and maintenance of a system. The first step in applying RCM techniques is to establish the user's expectations about various characteristics of the system on which RCM will be performed. Then, all the modes that the system can fail in must be identified, and an FMEA or FMECA is performed to identify root causes of these failure modes. From that information, an appropriate combination of types of maintenance is selected, and an appropriate schedule of those maintenance actions is planned. The maintenance plan is then implemented, and data is collected to refine and improve the maintenance schedule.

RCM is a systematic process of preserving a system's or asset's function by selecting and applying effective preventive maintenance (PM) tasks. However, it differs from PM in focusing on function rather than equipment. RCM governs the maintenance policy at the level of plant or equipment type. In general, the concept of RCM is applicable to large and complex systems such as large passenger aircraft, chemical plants, oil refineries, electrical power stations, *etc*.

The main features of RCM are:

- A focus on the preservation of system function;
- Identification of specific failure modes to define loss of this function;
- Prioritizating the failure modes, as not all functions or functional failures have the same importance; and
- Identification of effective and applicable PM tasks that will prevent, and discover or detect the onset of appropriate failure modes based on cost-effective options.

The following process is followed as RCM:

1. The objectives of maintenance with respect to a particular asset are defined by the functions of the asset and its associated desired performance standards.
2. Functional failures are identified.
3. Failure modes which are likely to cause loss of each function are also identified.
4. Failure effects are assessed.
5. Failure consequences are quantified to identify the criticality of failure in terms of the following categories: hidden failure, safety and environmental, operational and non-operational.
6. Functions, functional failures, failure modes, and criticality are analyzed to identify opportunities for improving performance and/or safety.
7. Preventive tasks are established. These may be one of three main types: scheduled on-condition tasks which employ condition-based or predictive maintenance, scheduled restoration, and scheduled discard tasks.

Although the main aim of using RCM is to reduce the total costs associated with system failure and downtime, evaluating the returns from an RCM program solely by measuring its impact on costs may hide many other less tangible benefits such as:

- Improving the system availability,
- Optimizing spare parts inventory,
- Identifying component failure significance and hidden failure modes as well as previously unknown failure scenarios,
- Providing training opportunities for system engineers and operations personnel,
- Identifying areas for potential design enhancement, and
- Providing detailed review and improvement where necessary.

The RCM implementation generally involves high initial costs and quite often results in successful investment, but there have been some cases of unsuccessful implementation, which makes a prior economic evaluation of RCM an important step before it is adopted. In fact, RCM should not be undertaken if the financial benefits cannot be demonstrated to outweigh the involved costs. However, the financial benefits and costs associated with RCM are difficult to assess due to the fact that areas of savings are vague; there are no clear cause and effect relationships in the evaluation process. Costs can more easily be identified than benefits. Costs include initial outlays, primarily for training, and ongoing costs, including maintenance and support personnel and expenditures associated with the maintenance introduced as a result of RCM findings. Benefits can also be identified through a series of steps. Firstly, one can start by identifying the current problems that can be resolved through RCM. Secondly, one can estimate how much improvement would result through the adoption of RCM for the identified problems. Lastly, one should quantify each of the improvements in the larger sense of company's performance (profits, plant availability, personnel cost, *etc*.). When that quantification is done, then the economic benefits of RCM can be evaluated to see if its adoption is justified or not.

The value of RCM lies in the fact that it recognizes that the consequences of failures are far more important than their technical characteristics. In fact, it recognizes that the only reason for doing any kind of proactive maintenance is not to avoid failures *per se*, but to avoid or at least minimize the consequences of failures. In fact, the RCM process classifies these consequences into the following four groups:

- *Hidden failure consequences*: Hidden failures have no direct impact, but they may lead to multiple failures, often with catastrophic consequences. (Often these failures are associated with protective devices which are not fail-safe.)
- *Safety and environmental consequences:* A failure has safety consequences if it has the potential to injure or kill someone. It has environmental consequences if it breaches any environmental standard.
- *Operational consequences:* A failure has operational consequences if it affects production, product quality, customer service, or operating costs or cost of repairs.
- *Non-operational consequences:* Failures belonging to this category neither affect safety nor production, but involve only the direct cost of repair.

46.4 Total Productive Maintenance

It is a well-known fact that in many factories, the operating time is less than 50% of the gross available hours per year; this obviously shows that assets are not being used to the fullest extent. This is partly due to *scheduled downtime*, which includes holidays, no production planned due to limited load, spare capacity to cope with volume flexibility, *etc*. The other part is caused by the fact that production is not wholly efficient. The reasons for this can be categorized into losses, which can be influenced during development and production phase. The total productive maintenance is a proactive equipment maintenance strategy designed to improve overall equipment effectiveness. It actually breaks the barrier between the maintenance department and the production department of a company.

Total Productive Maintenance: This is an approach to optimize the effectiveness of production means in a structured manner. TPM focuses on improving the planned loading time. The gap (losses) between 100% and actual efficiency can be categorized into three categories: availability, performance and yield (quality rate).

- *Availability losses:* These include breakdowns and changeover situations when the line is not running while it should be.
- *Performance losses:* These are basically due to speed losses and small stops, idling, or empty positions when the line is running but is not providing the quantity it should.
- *Yield losses:* These occur when the line is producing products, but there are losses due to rejects and start-up quality losses.

These losses lead to the overall equipment effectiveness (OEE) indicator, which tells how efficiently the planned production process is. TPM helps to improve the OEE by providing a structure to quantify these losses, and by subsequently giving priority to the most important ones. TPM provides concepts and tools to achieve both short and long term improvements.

Total productive maintenance is not the same as a maintenance department that repairs breakdowns (breakdown maintenance). TPM is a critical adjunct to lean manufacturing. If machine uptime is not predictable and if process capability is not sustained, we cannot produce at the velocity of sales. One way to think of TPM is *deterioration prevention* and *maintenance reduction*, not fixing machines. For this reason many people refer to TPM as *total productive manufacturing* or *total process management*. TPM is a proactive approach that essentially aims to prevent any kind of slack before occurrence. Its motto is "*zero error, zero work-related accident, and zero loss*". TPM has five goals:

1. Maximize equipment effectiveness;
2. Develop a system of productive maintenance for the life of the equipment;
3. Involve all departments that plan, design, use, or maintain equipment in implementing TPM;
4. Actively involve all employees; and
5. Promote TPM through motivational management.

For this concept to function properly, the machines must be ready when they are needed, and they must be shut down in such a fashion as to be ready the next time. Key measures include efficiency while running and quality. Overall equipment effectiveness (or OEE) tells us how TPM is working, not just the typical measures of uptime and throughput. OEE is actually the product of availability, performance efficiency, and the quality rate. Operators know what maintenance tasks are theirs; they also know what tasks are appropriate for the skilled trades' maintenance crews. TPM is a philosophy that helps create ownership of the manufacturing process among all employees. Teamwork is vital to the long-term success of TPM. The maintenance group performs equipment modifications that would improve reliability. These modifications are then incorporated into new equipment. The work of the maintenance group is then to make changes that will lead to maintenance prevention. Thus *preventive maintenance* along with *maintenance prevention* and *maintainability improvement* are grouped as *productive maintenance*. The aim of productive maintenance is to maximize plant and equipment effectiveness and to achieve the optimum life cycle cost of production equipment.

Nippondenso of Japan was first to implement TPM. It had already had quality circles which involved the employees in changes. Therefore, all employees took part in implementing productive maintenance. Based on these developments, Nippondenso was awarded the distinguished plant prize for developing and implementing TPM by the Japanese Institute of Plant Engineers (JIPE). Thus Nippondenso of the Toyota group became the first company to obtain the TPM certification.

TPM identifies sixteen types of wastes (*Muda*) and then works systematically to eliminate them by making improvements (*Kaizen*). TPM has eight pillars of activity, each being set to achieve a "*zero*" target. These pillars are:

1. Focused improvement (*Kobetsu-Kaizen*): for eliminating waste,
2. Autonomous maintenance (*Jishu-Hozen*): involves daily maintenance activities carried out by the operators themselves (the key players) which prevent the deterioration of the equipment,
3. Planned maintenance: for achieving zero breakdowns,
4. Education and training: for increasing productivity,
5. Early equipment/product management: to reduce waste occurring during the implementation of a new machine or the production of a new product,
6. Quality maintenance (*Hinshitsu-Hozen*): actually "*maintenance for quality*", it includes the most effective quality tool of TPM, "*poka-yoke*", which aims to achieve zero loss by taking necessary measures to prevent loss,

7. Safety, hygiene, and environment: for achieving zero work-related accidents and for protecting the environment, and
8. Office TPM: for involvement of all parties to TPM since office processes can be improved in a similar manner as well.

46.5 Computerized Maintenance Management System

Computerized maintenance management system (CMMS) is also known as *enterprise asset management* (EAM). A CMMS is a stand-alone computer program used to manage maintenance work, labor, and inventory in a company, whereas EAM not only does all the functions of a CMMS, but also integrates with the company's financial, human resource, material management, and other ERP (enterprise resource planning) applications. In the past, stand alone CMMS had an advantage over EAM in terms of features, ease of use and functionality.

A CMMS maintains a computer database of an organization's complete maintenance operations. This database is intended to help maintenance staff do their jobs more effectively (for example, determining which storerooms contain the spare parts they may need) and to help management make informed decisions, such as in calculating the cost of maintenance for each piece of equipment used by the organization and in allocation of resources judiciously. This information can also be helpful in dealing with third parties. For instance, if the organization is involved in a liability suit, the database information available with the CMMS can be used as evidence to support that proper safety maintenance was performed. CMMS can be used by any organization that must perform maintenance on equipment and property. Some CMMS products focus on particular industry sectors (*e.g.*, the maintenance of vehicle fleets or health care facilities, *etc.*). Other products aim to be more general. To identify CMMS vendors, a search for CMMS using any internet search engine can be performed.

Different CMMS packages offer a wide range of capabilities. A typical package may have the following features:

- Work orders: Scheduling jobs, assigning personnel, reserving materials, recording costs, and tracking relevant information such as the cause of the problem, record of downtime, and suggestions for further action required.
- Preventive maintenance (PM): Keeps track of PM inspections and jobs, including step-by-step instructions or check-lists, lists of materials required, and other pertinent details. Typically, the CMMS schedules PM jobs automatically-different software packages offer different techniques for reporting when a job should be performed.
- Asset management: Recording data about equipment and property including specifications, warranty information, service contracts, spare parts, purchase date, expected lifetime, *etc*. that might be of help to management or maintenance workers.
- Inventory control: Management of spare parts, tools, and other materials including the specification of materials required for particular jobs, records of where materials are stored, determining when more materials should be purchased, tracking shipment receipts, and taking inventory.

CMMS can produce status reports and documents giving details or summaries of maintenance activities. The more sophisticated the package is, the more analysis facilities are possible. Many CMMS packages can also be hosted by the company selling the product on an outside server, meaning that the company buying the software hosts the product on their own server or LAN. CMMS packages are closely related to facility management system packages (also called facility management software).

By adding some powerful reliability management tools, one can manage the information around maintenance, reliability, and ultimately a physical asset management (PAM). In fact, it can begin with the selection, implementation, data accuracy, failure coding, asset hierarchy, work order history,

user adoption, training, enforcement, reporting, key performance indicators (KPIs), dashboards, budgeting, planning, scheduling, mobile options, material management, and many more factors and will determine the result one can get with CMMS or EAM.

Last but not least, one must realize that these software systems are simply automating the underlying maintenance process, so if one is dealing with a poor maintenance process, adding CMMS will not make it better.

References

[1] Rau John G. Optimization and probability in systems engineering. Van Nostrand Reinhold, New York, 1970.

[2] Moss Marvin A. Designing for minimal maintenance expense: The practical application of reliability and maintainability. Marcel Dekker, New York, 1985.

[3] Anderson Ronald T, Neri Lewis. Reliability-centered maintenance: Management and engineering methods. Elsevier Applied Science, London, 1990.

[4] Misra KB. Reliability analysis and prediction: A methodology oriented treatment. Elsevier, Amsterdam, 1992.

[5] Smith AM. Reliability-centered maintenance. McGraw-Hill, New York, 1993

[6] Knezevic Jezdimir. Reliability, maintainability and supportability. McGraw-Hill, New York, 1993

[7] Blanchard Benjamin S, Verma Dinesh, Peterson Elmer L. Maintainability: A key to effective serviceability and maintenance management. John Wiley, New York, 1995.

[8] Ebeling Charles E. An introduction to reliability and maintainability engineering. McGraw-Hill, New York, 1996.

[9] Elsayed A Elsayed. Reliability engineering. Addison Wesley Longman, New York, 1996.

[10] Lewis EE. Introduction to reliability engineering. John Wiley, New York, 1996.

[11] Kelly Anthony. Maintenance strategy – Business-centered maintenance. Butterworth Heinemann, Oxford, 1997.

[12] Kelly Anthony. Maintenance organization and systems – Business-centered maintenance. Butterworth Heinemann, Oxford, 1997.

[13] Knezevic Jezdimir. Systems maintainability: Analysis, engineering and management. Kluwer, Dordrecht, 1997.

[14] Moubray John. Reliability centered maintenance (2nd edition). Butterworth-Heinemann, Oxford, 1997.

[15] Stoneham Derek. Maintenance management and technology handbook. Elsevier, London, 1998.

[16] Kumar UD, Crocker J, El-Haram M. Reliability, maintenance and logistic support- A life cycle approach. Kluwer, Boston, 2000.

[17] Gertsbakh IB. Reliability theory with applications to preventive maintenance. Springer, Berlin, 2000.

[18] Mobley Keith. An introduction to predictive maintenance. Butterworth-Heinemann, Oxford, 2002.

[19] Narayana V. Effective maintenance management: Risk and reliability strategies for optimizing performance. Industrial Press, New York, 2004.

[20] Nakagawa Toshio. Maintenance theory of reliability. Springer, London, 2005.

[21] Bloom Neil B. Reliability centered maintenance: Implementation made simple. McGraw-Hill, New York, 2005.

[22] Wang Hongzhou, Pham Hoang. Reliability and optimal maintenance. Springer, London, 2006.

[23] Murthy DNP, Blischke WR. Warranty Management and Product Manufacture. Springer, London, 2006.

[24] Jardine Andrew KS, Tsang Albert HC. Maintenance, replacement, and reliability: Theory and applications. Taylor and Francis, Boca Raton, FL, 2006.

[25] Rao BKN. Toward the universal theory of failure. In Proceedings of 19th International Congress COMADEM 2006. Kumar, Parida and Rao (Eds.) Luleå University Press, Sweden, 2006.

47

System Maintenance: Trends in Management and Technology

Uday Kumar

Division of Operation and maintenance Engineering, Luleå University of Technology,
S-97187, Luleå, Sweden

Abstract: Modern day systems are large, complex and automated. The high demands on the performance of such systems has created a need for new management and engineering solutions in the area of the maintenance of the complex systems. This need is mainly motivated by the steeply increasing cost of downtime. This chapter presents an overview of the recent trends in management of maintenance function and maintenance technology.

47.1 Introduction

Maintenance is necessary when a component (or system) is likely to fail or fails to fulfil its required function and involves servicing, replacement or repair. Some failures directly affect the operational capability and performance of the system. The main purpose of the maintenance function is to avoid these failures or to restore the system to its operating state after it has failed to fulfil the required function. In short, the maintenance function can be defined as activities for retaining a system in an operating state or restoring it to a state that is considered necessary for its operation and utilization. Therefore, the fundamental step in the effective management of the maintenance process is the accurate determination of the maintenance need of the system, which in turn is determined by the state of the equipment, and the actions that must be taken to restore it or retain it in an operating condition [1]. Furthermore, the maintenance needs are quantified by the consequences of the corresponding failures. Therefore, the driving element in all maintenance decisions is not the failure of the given item or system, but the consequences of the failure of that particular item or system [2].

The increased level of automation and the high demands on system performance have created a need for a new engineering approach and new managment techniques in the field of equipment and asset management. This need is mainly motivated by the steeply increasing cost of maintenance and downtime. For example, the amount spent on the maintenance budget for Europe is around 1500 billion Euros *per* year [3], and for a small country like Sweden it is about 20 billion Euros *per* year if only the direct cost of maintenance is taken into account [4]. Besides, breakdowns and downtime also result in a loss of product quality and production, as well as having a negative impact on health, safety, and the environment. A safety-related example from the recent past is the accident at British Petroleum's Texas refinery in the USA, which killed 15 and injured about 500 persons, apart from costing a

billion dollars in repair and compensation [5]. Prevention of such accidents could have enhanced BP's image, besides saving billions of dollars. In short, the discipline of maintenance has evolved over the years to become an indispensable field in engineering.

In general, the maintenance approaches implemented and practised by companies can be classified into two major groups, namely planned maintenance and unplanned maintenance. These approaches can be further subdivided into the preventive and the corrective maintenance approaches. The corrective maintenance approach is reactive in nature, whereas preventive maintenance is a form of proactive maintenance activity (see Figure 47.1). The preventive maintenance approach can be time-based or condition-based.

The traditional aim of the condition monitoring technique has been the early prediction of failures by monitoring certain critical system parameters, and now it is an established fact that the judicious application of condition monitoring techniques can help in controlling and optimizing the colossal maintenance problem. The dream figure of 80% planned maintenance and 20% emergency or running repairs looks realistic today, if one believes in the capability of "on-line" and "off-line" condition monitoring devices and instrumentation. Figure 47.1 illustrates the evolution of the business of maintenance through the years [6]. In the past maintenance was not an issue, but now we are talking about self-maintenance and maintenance-free systems.

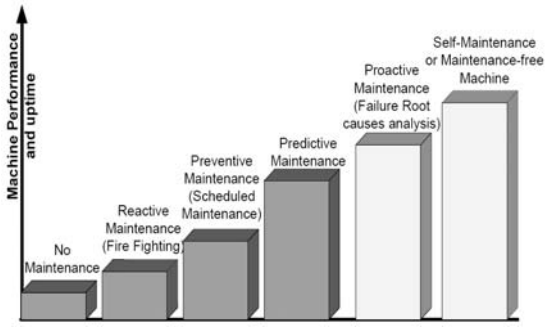


Figure 47.1. Development and evolution of the concept of maintenance with time [6]

47.2 Why Does a Component or a System Fail and What Is the Role of Maintenance?

To understand the evolution and developments taking place in maintenance engineering and management, it is essential to understand why we need to think about maintenance and what role it plays in the achievement of business goals.

Most physical products and systems wear, tear, and deteriorate with age and usage. In general, due to cost and technological considerations, it is almost impossible to design a system that is maintenance-free. In fact, maintenance requirements come into consideration mainly due to a lack of properly designed reliability and quality for the tasks or functions to be performed. Thus, the role of maintenance and product support can be perceived as the process that compensates for deficiencies in design both in terms of product reliability and product output quality. These shortcomings in design are compensated for through appropriate maintenance and product support programs (Figures 47.2 and 47.3).

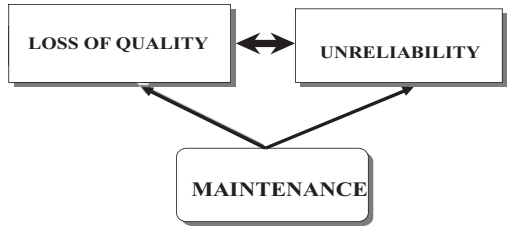


Figure 47.2. Maintenance compensates for the unreliability and loss of quality in the designed product

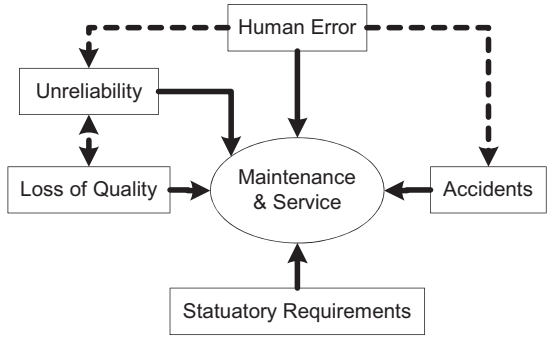


Figure 47.3. Root causes of product support and maintenance

Apart from unreliability and poor quality, other factors such as human error, statutory requirements, accidents, *etc.*, also influence the design and development of product support and the maintenance concepts [7].

In the following sections we present a brief review of recent trends in maintenance management and maintenance technology. The first section introduces the subject area; the second section presents a review of the recent developments being made for effective control and management of the maintenance function by companies and researchers. The third section presents a brief overview of the recent advances in condition monitoring and maintenance engineering approaches being adopted and implemented by companies all over the world.

47.3 Trends in Management of the Maintenance Process

It is obvious that maintaining equipment and plants is a very costly and time-consuming activity. Maintenance is also important for health and safety, since records show that inadequate maintenance activities are closely associated with excessive accident rates [8]. As a result, there has been a major paradigm shift in the maintenance philosophy of many companies aiming at a high degree of mechanization and automation. Maintenance is no longer a necessary evil "that costs what it costs", but an important function that creates additional value (see [9]) in the business process as illustrated in Figure 47.4.

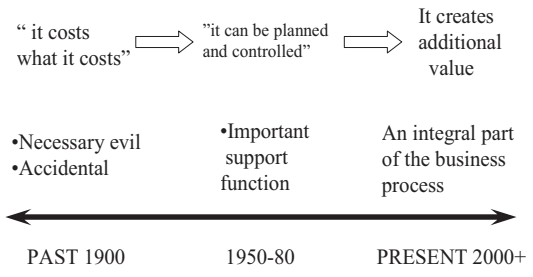


Figure 47.4. Paradigm shift in asset managers' views of the maintenance discipline

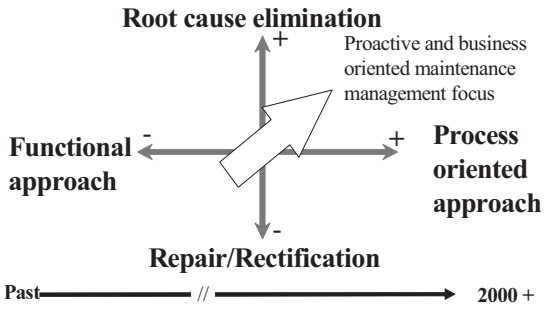


Figure 47.5. Paradigm shift in maintenance work culture

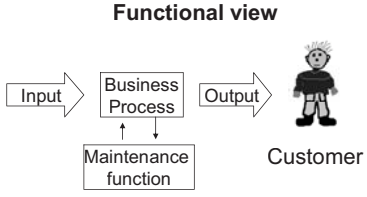


Figure 47.6. Functional approach of the maintenance discipline

Accordingly, the focus of senior asset managers has shifted from "fail and fix" to root cause elimination, and from functional thinking (we and them) to a process-oriented approach that encourages a process-oriented work culture in maintenance (*i.e.*, a focus on the end customer), see Figure 47.5. Furthermore, a closer look at the style of maintenance management reveals that many companies are treating maintenance as an integral part of their business process, and not as a standalone support function. Accordingly, the focus of maintenance management has shifted from merely being responsible for the delivery of agreed reliability and availability to supplying services to fulfill the requirements of customers and stakeholders [10].

This has brought about a change in the attitude of maintenance engineers and managers and their focus has shifted to the end customers, apart from meeting set availability and equipment capacity targets (see Figures 47.6 and 47.7).

47.4 TPM Implementation

The search for appropriate techniques for achieving excellence in maintenance with the involvement of

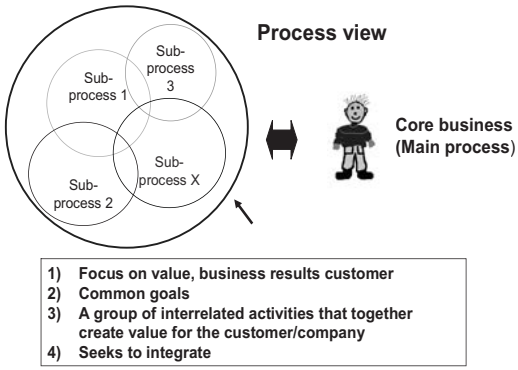


Figure 47.7. Process-oriented approach of the maintenance discipline

all the employees in the organization has led to many companies implementing the Total Productive Maintenance (TPM) philosophy in some form or another. The strategy of dividing up the maintenance tasks between operators and maintenance specialists has made the TPM approach quite popular in the manufacturing industry. TPM combines the conventional practice of preventive maintenance with the concept of total employee involvement through small group activities. The result is an innovative system for equipment maintenance that optimizes productivity, eliminates breakdowns and promotes the philosophy of autonomous maintenance through continuous improvement. In general, the key to the success of the TPM approach is the fact that the operator performs the first line maintenance and specialized jobs are carried out by experts.

TPM seriously takes into account the social factors and cultural background in its endeavour to achieve the overall effectiveness of the operating system. See [11] for a detailed discussion of TPM philosophy. Since social factors and employees' backgrounds play an important role, TPM is not a stereotype implementation of some set rules. The management effort needs a human touch to achieve the best out of the existing production system. The success of TPM is dependent on the success of team work between the operation and the maintenance department. In TPM, these teams are also referred to as total quality circles (TQC) in maintenance.

TPM is based on the application of five S's, namely seiri-organization, seiton- neatness, seiso-purity, seiketsu-cleanliness and shitsuke-discipline, which are central to all the Japanese methods that have evolved since the early 1950s.

It is appropriate to mention that the results of TPM take around three to four years to become visible, as it involves the soft side of human nature. Since it takes a long time to implement TPM, many companies are adopting a lean version of TPM, *i.e.*, they are focusing on a partial implementation.

To manage the maintenance function effectively, one needs to plan and predict the future maintenance requirement while keeping in view the strategic production and operation goal of the company. The main challenge is to implement a decision support system that facilitates correct decision making when dealing with maintenance-related issues. One such approach is risk-based decision making.

47.5 Application of Risk-based Decision Making in Maintenance

The main purpose of maintenance is to reduce the business risk. Taking decisions concerning the selection of a maintenance strategy using risk-based criteria is essential to develop cost-effective maintenance policies for mechanized and automated systems, because in this approach technical features (such as reliability and maintainability characteristics) are analyzed considering the economic and safety consequences of each alternative at hand. Therefore, it is natural that an increasing number of assets and plant managers are adopting risk assessment procedures as an integral part of the maintenance planning [2]. This approach provides a holistic view of the various decision scenarios concerning the maintenance strategy where the cost consequences of every possible solution can be assessed quantitatively.

Risk analysis is a technique for identifying, characterizing, quantifying, and evaluating the loss due to an event. In system risk analysis, reliability and maintainability (see the section on design-out maintenance) are integrated at various stages of the

analysis. Risk can be formally defined as the potential of loss or injury resulting from exposure to a hazard or failure. Risk can be viewed both qualitatively and quantitatively. In general, risk analysis consists of answers to the following questions [12]:

- What can go wrong and lead to a system failure?
- How likely is this to happen?
- If it happens, what consequences are to be expected?

Therefore, risk can be defined qualitatively as the following set of triplets

$$R = E_i P_i C_i,$$

where

E_i is the scenario of events that leads to a failure,
Pi is the probability of the occurrence of event i, and C_i is the consequence of scenario i. For a particular failure mode, risk can be quantified by (see also Figure 47.8):

Risk = the probability of occurrence x the consequences of the failure

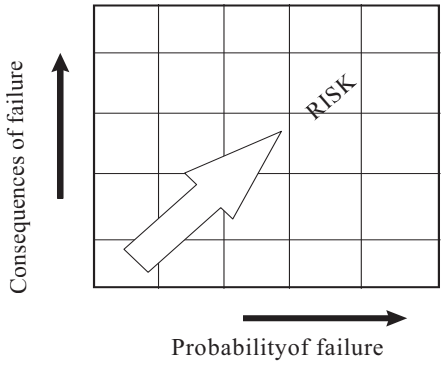


Figure 47.8. Illustration of the risk concept

In general, three classes of consequences are relevant for system namely safety consequences, economic consequences and environmental consequences. To deal with the estimated risk, preventive maintenance programmes are implemented to control the occurrence of failures and at the same time efforts are also made to contain the intensity and effect of consequences through various damage control measures. Figure 47.9 illustrates the approach.

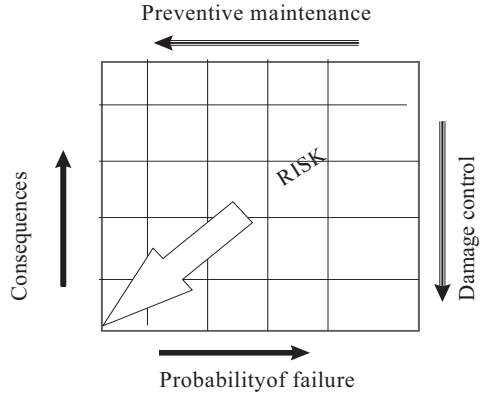


Figure 47.9. Risk and its control measures

For each of the potential design changes or modifications that are to be identified by the experts, a cost-benefit comparison can be used to select the viable modification options based on a comparison of expected benefits versus estimated costs. In fact the cost, the level of risk and the benefits from risk control are closely linked and they cannot be evaluated separately. In other words, any anticipated increase in benefit from a decision may increase the risk if the cost is kept constant, or any reduction in risk may reduce the benefit as the cost may increase. Such analysis clearly shows the rate of cost intensity of risk elimination.

47.6 Outsourcing of Maintenance and Purchasing of the Required Functions

It is being argued by many asset managers and leading companies that it is preferable to concentrate on the core business and that the business of maintenance, which has been expanding critically with the evolution of technology, should be taken care of by the specialists. This way of thinking is gradually spreading and many managers are willing to contract out the maintenance function to the authorised service providers or the original equipment manufacturer (OEM). This approach has helped many companies

to maintain a lean and flat maintenance organization. Another trend in maintenance management is for the equipment operator to enter into a contractual agreement with the equipment supplier whereby the supplier is responsible for repair and maintenance, including the storage of spare parts, *etc.* In such a contract, a specified level of availability is usually demanded and failure to meet it results in the supplier being stiffly penalized. It is the firm belief of senior asset managers that the development of a sound subcontracting system for maintenance can reduce the cost of maintenance manifold, and this practice is on the increase in many industries. However, it is also being criticized, because control of the availability of machines is shifted to some external organization over which one has little control.

Types and forms of maintenance and service contract:

- Contracting-out of the routine maintenance tasks
- Outsourcing
- Partnering

47.6.1 Contracting-out of the Maintenance Tasks

Many asset managers adopt the practice of contracting out a part of their maintenance work load to service providers or to original equipment manufacturers (OEM) to cut down their cost and maintain a lean organization. The exchange of data and information is limited with such an approach and such a relationship with the service provider and is mainly governed by the written contact. Such a form of service outsourcing does not facilitate a long-term relationship, as it is mostly based on the premise, "I win and do not care what happens to you."

47.6.2 Outsourcing

Outsourcing is a more developed form of traditional contracting-out. In the outsourcing process one establishes a form of relationship with the service provider where the service receiver on a case-to-case basis does not hesitate to share even confidential information [13].

47.6.2.1 Partial Outsourcing

In this approach, an OEM sells a system accompanied by an attractive bundle of service and maintenance provisions. The maintenance work is partially outsourced to the OEM or a service supplier. While the operator out sources some or all of the maintenance work, they still own the product and their employees operate it. For example, in the case of a drill machine, a mine-operator can choose to outsource the maintenance of the hydraulics and IT-related services to the OEM or to some independent service provider.

Alternatively, a mine operator/user may choose to outsource all the maintenance work to an OEM or to an authorized service and maintenance supplier. Due to the probability of fast technological developments, a management may prefer to focus its attention and resources upon core business activities. Fewer and fewer companies seem willing to buy a system, use it and maintain it; the preference is to outsource maintenance/ services so as to share business responsibilities with an OEM/supplier. Outsourcing is viewed as a means to ensure far greater cost discipline while at the same time improving the quality of service and the product delivery capability. For instance, returning to the drill machine, a mine operator may outsource all the maintenance-related work (not only the maintenance of hydraulics or a particular drilling machine part). Managers and operators/ companies use outsourcing as a means to focus on the core business and thereby minimize the business risk, in addition to increasing competitiveness. Outsourcing has changed not just the face of the workplace but also societal attitudes towards work and employment.

The decision to outsource is usually based on the premise that an OEM/supplier has some inherent advantage over the host company in varying forms of shared supervision. This can cause conflict between the workers of an OEM/supplier/ contractor and a host company, since officially these workers are under the administrative control of the contractor, while in

reality the host company controls them. Therefore, the terms and conditions related to the role and responsibilities of all the actors should be clearly defined in the contract (negotiated agreement) to avoid a loss of control, reduced competence, and decreased operational flexibility. Recently conducted surveys report high levels of dissatisfaction with outsourcing [14]. On the other hand, outsourcing, when carefully managed, offers excellent potential in the sharing of business risk and the enhancement of business performance between partners. Outsourcing is often a matter of trust and cooperation between the parties involved. The main driver of outsourcing is the aim of achieving cost benefits. The available literature [15], [16] offers details on the management of different elements in outsourcing.

47.6.2.2 Full Outsourcing

With this newest type of strategy a customer/mine operator owns a system but all the support required for the mining equipment and the equipment operators' related services is provided by the OEM or equipment supplier at agreed prices or as part of the original selling price. This combination of system, services, support and knowledge from an OEM to a mine operator means that full service is provided. Full service in the mining industry usually means that the OEM/service provider executes all the corrective, preventive and predictive maintenance activities, as well as all the support to the equipment operator/customer (for details see [17] and [18]. Such support ranges from training to machine maintenance. A critical element is the fact that support is given to a mine operator for using the drill machine effectively and efficiently. In this form of full outsourcing an OEM/service provider is responsible for providing an agreed level of availability and reliability. The knowledge provided includes when, why, and how a drill machine is to be used to achieve the maximum profit. This is more or less an individualized problem solving service sold to a mine operator/customer as part of a package.

47.6.2.3 Partnering

This is the most developed form of contracting-out of jobs and in such a form the problem is owned by both the partners with some form of incentive to stimulate development and innovation in the services. Here asset managers share everything with service providers (partners) including the profit and losses, and mostly this is based on long-term understanding of each other's business processes, which are mainly focused on creating a WIN–WIN situation for both the partners (see Figure 47.10). For details see [19].

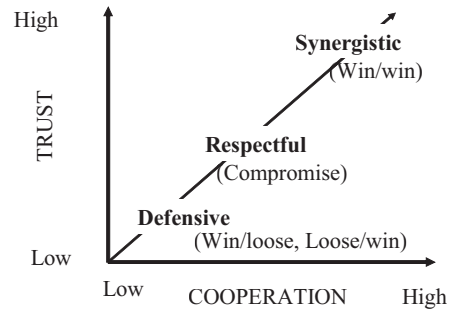


Figure 47.10. Outsourcing model built on cooperation and trust(adapted from [20])

The trend in maintenance can be illustrated as shown in Figure 47.11 from situation I to II but the business is drifting towards type II (leasing and functional product).

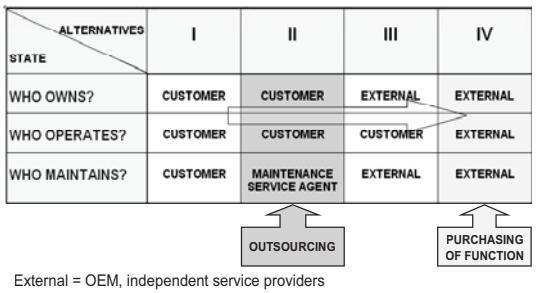


Figure 47.11. Trends in outsourcing leading to the concepts of functional products

47.6.3 Purchasing the Required Function: The Concept of Functional Products

Functional products: Modern-day industry is becoming less physical and more cognitive as manual labor is gradually being replaced by machine operation. The machines involved are expected to perform round the clock. However, due to design problems, these systems are not able to meet customers' requirements in terms of system performance and effectiveness. This is often due to poorly designed reliability and maintainability characteristics, combined with poor maintenance and product support strategy, which often lead to unscheduled stoppages (failures). This has given a new dimension to the problem of effective and efficient management of maintenance and service processes. To avoid the complexities of maintenance management, many customers/users prefer to purchase only the required function, not the machines or systems, so that the responsibility of maintenance and product support lies with the organization delivering the required function. With the advent of this trend, the focus has shifted to the design of functional products (see Figure 47.11).

A functional product may be defined as a product whose function is purchased by the user and not the actual machine/system delivering the function. For details see [21] and [22]. Often designers and manufacturers develop systems and sell them to users (the continuous line). This is also called a technological push, *i.e.* one develops a system and creates a need for it. However, systems should be developed keeping in view the application type customer-pull. The designed product characteristics define the types of application which the product can be subjected to and the type of product support needed to achieve the expected function and performance.

Without any formal measures of performance, it is difficult to plan control and improve the outcome of the maintenance process. Today, maintenance performance measurement (MPM) is receiving a great amount of attention from asset managers and maintenance engineers, mainly due to its newly found role in the prevalent business environment [23] and [24].

47.6.4 Maintenance Performance Measurement

Measuring maintenance process activity is nothing new and previously used to be carried out with scorecards or with indicators like maintenance cost per unit, maintenance budget, overtime costs and non-availability index due to maintenance, *etc.* However, these maintenance indicators are found to be stand-alone indicators, mostly localized to the shop floor or operational area only and not linked to the corporate business level. With the current paradigm shift in maintenance, today senior management can visualize the linkage and are keen to know the value created by the maintenance process.

In the 1980s, the term "productivity" was replaced with "performance", as the criteria of the productivity paradigm were unable to satisfy various stakeholders. It was realized that the shortcomings of the prevailing performance measurement systems, most of which were based on financial measures. Traditional financial performance measures provide little indication of future performance and encourage short-termism [25]; they are internally rather than externally focused, with little regard for competitors or customers [26], [27]. Moreover, the traditional performance measures lack a strategic focus and do not encourage innovation. Normally, most organizations measure what is easy to measure, collecting all sorts of data, which ultimately leads to data overload.

A PM system is defined as the set of metrics used to quantify the efficiency and effectiveness of actions [27]. The MPM concept adopts the PM system, which is used for the strategic and day-to-day running of the organization, and for planning, controlling and implementing improvements, including monitoring changes. A key performance indicator (KPI) needs to be defined for each element of a strategic plan and the KPI can be converted into the PI at the basic shop floor or operational level.

Presently, maintenance performance measurement forms an integral part of performance management in any production or manufacturing organization. In the MPM system, the corporate

goals need to be cascaded down into operational targets at the shop floor level, and the outcome results or actual lagging indicators need to be aggregated at a higher level. The real challenge is how to cascade the goal vertically down the organization and aggregate the outcome at various levels upwards. It is also a challenge to integrate activities amongst various departments within organizations horizontally so that the total maintenance effectiveness and desired business objectives is achieved. An all-out effort is currently being made to create a link and effect model to measure the contribution of maintenance to the company's business goals [23]. Today, researchers have developed a multiple criteria and hierarchical MPM framework which is balanced and integrated. For details see [28]. With the application of information and communication technology (ICT) and e-Maintenance, companies can look forward to having an efficient MPM system based on server-based software applications, the latest embedded internet interface devices and state-of-the-art data security. The application of ICT and e-Maintenance has facilitated real-time data collection and analysis, and cost-effective decision making [23].

47.7 Trends in Maintenance Technology and Engineering

The different concepts and tools used in maintenance engineering have evolved over the years with the objective of continuous improvement in maintenance planning and management. With the introduction of the functional product to the market, OEMs have directed their focus on tackling the maintenance needs of a system, which can minimize the life cycle cost of the system. In this connection many designers have two alternatives: either to design out maintenance using available or innovative engineering solutions or, in cases where this is not possible, to opt for the design for maintainability alternatives.

47.7.1 Design out and Design for Maintenance

More often than not it is becoming standard practice to use risk analysis in combination with LCC analysis to arrive at a correct decision as to whether to design out the maintenance need or design the system for maintenance, if the option of designing out is either technically unfeasible or economically unviable. For such exercises, knowledge of reliability and maintainability engineering is a must. It is important to consider system reliability and maintainability issues in all the phases of a system's conception, design, construction (manufacturing) and operation. Not only does this raise our consciousness of the issues in question, but it also usually results in real improvements in the reliability of the system, thereby reducing the risk of failure and leading to subsequent saving in maintenance.

47.7.2 Reliability

The reliability of equipment is the probability that it will perform its required function without failure under given conditions for an intended period of operation. The decision regarding the reliability characteristics of equipment is taken during the drawing board stage of equipment development. The aim is to prevent the occurrence of failures and also to eliminate their effects on the operational capability of systems. Among the factors which have an important influence on equipment reliability are:

- the period of use
- the environment of use

The mean time to failure (MTTF) is a measure commonly used to express the reliability of components or systems [29], [12].

47.7.3 Maintainability

The maintainability of equipment can be defined as the probability that it will be restored to a specified condition within a given time period using specified resources. High maintainability performance is obtained when the system is easy to maintain and repair. In general, maintainability is measured by the mean repair time, often called the mean time to repair (MTTR), which includes the total time for fault finding and the actual time spent carrying out the repair. Maintainability considerations are also

very important for units operating under tough conditions, for instance mining equipment [30].

Some of the prerequisites for a good maintainability standard are:

- interchangeability
- easy accessibility
- modular design

When considering maintenance in design, one generally has two options: one can either try to design out maintenance (Figure 47.12) and if this alternative is not feasible economically or due to lack of technology, then design for maintainability approach is adopted (see Figure 47.13).

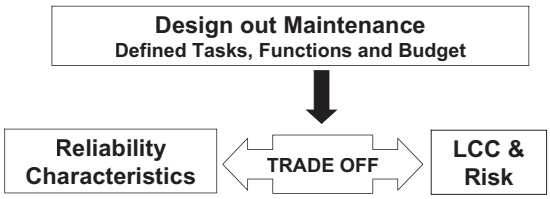


Figure 47.12. Designing out maintenance

However, if maintenance is to be designed out, one has to consider the reliability characteristics of the components and system *vis-à-vis* the task and function to be performed by them. In fact designing out maintenance is very much synonymous with designing for reliability. Besides the reliability characteristics of the component and system, one also has to consider the state of the art of the technology – a lack of available technology might not allow the elimination of maintenance need, or might make it too costly.

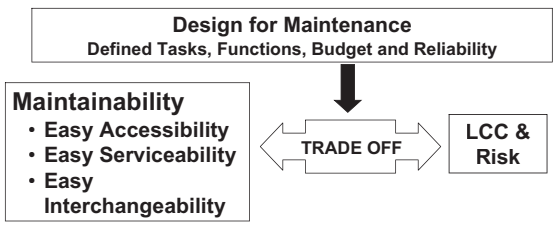


Figure 47.13. Designing for maintainability

There are also other factors to evaluate, such as product capacity, design alternatives, and payback of development costs, *etc.* There will always be a trade-off between these considerations. LCC analysis might be used to compare the design alternatives. The LCC analysis results have to be balanced against the market need, the customer's willingness to pay, customer preferences, *etc* [31].

In designing out maintenance, one has to use RAMS tools like FMECA (failure mode effects and criticality analysis), FTA (fault tree analysis), and risk analysis to arrive at the best LCC alternative. If the life cycle cost of *designing out maintenance* is higher compared to the alternative *designing for maintenance*, then we should naturally prefer the latter. The objectives of maintainability analysis are to reduce the product maintenance time and cost, and to determine labour and other related costs by using maintainability data to estimate item availability. The results should be reduced downtime, more efficient restoration of the product to an operating condition, and a maximization of operational readiness. If the reliability is too low, maintainability issues such as accessibility to parts that need to be maintained, and the serviceability and interchange ability of parts and systems have to be considered [29], [32]. Warranty and the life span are also issues to be evaluated.

Often it is not possible to design out maintenance because of a lack of technology, and one ends up trying to balance reliability, cost, and availability. Other ways to reduce the future maintenance need are to reduce the capacity, to substitute/eliminate the weak functions, or to replace weak components with ones that are more robust. If one allows the system/component to fail due to various limitations, then one needs to make provision for easy and quick repair/replacement. Thus, when designing for maintenance, one will first have to examine the reliability characteristics, and thereafter decide the maintainability characteristics. Both R and M are traded off to meet the design requirement. LCC analysis, in combination with risk analysis methods, could be a viable tool for evaluating these issues [33], [34].

47.7.3.1 Design for Data Collection, Diagnostics, Prognostics, Internet Applications, etc.

As products become more complex, failures and faults become harder and more time-consuming to diagnose. The designer's goal with respect to design for diagnosability is to facilitate the process of determining the parameters that are not in the designated state. Once the parameters that are not in the intended state are isolated, a repair action can take place to return the parameters to the design state. Automated sensor-based diagnostics systems have been the focus in research on diagnostics in mechanical systems [7].

47.8 Condition Monitoring and Condition-based Maintenance Strategy

A closer look at recent advances in maintenance in different parts of the world suggests that most companies are increasingly using some type of condition monitoring device on their critical units. Most equipment manufacturers have developed some form of condition monitoring device in close cooperation with the users of the equipment. Usually in such systems, the performance data from the machine is collected automatically. The collected data is analyzed either by using professional software or manually to extract information from the data. By the judicious use of information, new knowledge of system health is generated, which provides a basis for decision making in maintenance (Figure 47.14).

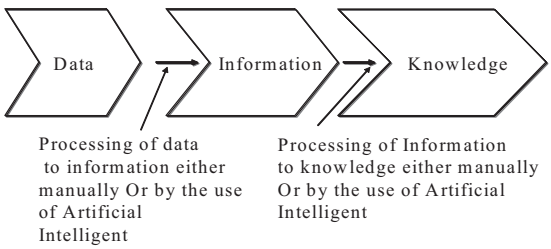


Figure 47.14. Processing of raw data into useful information and knowledge

A close examination of the development trends in condition monitoring technologies clearly shows that the focus has shifted from fault diagnostics to prognostics. In fact, equipment users are demanding zero breakdowns during operation and production, leading to more focus on prognostics technologies. This trend has stimulated R and D in the field of sensor technology and also in the area of future and emerging technology. Today operators are demanding production systems with a self-healing and self-maintaining ICT infrastructure. The intelligent application of a prognostics model can detect failures before they occur.

Currently many suppliers are offering so-called "expert" systems for fault diagnosis and prognosis. At present, these expert systems are still essentially rule-based systems, and like all rule-based systems, the results are only as good as the rules that have been established within the system. The reality is that these rule-based expert systems are still significantly weaker than even a moderately experienced maintenance engineer or analyst in identifying and diagnosing faults. Nevertheless, an imperative, if smart sensor technology is to work, and if widespread on-line vibration monitoring is to proliferate, is the development of better and more accurate "expert" software. Further advances can be made through the use of fuzzy logic and neural network processes in condition monitoring software.

47.8.1 Sensor to Sensor (S2S)

In expert systems the data is transmitted from sensor to sensor at the plant and equipment level. Sensors are embedded in the system or subsystem for collecting data which is converted to the e-health information of the plant and machinery. This e-health information provides support for the management for monitoring and control of the productivity, besides correct decision making.

47.8.2 Sensor to Business (S2B)

Today researchers and companies are busy developing Web-enabled remote monitoring sensor-to-business device platforms for the remote monitoring and prognostics of diversified products

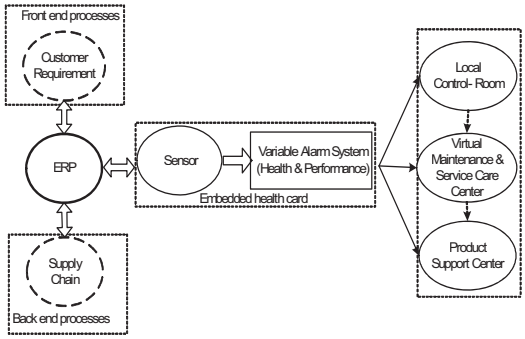


Figure 47.15. A schematic diagram of sensor to business communication

[6]. The rapid development of smart sensors and Web-enabled technologies is an important enabler for remote monitoring and prognostics. Figure 47.15 illustrates one sensor-to-business scenario where embedded sensors in machines and systems will only trigger alarms regarding impending failures after evaluating the total business risk using information and data from an enterprise resource planning (ERP) system.

Such sensors are smart and make provision for variable alarms depending on the evaluated business risk for each viable alternative for the situation encountered.

47.9 ICT Application in Maintenance: e-Maintenance 24-7

With the emergence of intelligent and smart sensors to measure and monitor the health state of components and the implementation of information and communication technologies (ICT), the conceptualization and implementation of e-Maintenance are becoming a reality. e-Maintenance facilitates decision making in real time by monitoring plant and systems health and its behaviour in real time, by benchmarking the status against the specified standards and by evaluating the associated business risks with various alternatives at hand, using embedded intelligent sensors and internet-based technology. To benchmark the health state and the performance characteristics, the experts invariably envision the generation and implementation of different types of performance trend charts and indicators when making decisions in maintenance. Although e-Maintenance shows a great deal of promise, the seamless integration of ICT into the industrial environment and setting remains a challenge. Understanding the requirements and constraints from the perspective of maintenance performance and ICT is essential for the effective implementation of such concepts. The related issues need to be addressed for the successful use of ICT and e-Maintenance for measuring maintenance performance.

The main problem for decision-making in the operation and maintenance process is the non-availability of relevant data and information. The recent application of information and communication technology (ICT) and other emerging technologies facilitates the easy and effective collection of data and information. E-condition monitoring, using intelligent health monitoring techniques like embedded intelligent sensors through a wireless communication system, is integrated with the maintenance process, to monitor and control the health status of plant and machinery. This is achieved by analyzing the data after it has been collected and effective decision making. The most important application of the measurement is the identification of opportunities to improve the state of existing equipment and plants before new investment or to promote improved supplier performance.

e-Maintenance provides the organization with intelligent tools to monitor and manage assets like machines and plant proactively through ICT. e-Maintenance creates a virtual knowledge centre consisting of users, technicians/experts and manufacturers, and specializing in operation and maintenance in the manufacturing, process and service industries. Moreover, e-Maintenance provides a holistic solution for the process industry with the objectives of reducing the overall costs and achieving savings in resources through maintenance performance indicators (MPIs). Condition monitoring techniques generally include one or several alarms that are triggered if a tolerance limit is exceeded or if a trend deviates from the expected values in time. References of the working points of signals are provided by knowledge-based systems and by comparison with a model of the system. These signals are acquired

by a sensor system [35]. An e-Maintenance solution consists of the virtual connectivity of:

- Plant/equipment fitted with intelligent and wireless sensors
- On-line (wireless) connectivity to out-sourcing contractors/stakeholders
- Operation/control platform of an online and wireless warning system
- Virtual maintenance team or expert support

Real-time connectivity amongst all the stake-holders concerned is a factor which facilitates the collection of system health and performance information. US companies have a substantial lead in the area of interoperable maintenance-oriented tools with MIMOSA (Machinery Information Management Open System Alliance), which has elaborated a set of standards [36]. In Europe, there are organizations like ITEA (Information Technology for European Advancement), which was established in 1999 and is conducting the PROTEUS project (ITEA 01011) to provide a fully integrated platform to support any broad e-Maintenance strategy [37]. Other e-Maintenance platforms which are trying to standardize are CASIP [38] and GEM@WORK [39].

47.9.1 The e-Maintenance Framework

Some of the existing e-Maintenance solutions provide server-based software and equipment-embedded internet interface devices (health management cards) for condition monitoring. These e-Maintenance solutions provide 24 x 7 (24 hours a day and 7 days a week) real-time monitoring, control and alerts at the operating centre. This type of system converts data into information that is available to all the stakeholders concerned for decision-making and predicting the performance condition of the plant and machinery on a real-time basis. This enables the system to make a match with the e-business and supply chain requirements. For example, once the supervisor knows the plant degradation condition and its related effects on material and inventory, then the delivery status can be planned and coordinated with greater speed to satisfy the customer.

A broad e-Maintenance framework indicating different stakeholders and their role is given in Figure 47.16. A stakeholder is a party having a right, share or claim in a system or in its possession of characteristics that meet that party's needs and expectations [40]. In this framework, the internal stakeholders are, *e.g.*, the management, employees, and different groups or departments, and external stakeholders are the customers, suppliers, out-sourcing agencies and partners, regulating authorities, and virtual consultants/experts, *etc.* The health condition data of the plant/machinery is collected through the e-health card/intelligent embedded sensors and compared with the pre-specified MPI limits. Accordingly, once the warning or alarm level is reached, all the affected parties receive a signal telling them to have a look and take appropriate preventive/predictive action. The maintenance control centre (MCC) controls, monitors and coordinates all the maintenance activities in-house or through the on-line help of the experts and virtual repair teams.

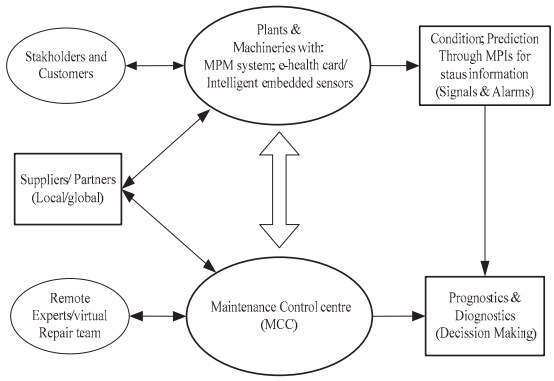


Figure 47.16. e-Maintenance framework (MPM –maintenance performance measurement, MPIs – maintenance performance indicators)

The suppliers or the outsourcing partners are also part of this e-Maintenance network and provide real-time support as and when required. Since the customers and other stakeholders are receiving real-time information and support as well, the e-Maintenance framework can take care of all the stakeholders. As can be seen, e-Maintenance creates a virtual knowledge centre consisting of users, technicians/experts and manufacturers, and specializing in operation and maintenance. E-Maintenance can provide a holistic solution for the

process industry with the objectives of reducing the overall costs and achieving savings in resources through MPIs like OEE and ROMI, *etc.* The problem today in a plant health management system is the existing information islands, *i.e.,* the different specialized systems within an organization speaking a different data and information language.

Maintenance has come a long way from the mechatronics to the infotronics stage. Adopting the emerging condition-based component degradation and monitoring system, integrated with an appropriate e-Maintenance model, organizations can achieve effective maintenance monitoring and control through measuring maintenance performance. Managing varieties of condition monitoring information demands effective methods in order to achieve the desired maintenance performance. With the development and emergence of intelligent e-Maintenance in the manufacturing and process industries, the objective of managing the maintenance information system is to convert the field data into useful information, so that decisions aiming to achieve the desired maintenance performance can be made on-line and/or remotely through wireless communication.

However, various constraints and challenges are to be resolved, as is appropriate to the different organizations, prior to the e-Maintenance system's adoption and implementation. The e-Maintenance real-time measuring system can act as a performance driver and help the organizations to know the plant/equipment health state and take prognostic action well in advance. This integrated approach of the e-Maintenance system, using ICT for measuring maintenance performance, can support and facilitate the organization in achieving transparency and good corporate governance, while taking care of the health, safety (accident prevention), economic, and environmental issues.

47.10 Conclusions

In this chapter the author has focused on the application of and future trends in ICT and e-Maintenance, besides purchasing the maintenance function as a functional product. It is essential that the engineers, managers and researchers involved in the operation and maintenance of systems are aware of the development of these trends in technology and management, so as to update their know how and keep pace with the technology and global competition.

Acknowledgement

The author gratefully acknowledges the help of Dr. Aditya Parida and Mr. Saurabh Kumar of Luleå University of Technology, Sweden, and Dr. Tore Markeset, University of Stavanger, Norway in the preparation of this manuscript.

References

[1] Tomlingson PD. Achieving world class maintenance status. SME 2006; 58(11):30–33.
[2] Kumar U. Reliability and risk based maintenance strategies. Journal of Mine, Metal and Fuels 1998; XLV: 76–80.
[3] Altmannshoffer R. Industrielles FM. Der Facility Manager (In German) 2006; April.
[4] Ahlmann H. From traditional practice to the new understanding: The significance of life cycle profit concept in the management of industrial enterprises. Proceedings of the International Foundation for Research in Maintenance, Sweden 2002.
[5] Bream R. Lawsuit poses further risk to BP's image. Financial Times, 2006; June.
[6] Lee J, Wang H. New technologies for maintenance. In Complex System Maintenance Handbook. Kobbacy KAH and Murthy DNP (Eds.); Springer-Verlag, London, 2008: 49-78.
[7] Markeset T, Kumar U. Design and development of maintenance concepts for industrial systems. Journal of Quality in Maintenance Engineering 2003; 9(4):376–392.
[8] Rushworth AM, Mason S. The Bretby maintainability index: A method of systematically applying ergonomic principles to reduce costs and accidents in maintenance operations. Maintenance 1992; 7(2): 7–14.
[9] Liyanage JP, Kumar U. Towards a value-based view on operation and maintenance performance management. Journal of Quality in Maintenance Engineering 2003; 9(4): 333–350.
[10] Söderholm P. Maintenance and continuous improvement of complex systems: linking stakeholder requirements to the use of built-in test systems. PhD Thesis, Luleå University of Technology, 2005.

[11] Nakajima S. Total productive maintenance. Productivity Press, Cambridge, MA, 1989.
[12] Moddares M. Reliability and risk analysis. Marcel Dekker, New York, 1993.
[13] Allen S, Chandrashekar A. Outsourcing services: the contract is just the beginning. Business Horizon 2000; 43 (2):25–34.
[14] Kakabadse A. Kakabadse N. Trends in outsourcing: contrasting USA and Europe, European Management Journal 2002; 20:189–198.
[15] Bragg SM. Outsourcing: a guide to selecting the correct business unit, negotiating the contract, maintaining the control of the process. Wiley, New York, 1998.
[16] Gay CL, Essinger J. Inside outsourcing: the insider's guide to managing strategic sourcing. Nicholas Bearley Publication, London, 2000.
[17] Stremersch S, Wuyts S, Frambach RT. The purchasing of full-service contracts: an exploratory study within the industrial maintenance market. Industrial Marketing Management 2001; 30:1–12.
[18] Kumar R, Kumar U. A conceptual framework for the development of a service delivery strategy for industrial systems and products. The Journal of Business and Industrial Marketing 2004; 19(5): 310–319.
[19] Espling U, Olsson U. Partnering in a railway infrastructure maintenance contract: a case study. Journal of Quality in Maintenance Engineering 2004; 10 (4):248–253.
[20] Covey SR. The seven habits of highly effective people. Simon and Schuster, UK, 1999.
[21] Kumar R, Kumar U. Service delivery strategy: trends in mining industries. International Journal of Mining and Reclamation 2004; 18 (4):299–307.
[22] Markeset T, Kumar U. Product support strategy: conventional versus functional products. Journal of Quality in Maintenance Engineering 2005; 11(1):53–67.
[23] Parida A, Kumar U. Maintenance performance measurement (MPM): issues and challenges. Journal of Quality in Maintenance Engineering 2006; 12(3): 239–251.
[24] Parida A. Development of a multi-criteria hierarchical framework for maintenance performance measurement-concepts, issues and challenges. PhD Thesis, Luleå University of Technology, 2006.
[25] Kaplan RS. Accounting lag: The obsolescence of cost accounting systems. California Management Review 1986; 28 (2):174–99.
[26] Kaplan RS, Norton DP. The balanced scorecard-measures that drive performance. Harvard Business Review 1992; 71–79.
[27] Neely AD. Gregory M, Platts K. Performance measurement system design: a literature review and research agenda. International Journal of Operations and Production Management 1995; 15 (4): 80–116.
[28] Parida A. Chattopadhyay G, Kumar U. Multi criteria maintenance performance measurement: a conceptual model. Proceedings of the 18th International Congress on Condition Monitoring and Diagnostic Management (COMADEM,} Cranfield University, UK 2005; 349–356.
[29] Dhillon BS. Design reliability: fundamentals and applications. CRC Press LLC, New York, 1999.
[30] Dhillon BS. Engineering maintenance: a modern approach. CRC Press LLC, Florida, 2002.
[31] Markeset T, Kumar U. Integration of RAM and risk analysis in product design and development work processes. Journal of Quality in Maintenance Engineering 2003b; 9(4):393–410.
[32] Thompson G. Improving maintainability and reliability through design. Professional Engineering Publishing. UK, 1999.
[33] Moss MA. Designing for minimal maintenance expense. Marcel Dekker, New York, 1985.
[34] Markeset T, Kumar U. Application of LCC techniques in equipment selection. In proceedings of 10th MPES Symposium 2000; 575– 580.
[35] Lodewijks G. Strategies for automated maintenance of belt conveyer systems. Bulk Solids Handlings 2004; 24 (1):16–22.
[36] Kahn J, Klemme-Wolf H. Overview of MIMOSA and the open system architecture for enterprise application integration. E-Proceedings of the International seminar on Intelligent Maintenance, Arles, France, July 15–17, 2004.
[37] Thomas B, Denis R, Jacek S, Jean-Pierre T, Noureddine Z. PROTEUS – an integration platform for distributed maintenance systems. Proceedings of the 17th European Congress 2004; May: 333–341.
[38] Baptise J. A case study of remote diagnosis and e-maintenance information system. e-Proceedings of Intelligent Maintenance System Arles, France 2004; 15–17 July.
[39] Wang X, Liu C, Lee J. Intelligent maintenance based on multi-sensor data fusion to web-enabled automation systems. E-Proceedings of the International seminar on Intelligent Maintenance, Arles, France, July 15–17, 2004.
[40] ISO/IEC 15288, Systems engineering: System life cycle processes. International Organization for Standardization, Geneva Commission Electro-technique Internationale, Geneva 2002.

48

Maintenance Models and Optimization

Lirong Cui

School of Management and Economics,
Beijing Institute of Technology, Beijing, 100081, P.R. China

Abstract: In this chapter, maintenance models and policies, optimal problems, and related techniques are summarized, based on two recent survey papers and the latest research papers. The summary is done in terms of classification of the discussed problems, but some important ones are emphasized in detail. Finally, future developments and some new trends in the subject of maintenance are presented. The use effectiveness of a system depends not only on its reliability but also on maintainability, which makes the products or systems more competitive. In this chapter, we shall give a review for maintenance models and their optimization.

48.1 Introduction

Nowadays many systems, such as production lines, weapon equipment, nuclear power stations, devices, vehicles, aircraft, *etc*., have become more and more complex. The costs of their usage are also getting even higher than before. Maintenance has to be carried out in order to keep these systems' performance close to the level of the original design. Most systems used in practice are subject to deterioration with usage and age. For those deteriorated systems, maintenance, such as monitoring, repairs, and replacements, can result in extending their usage lifetimes and keeping the quality of operations, reducing the cost of operations and preventing the occurrence of system failures. Thus the study of maintenance has become more interesting over the past decades.

The subject of maintenance has been widely studied over the past several decades, and it is still an interesting topic because of its importance and usefulness. Maintenance models are the basis of any maintenance quantitative analysis, which can be used to analyze and evaluate the performances of systems. There has been a lot of literature on research into maintenance problems so far. Several scholars have published survey or review papers to summarize maintenance research results. In this chapter, in order to present some new points of view on maintenance models and their optimization, the author will focus more on recent research papers on maintenance and two recent review papers, one by Wang [53] and another by Dekker *et al*. [18].

The aims of the chapter are to survey the important research on maintenance problems, including maintenance models, maintenance polices, maintenance optimization, and others. Based on those and the author's point of view, the chapter will point out some new trends in the subject.

In practice, maintenance is divided into two major classes: one is so-called corrective maintenance (CM), the other preventive maintenance (PM). Corrective maintenance aims to restore the system to a specified condition when the system fails. Preventive maintenance aims to retain or restore the system in a specified condition when the system is operating. Here maintenance will be a general term and may represent either corrective maintenance or preventive maintenance. In this chapter, many terms used in the subject of maintenance are well known and are not here defined, otherwise they are defined before they are used.

Maintenance models are the basis of any maintenance quantitative analysis, so first let us look at which factors will affect the maintenance models. The following ten factors are often discussed, which distinguish the maintenance models in essential.

1. Maintenance polices: for example, age replacement, block replacement, failure limit, *etc*.;
2. System structures: for example, series structure, parallel structure, *k*-out-of-*n* structure, *etc*.;
3. Maintenance degree: for example, perfect maintenance, imperfect maintenance, minimal maintenance, *etc*.;
4. Optimization criteria: for example, minimize cost rate, maximize availability, maximize reliability, *etc*.;
5. Distributions of components: for example, exponential distribution, Weibull distributions, gamma distributions, *etc*.;
6. Shut-off rules: for example, for multi-unit systems, when some units fail, some other units may continue to operate or be in states of suspended animation with the system down—a different shut-off rule results in different availability;
7. System information: for example, perfect, imperfect, continuous, inspection and monitoring, *etc*.;
8. Model types: for example, continuous and discrete;
9. Maintenance action distributions: for example, exponential distribution, Weibull distributions, phase-type distribution, *etc*.; and
10. Other assumptions: for example, independence or dependence among distributions or factors.

Systems we shall discuss in this chapter consist of units (components), which may be of two kinds: single-unit systems and multi-unit systems. If a system can be maintained we call it a repairable system. We assume that any system discussed in the chapter has only two possible kinds of states: working state and failure state: this applies to the components of the system as well. The maintenance indexes for the system are usually as follows,

1. *Availability:* There are several kinds of availability indexes. For example,

2. *Point availability:*

$A(t) =$

$P\{$*the system is in a working state at time* $t\}$.'

Limit availability:

$$A = \lim_{t\to\infty} A(t)$$
$$= \lim_{t\to\infty} P\{\text{the system is in a working state at time } t\},$$

if the limit exists,

Average availability over (t_1, t_2):

$$A_{(t_1,t_2)} = \frac{1}{t_2 - t_1}\int_{t_1}^{t_2} A(u)du \text{ , and}$$

Limit average availability:

$$A_{AV\infty} = \lim_{t\to\infty}\frac{1}{t}\int_0^t A(u)du,$$

if the limit exists.

3. *Reliability:* Several indexes have been used to describe the system reliability related performances. For example, *repairable system reliability:*

$R(t) = P\{$*the system never fails before time* $t\}$.

Mean time to first failure MTTFF

Mean time to failure MTTF
Mean up time MUT
Mean down time MDT
Mean time between failures MTBF

4. *Capacity of repair:* How many repairmen or devices can be used in the repairable system? In general, the following indexes are used:
   Pointwise busy probability of repairmen:
   $B(t) = P\{\text{the repairmen or devices are busy at time } t\}$,
   Steady-state busy probability of repairmen:
   $B = \lim_{t\to\infty} B(t)$
   $= P\{\text{the repairmen or devices are busy at time } t\}$,
   if the limit exists.
   Mean time to repair: MTTR.

5. *Failure frequency:* This reflects the frequency of failures occurring in the repairable systems, which can be depicted by the following indexes:
   The average number of failures occurring in the time interval $(0,t]$, :
   $M_i(t) = E\{N(t) \mid X(0) = i\}$,
   Pointwise failure frequency:
   $$m_i(t) = \frac{d}{dt} M_i(t), \text{ , and}$$
   Steady-state failure frequency:
   $$m_i = \lim_{t\to\infty} m_i(t) = \lim_{t\to\infty} \frac{d}{dt} M_i(t),$$
   if the limit exists.

   Here, $N(t)$ is the number of failures of the system occurring in the time interval, and $\{X(t), t \geq 0\}$ is a stochastic process describing the repairable system.

The remainder of this chapter is organized as follows. Section 48.2 reviews the previous important contributions to the subject of maintenance. In this chapter the author mainly focuses on recent papers and the two recent survey papers mentioned above. In Section 48.3, maintenance models are presented and summarized in some categories for both single-unit and multi-unit systems. Section 48.4 presents the maintenance policies in terms of classes. Section 48.5 reports on maintenance optimization for various categories of maintenance problems; also techniques of optimization are discussed. In Section 48.6 other issues related to the subject of maintenance are considered. Section 48.7 discusses future developments and new trends, based on a literature survey and the author's point of view.

48.2 Previous Contributions

During the past several years, the subject of maintenance has continued to be a topic of growing interest. For example, some papers appeared in the journal IEEE Transactions on Reliability. Zhang [56, 57] uses a geometric process to describe a deteriorating simple repairable system with two and three states, respectively, and then the optimal policies are given in terms of the minimal average cost. Bunea and Bedford [9] consider the effect of model uncertainty on maintenance optimization; they point out that the optimal replacement interval and optimal replacement cost can be dramatically non-optimal when the wrong model is used. Cui *et al.* [16] study optimal maintenance problems to maximize the expected system lifetime under fixed resources when repair actions can only be selected between perfect and minimal repairs. Perez-Ocon and Montoro-Cazorla [37] consider a repairable system with phase-type distributions for lifetime of system and repair times. Cassady *et al*. [10] use the simulation method to analyze a generic model of system availability under imperfect maintenance, in which Kijima's first virtual age model is used. Attardi and Pulcini [3] discuss statistical inference on a repairable model with bounded failure intensity. Wang and Trivedi [52] study the computation for steady-state mean time to failure for non-coherent repairable systems. Wu and Clements-Croome [55] study optimal maintenance policies under different operational schedules, in which three models are presented and cost functions are more developed. Zheng *et al.* [59] consider single-unit Markov repairable models with repair time omission, in which some ideas

result from the modeling of ion channels. Jiang *et al.* [27] give a review of the assessment of repairable-system reliability using proportional intensity models.

Some papers appeared in the European Journal of Operational Research. For example, Chien and Sheu [13, 14] discuss an extended optimal age-replacement policy with minimal repair of a system subject to shocks. Smidt-Destombes *et al.* [47] study the system availability which depends on maintenance policy, spare part inventory level, repair capacity and repair job priority setting. Jaturonnatee *et al* [26] consider optimal preventive maintenance of leased equipment with corrective minimal repairs, in which the optimal parameters of preventive maintenance policy are given. Grigoriev *et al.* [22] deal with a scheduling maintenance service system to model and solve its periodic maintenance problem. Zhang [58] corrects Sheu's [46] wrong statement for a bivariate optimal replacement policy for a repairable system. Quan *et al* [41] use an evolutionary algorithm to discuss the multi-objective preventive maintenance schedules. Crowder and Lawless [15] discuss preventive maintenance using wear process to describe system degradation. Bai and Pham [4] present some results for multi-component systems on renewable full-service warranty policies. Tang and Lam [50] propose a δ-shock maintenance model for a deteriorating system, in which it is assumed that shocks arrive according to a renewal process and the inter-arrival times of shocks have a Weibull or gamma distribution. The threshold values follow an increasing geometric process. In this model, attention is paid to the "frequency" of shocks rather than the accumulated amount of damage of shocks, which is different from other shock models. Ribeiro *et al.* [43] study the joint optimization of maintenance and buffer size in a manufacturing system using a mixed integer linear programming model. Glazebrook *et al* [21] discuss maintenance policy for a team of R repairmen and M non-identical machines by using a Markov decision process. Liao *et al.* [33] study the condition-based maintenance policies in which monitoring is performed continuously for a degrading system. Chien *et al.* [13, 14] consider an extended optimal replacement model of systems subject to shocks, in which the probability of a type II failure is permitted to depend on the number of shocks since the last replacement. Wang and Pham [54] study the availability and maintenance of series systems subject to imperfect repair and in which the failures and repairs are correlated. Vaughan [51] addresses inventory policy for spare parts under failure replacement and preventive maintenance. Juang and Anderson [28] consider a Bayesian theoretic approach to determine an optimal adaptive maintenance policy with minimal repair, in which some statistical inferences are given for maintenance problems. Apeland and Scarf [1] use the fully subjective approach to modeling inspection maintenance. Hsieh and Chiu [25] discuss the optimal maintenance policy for a multi-state deteriorating standby system, in which the optimal number of standby components required in the system is given. Bloch-Mercier [8] proposes a preventive maintenance policy with sequential checking procedure for a Markov deteriorating system, in which the deteriorating degree is measured with a finite discrete scale; repairs follow general distributions, and failures are instantaneously detected.

In the journal Reliability Engineering and System Safety there also are some papers related to maintenance. For example, Qu *et al.* [40] discuss the problems of enhanced diagnostic certainty using information entropy theory. Kim *et al.* [30] deal with the warranty and discrete preventive maintenance problem, in which the model determines when preventive maintenance actions should be carried out at discrete time instants over the warranty period. Castro and Alfa [11] consider two models to describe maintenance policy based on the lifetime of a system, in which the phase type distribution is used as the system lifetime distribution. Perez-Ocon and Montoro-Cazorla [38] discuss the cold standby repairable system with operational and repair times also following phase type distributions. Doyen and Gaudoin [19] consider two models for imperfect repair of systems, in which the repair effects are described by failure intensity and system virtual age. Smidt-Destombes *et al*. [48] study the interaction between preventive maintenance policy, spare part

inventories and repair capacity for a *k*-out-of-*n* system with exponentially distributed component lifetimes and repair times. Moustaf *et al* [35] deal with a maintenance model for a multi-state semi-Markovian deteriorating system, in which the control limit policy and the policy-iteration algorithm are used to find optimal maintenance policies that minimize the expected long-run cost rate of the system. Pongpech and Murthy [39] study the leased equipment periodic preventive maintenance policy, in which the tradeoff between penalty and maintenance costs is achieved. Rajpal *et al.* [42] propose an artificial neural network for modeling the reliability, availability, and maintainability of a repairable system.

Of course, in addition to the papers appearing in the three main reliability journals, many articles related to the subject of maintenance have been published. Because of the limitation of contents of this section, they can not be listed totally, even some papers that appeared in the three journals. The author will try his best to consider these contributions, including those important ones before 2002, in the next sections. In fact, the maintenance problems discussed in published papers are mostly related to the ten factors stated in Section 48.1, the different factors considered result in the different papers.

48.3 Maintenance Models

Since there have been numerous papers and books on maintenance models in the past decades, in this chapter the author will divide them into several categories in order to describe them clearly and concisely. At the same time, some very important maintenance models will be emphasized as typical representations. In this chapter, maintenance models are classified in terms of the following categories:

1. Time models,
2. Degradation degree models,
3. Cost models,
4. Shock models,
5. Inspection models.
6. Reliability/availability models
7. Warranty models.

The systems related to maintenance problems consist of a single unit or multi-units. The single-unit system is a special case of a multi-unit system, but there exist some different aspects for repairable systems. The maintenance models for these systems have some different points shown in Table 48.1.

Table 48.1. Different points for both systems

System No	Single-unit System	Multi-unit System
1	Non-structure	Structure
2	Without shut-off rules	Shut-off rules
3	Non-dependence, or failure dependence or block/opportunistic policies, exists	Dependence, Interactions—some dependences can be assumed among units (components)
4	One repair facility	One or more repair facilities
5	Non-repair priority	Some repair priority may exist
6	Non-detecting	Sometimes, need to detect which component fails

In the following, the models classified above are detailed, but single-unit and multi-unit repairable systems will not be distinguished.

1. *Time model*. In this model some units of the repairable system are repaired or replaced at a specified time instant, such as the so-called age-dependence model including PM and CM, the periodic repair model, *etc*. The characteristic of this kind of model is a specified repair time instant. In this model, the repair effects are used extensively, in which the concepts of minimal, imperfect and perfect repair are employed. The effects of maintenance can

be described by the lifetime (such as virtual age), reliability, or failure rate of the system or component. The optimization of problems based on the time model is to find optimal repair time instants to minimize some objective function, usually on cost concerns, or maximize some reliability/ availability function. A typical paper on this kind of model is by Barlow and Hunter [5]. Later, many extensions have been done on this kind of model, however, these extensions are with two decision variables at most for optimization.

2. *Degradation degree models*. In this model units can be repaired or replaced at a predetermined system or component deteriorating level, such as the so-called failure limit model, failure number limit model, *etc*. As mentioned before, the degree of deterioration can be described by the failure rate, reliability, age or virtual age, accumulated damage, *etc*. The idea of the model is very natural, because when the system deteriorates, it should be repaired in order to maintain the system reliability or availability. The various measurements of degree of deterioration used result in different detailed models, but they should be equivalent to each other in essence: for example, a predetermined failure rate corresponds to a predetermined age or virtual age, and *vice versa*. The difference is only in the measure of the degree of deterioration for these kinds of models, perhaps needing different efforts of computation and discussions on properties of the models. An early example of this kind of model was presented by Bergman [7].
3. *Cost models*. In this model the main focus is on maintenance costs, and the maintenance actions, strategies, and optimizations depend strongly upon the costs. For example, Seo and Ahn [44] build an artificial neural network with 24 product attributes as input layer nodes, two hidden layers with 20 and 18 nodes respectively, and one output layer node to describe maintenance costs. Other examples of this kind of model are regression models for maintenance related costs, which have appeared in many books. Although many maintenance models put some costs as optimal objective functions, the author does not want to classify them as cost models in general, because these models focus mainly on maintenance actions and strategies. Of course, the model classification depends on the purpose of discussion and any classification rules can be changed depending on the situation.
4. *Shock models*. In general, there are two ways to describe the rules of occurrences of failures for repairable systems. One is to assume that the lifetime(s) of system (components) have followed some distribution(s); another is to assume that the system (components) is (are) subject to shocks arriving according to some stochastic process. The second way has attracted more attention recently, because many practical situations can be suitably described by these assumptions. The shock models are formed this way. For example, Lam [32] introduces so-called 'geometric processes' to describe these phenomena. For another example, the physical damage measure process $\{X(t), t \geq 0\}$ is a compound process,

$$X_t = \sum_{i=1}^{N(t)} Y_i,$$

where $\{N(t), t \geq 0\}$ is a counting process and Y_i is the damage measure for the ith shock arriving for the system. This kind of model is usually more complicated in its mathematical description and manipulation.
5. *Inspection models*. To apply any maintenance actions we first need to find which component fails or decide how to know whether the repairable system operates or not. Inspection models focus on the inspection procedure, inspection method, inspection input, information from inspection, *etc*. The inspection factor in both theory and

practice is more important for maintenance actions and optimal strategy options. In general, there are two kinds of inspections: continuous and discrete inspections. For example, the classical failure (hazard) rate is defined as

$$\lambda(t) = \lim_{t\to\infty} \frac{1}{h} P\{T \in [t, t+h] \mid T > t\},$$

where T denotes the system lifetime. Arjas [2] proposed a so-called hazard rate process which describes a multi-unit system's failure rate. The process is defined as follows:

$$\Lambda_t = \lim_{t\to 0} \frac{1}{h} P\{T \in [t, t+h] \mid \{T > t\} \cap \mathcal{F}_t\}.$$

Where filtration is given by

$$\mathcal{F}_t = \sigma(T \le t, Z \le t, T_i \le t, i = 1, 2, \cdots, n),$$

and $T_i, 1 \le i \le n,$ are the unit failure times, n is the number of units, and Z is the occurrence time of a shock. He also defined (and referred to as "observed hazard rate"):

$$\Lambda_t^0 = \lim_{h\to 0} \frac{1}{h} P\{T \in [t, t+h] \mid \{T > t\} \cap \mathcal{F}_t^0\},$$

where the filtration $\mathcal{F}_t^0$ is determined by other observed information. Another example is Barros *et al*. [6] who study optimal replacement times using imperfect monitoring information. Inspection models can be extended in many ways, but perhaps the models become more and more complicated, which is inconvenient in theoretical analysis and practical use.

6. *Reliability/availability models*. In this model, the reliability or availability is found for repairable systems under some maintenance assumptions. The characteristic of the model is the focus on the system reliability or availability in most situations. This model is a basis for many maintenance optimization questions, and it has been studied a lot over the past decades. Research interest in this direction is still hot now. For example, Zheng *et al.* [57] establish some new maintenance models in which reliability and availability are mainly concerned, because people must pay more attention to reliability and availability for any new maintenance models. The author believes that this kind of model can be extended greatly, driven by practical situations and theoretical interest. Further examples are various virtual age models, in which the virtual age receives attention in order to track system reliability. Table 48.2 lists various models.
7. *Warranty models*. The model is built in terms of problems related to maintenance during a product warranty period. The research into this kind model has been greatly driven by practical situations, and it can be used in making practical product warranty policies. As Kim *et al.* [30] pointed out, the warranty period offered has been progressively getting longer. The warranty periods for cars have been changed from three months, one year, and three or five years since the thirties, sixties, and currently, respectively. Many maintenance actions can be carried out in order to reduce the costs of buyers and manufacturers, so that the related models must be studied more. For example, Murthy and Djamaludin [36] give a review on warranty literature over the period 1990–2001. Maintenance is one of most important factors in warranty study, and our warranty models focus on maintenance actions and strategies in the product warranty period instead of other warranty considerations.

The classification of maintenance models given above differs from that in the previous literature, and the maintenance models for single-unit and multi-unit systems are not partitioned on the basis of different points for the two systems.

Similar to other literature, Wang [53] lists the maintenance models for repairable systems in the following categories:

1. Age-dependent PM model,
2. Periodic PM model,

Table 48.2. Various virtual age models

Proposed by	Virtual age after repair $v(t_i+0)$	Notes
Kijima [29]	$v(t_{i-1})+\theta_i X_i$	θ_i —degree of repair
Kijima [29]	$\theta_i[v(t_{i-1})+X_i]$	X_i —lifetime during the ith operating phase
Stadje and Zuckerman [49]	$v(t_{i-1})+X_i-d$	d —between 0 and $v(t_{i-1})$
Finkestein [20]	$g(v(t_{i-1})+X_i)$	$g(\bullet)$ —general positive function
Guo and Love [24]	$(1-w_i)v(t_{i-1})+\theta_i X_i$	$h(\bullet)$, $\psi(\bullet)$, $q(\bullet)$ are positive functions
Dagpunar [17] Makis [34]	$f(v(t_{i-1}), X_i)$	
Guo *et al*. [23]	$h(\psi[v(t_{i-1})]+q(X_i))$	

3. Failure limit model,
4. Sequential PM model,
5. Repair limit model,
6. Distribution-free and semi-parametric model, and
7. Effects of repair model.

The classification of maintenance models may be done in many ways, but the criterion of better maintenance models is whether they can describe the practical situation correctly and be used conveniently. Each class of maintenance model has its own focus and characteristic, which are real points to be considered in both theory and practice.

48.4 Maintenance Policies

As mentioned before, the maintenance policy, *i.e.*, when and how to repair the failed system, is one of the important factors which affect the maintenance results. The meanings of terms for policy and strategy are the same as for maintenance problems in this chapter. Before classification, some important definitions need to be made. The repair action in general contains replacement and mending actions. The effects of repair for a failed system or components can be measured by the degree of repairs. The degree of repairs, denoted by θ, is between 0 and 1, and when $\theta=0$, it is called maximal repair or perfect repair, or replacement. When $\theta=1$, it is called minimal repair, *i.e.*, under minimal repair the failure rate after repair is the same as that just before failure. When $0<\theta<1$, it is called imperfect repair. Another important concept is so-called virtual age, which was first proposed by Kijima [29]. The maintenance policy (strategy) can be classified into the following classes. Of course, like maintenance models, the different classification standards result in different classes.

1. Time-dependent maintenance policy,
2. Degradation degree-dependent maintenance policy,
3. Mixed time and deteriorating degree dependent maintenance policy,
4. Detecting information-dependent maintenance policy,
5. Block maintenance policy,
6. Priority maintenance policy, and
7. Other maintenance policy.

In the following, the listed models above will be detailed according to their characteristic, advantages, and possible extension directions, *etc*.

1. *Time-dependent maintenance policy*. Under this policy, maintenance actions can be done at specified time instants; examples include age-dependent policy, periodic policy, sequential policy, *etc*. This policy has been studied more because of its intuitive and practical operation; on the other hand, it can be dealt with relatively easily in theory. It also may be extended to more than two time instants. For example, the maintenance action is done when the first, second, or third time-event happens, whichever occurs first. The detailed models may have more, but the simplest maintenance policies depend on a single time instant. This given time instant may be constant or a random variable. For example, the preventive maintenance time instant is given by

$$T = \begin{cases} X, & X \le t_0, \\ t_0, & X > t_0, \end{cases}$$

where t_0 is a predetermined time, and X is the lifetime of system. Thus, T is a random variable.

2. *Degradation degree-dependent maintenance policy*. Under this policy, the maintenance actions will be done at the time instant when the system degradation degree reaches a specified level. Examples include failure limit policy, repair limit policy, *etc*. This maintenance policy is very natural because when the deteriorating system becomes older or has accumulated more damage, maintenance actions should be carried out to rejuvenate the system. The threshold of degradation degree may be measured by the failure rate (hazard rate), reliability, age or virtual age, availability, number of failures, interval times of failures, *etc*. For example,

$$T = \inf_{t \ge 0} \{t : r(t) \ge r_0\},$$

is a time instant of maintenance action taken, where $r(t)$ is the failure rate of system and r_0 is a predetermined constant. In general, it is assumed that $r(t)$ is an increasing function in t.

3. *Mixed time and deteriorating degree dependent maintenance policy*. Under this policy, maintenance actions can be done at specified time instants or at the time instant when the system degradation degree reaches a specified level, whichever occurs first. For example, maintenance actions can be done at the following time instant T,

$$T = \min\{T_1, T_2\},$$

where

$$T_1 = \inf_{t \ge 0} \{t : r(t) \ge r_0\},$$

$$T_2 = XI_{\{X \le t_0\}} + t_0 I_{\{X > t\}}.$$

The characteristic of the policy is the combination of time dependent and degradation degree maintenance policies.

4. *Detecting information-dependent maintenance policy*. Under this policy, the maintenance action is carried out at a time instant which is determined in terms of detected information about the system. The information detected may be of various kinds, such as complete information or partial information. For example, for an imperfect monitored two-unit parallel system consisting of statistically dependent units, the preventive maintenance policy is determined by a stopping rule in which the observed failure rate is a stochastic process. For details see Barros *et al.* [6]. This policy may be extended more in the future, because it is based on observed information, which is more realistic.

5. *Block maintenance policy*. This policy specifies that the maintenance action will be done when more than two components are maintained together. Examples include group and opportunistic maintenance policies. Here the meaning of block is not necessarily a real block of physically adjacent components but may instead be any set of components, regardless of their physical constitution, which is convenient to treat together. Thus, the characteristic of the policy is to carry out maintenance actions together for several components, although the individual components may

receive different maintenance actions. For example, for a repairable parallel system consisting of five independent subsystems, the maintenance actions can be done at time

$$T = \min_{i \neq j \neq k} \max\{T_i, T_j, T_k\},$$
$$i, j, k \in \{1, 2, 3, 4, 5\},$$

where $T_1, T_2, \cdots, T_5$ are failure time instants for subsystems 1,2,…,5, respectively. The detailed maintenance actions are as follows, because of physical limitations such as the failed subsystem's temperature. The first and second failed subsystems are repaired, and the third failed subsystem is replaced. This policy is adopted perhaps because of costs, limitations of real situation, *etc*. The policy may be more applicable in real situations, because of dependence among costs, failures and other factors. Of course, the policy is just for multi-unit systems. Extensions of the policy may be done in terms of classes of units, relationship among costs, different mission phases, *etc*.

6. *Priority maintenance policy*. For multi-unit repairable systems, the repair facility may face several failed components at one time instant. Under this policy, it is specified which failed component should be repaired first, second, *etc*. That is, some components have priority to be treated in maintenance actions. For example, for a repairable consecutive-*k*-out-of-*n* system, the positions of failed components play important roles for maximizing the system availability, so that there necessarily exist some priority rules for this kind of repairable system. System performance, such as reliability or availability, may be improved greatly through such a policy. In fact, in any maintenance policy, some order of treatments for failed components exists, although in most situations people do not specify it explicitly. The policy may be extended to various priority rules like that in queuing theory and practical operation sequences.
7. *Other maintenance policies*. In addition to the policies mentioned above, here we classify the remaining maintenance policies as "other maintenance policy". In fact, many policies have appeared in the literature, which are driven by both practical applications and theoretic researches. Since maintenance policies involve many factors, which can be combined in a variety of ways, numerous maintenance policies are possible, although the class of maintenance policies may not increase greatly. On the other hand, a maintenance policy can be classified using a variety of criteria, such as continuous maintenance policy and discrete maintenance policy, PM policy and CM policy, replacement maintenance policy and imperfect repair maintenance policy, *etc*.

For most maintenance policies, there exist optimal maintenance policies, which maximize the system reliability and availability or minimize the failure frequency and downtime, maintenance costs, *etc*. It is clear that the optimal maintenance policy depends on the objective function, *i.e.*, the system improvement objectives determine the optimal maintenance policy parameters.

Figure 48.1 shows various factors about which a maintenance policy should mainly be concerned.

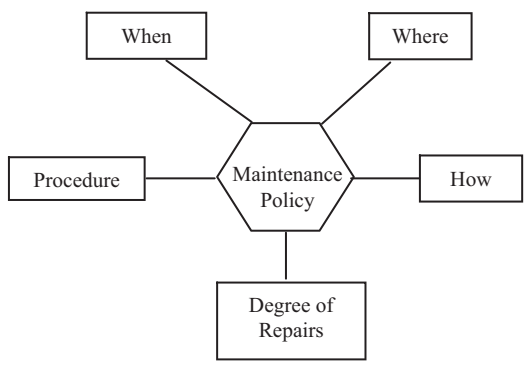


Figure 48.1. Various main factors concerned in a maintenance policy

48.5 Maintenance Optimization and Techniques

When various factors including maintenance policy and various assumptions which determine the maintenance models are defined, a maintenance model may be established after some efforts. Once a maintenance model is known, people can work on it in a mathematical way, *i.e.*, to find solutions and explain the real physical problems in terms of the solutions. In maintenance problems, it is usual to do some optimizations, and before finding the optimal solutions, we need to know the objective functions. The objective functions are usually determined by the maintenance purposes. Generally speaking, there are two kinds of optimization function: single-objective function and multi-objective functions. In addition, before finding optimal solutions, all constraints need to be considered, and then a set of constraint equations is built. In the literature, many objective functions are related to maintenance costs, such as the total average cost per time unit, the system reliability measures, *etc*.

For example, the following problem (refer to Kuo *et al.* [31], p. 333) is a single-objective function without constraints, which is an optimal planned-maintenance policy to be determined for preventive replacement of systems, the objective function is the replacement cost-rate. That is, find

$$\min_{t_p} C(t_p) = \frac{C_{pr}R(t_p) + C_{fr}(t_p)}{M(t_p) + t_{dpr}R(t_p) + t_{dfr}F(t_p)},$$

where

$C(t_p)$ --- *total expected replacement cost-rate*,

C_{pr} --- *cost of a preventive replacement*,

C_{fr} --- *cost of a failure replacement*,

$M(t_p)$ --- *mean-life during cycle* $[= \int_0^{t_p} R(t)dt]$,

$R(x)$ --- *reliability function* $[= 1 - F(x)]$,

t_{dpr} --- *mean down time for preventive replacement*,

t_{dfr} --- *mean down time for failure replacement*,

and

t_p --- *preventive replacement age.*

The optimal times t_p and t_p^* are found by minimizing $C(t_p)$ by the usual calculus method.

A problem involving a single-objective function with constraints is as follows. Find

$$\min_{t_p} C(t_p) = \frac{C_{pr}R(t_p) + C_{fr}(t_p)}{M(t_p) + t_{dpr}R(t_p) + t_{dfr}F(t_p)},$$

subject to

$$A(t_p) = \frac{\text{exp}ected\ operating\ time\ in\ the\ cycle}{\text{exp}ected\ cycle} = \frac{M(t_p)}{M(t_p) + t_{dpr}R(t_p) + t_{dfr}F(t_p)} \geq A_0.$$

where A_0 is the required minimal availability. For another example, Chelbi and Rezg [12] consider a repairable production unit subject to random failures, in which the buffer stock and optimal maintenance time are given for minimizing the total average cost per time unit and satisfying the availability constraint.

Similarly, a problem involving a multi-objective function without constraints, for example, is as follows. Find

$$\min_{t_p} C(t_p) = \frac{C_{pr}R(t_p) + C_{fr}(t_p)}{M(t_p) + t_{dpr}R(t_p) + t_{dfr}F(t_p)},$$

$$\max_{t_p} A(t_p) = \frac{M(t_p)}{M(t_p) + t_{dpr}R(t_p) + t_{dfr}F(t_p)}.$$

A problem involving a multi-objective functions with constraints, for example, is as follows. Find

$$\min_{t_p} C(t_p) = \frac{C_{pr}R(t_p) + C_{fr}(t_p)}{M(t_p) + t_{dpr}R(t_p) + t_{dfr}F(t_p)},$$

$$\max\ R(x,h) = \frac{R(x+h)}{R(x)}.$$

subject to

$$A(t_p) = \frac{M(t_p)}{M(t_p) + t_{dpr}R(t_p) + t_{dfr}F(t_p)} \geq A_0.$$

where $R(x,h)$ is mission reliability, *i.e.*, the probability that a system finishes a mission of length h which begins at age x.

The techniques for optimization in maintenance problems have received some attention. In general, there are two ways to find the optimal solutions. One way is by metaheuristic algorithms, such as genetic algorithms, tabu search, and simulated annealing techniques. Here the author wants to emphasize the genetic algorithm which has been used more recently. For example, in 2006, the journal Reliability Engineering and System Safety published a special issue on the applications of genetic algorithms in reliability problems. There is no doubt that genetic algorithms can be used in optimal maintenance problems. Another method uses exact algorithms, such as dynamic programming, implicit enumeration, lexicographic search procedure, integer programming, mixed integer programming, nonlinear programming techniques, *etc*. Even though many optimal techniques have been known, new optimal techniques are still developed, because each individual optimal problem has its own characteristics. Some optimal techniques can be proposed in terms of some individual special characteristic. On the other hand, we can list the optimal techniques in another way as follows:

1. Conventional approaches such as the usual calculus method,
2. Simulation approaches,
3. Algorithms,
4. Artificial neural networks,
5. Programming methods such as linear programming,
6. Fuzzy theory approaches.

When the objective and constraints of a practical problem are precisely known, then the model can be built in a precise manner. However, in most real-life situations, the objectives and the constraints are not precisely defined; sometimes the resource constraints are not very rigid. Under such imprecise conditions, the classical optimization approach does not serve much purpose. The fuzzy approach is very useful in dealing with qualitative statements, vague objectives, and imprecise information. For details on this approach, one can refer to Kuo *et al.* [31].

To summarize the section: if the optimal problem has been built, then it becomes an optimal mathematical problem; one can find solutions to the problem by using any optimal technique. Sometimes, for optimal problems involving multi-objective functions, one needs to understand the meaning of the optimal solutions, because these so-called optimal solutions differ from those of the optimal problems involving a single-objective function.

48.6 Maintenance Miscellanea

Maintenance models involve many factors. Any maintenance model is established under a particular environment or situation. In this section, we will discuss practical factors which may affect the maintenance model, such as maintenance management system, spares, maintenance software, maintenance costs, *etc*. We will also consider some other evaluation methods such as stochastic order for stochastic behaviors, optimal criterion, *etc*.

Now in many practical situations, the ERP (enterprise resource planning) system has been more and more used. As an important resource, the subject of maintenance can be included in the ERP system, or some software modules for maintenance models may be integrated into the ERP system. The decision-making on maintenance matters may be greatly affected by the ERP system. On the other hand, some new developments in the subject of maintenance can be input the ERP system, which may be more useful in practice. In a broad sense, the maintenance management system has more and more effect on maintenance decisions.

For inventory spares, it is no doubt that the quantity of spares and inventory allocation of spares have more effect on maintenance models if the models contain these factors. In fact, there is a great deal of research in the literature in this direction, and many companies have their own way to specify the related factors of spares. The study of spares still creates challenges in theory and practice in order to fit a variety of practical situations.

The cost factor for maintenance has been widely studied. Most maintenance related literature involves cost, but it seems that few maintenance models can be universal or fit many practical situations; they are more of theoretical interest. The author believes that more practical maintenance models related to costs need to be developed, because it is not that maintenance cost models are too complicated, rather they are too simple to describe real world situations properly. For example, different maintenance phases need different cost input intensities: changes in the optimal objective functions result in variable optimal cost solutions. Such examples can be given easily.

Comprehensive maintenance models need to consider more factors, which may increase the complexity of the models, but in the era of information this difficulty can be overcome. In fact, the use of maintenance models in most situations needs the help of computer programming, which is at least one of the reasons for the existence of much maintenance software in today's market.

Besides the factors mentioned above, we definitely need to consider some evaluation factors/methods which are not studied in detail in the previous sections.

In maintenance models, some indexes, such as the number of failures, age or virtual age, *etc.*, have random properties; they may be random variables or stochastic processes. Sometimes a comparison is needed among the various cases. For example,

$$N_1(t) \geq_{st} N_2(t), \text{ or } T_n^A \geq_{LR} T_n^B,$$

where $N_i(t)$ $(i = 1, 2)$ is the number of failures by time t for the ith maintenance policy. T_n^A *and* T_n^B are the virtual ages of a system under maintenance policies A and B, respectively, after the nth maintenance action.

The above inequalities can provide some information which the conventional comparison methods cannot. The stochastic order is a most useful approach to this kind of comparison, bringing new insight to understand the maintenance policy comparison. In addition, sometimes evaluation of the (joint) distribution function is difficult in maintenance models. We can study its stochastic properties, such as monotonicity, through the stochastic order. Although stochastic behaviors are sometimes studied by a distribution function and their characteristic values, the stochastic order is another effective approach. The stochastic order has many definitions. In general, the larger stochastic order, the hazard rate order, and the likelihood ratio order are used more often—one can refer to the book of Shaked and Shanthikumar [45]. The applications of stochastic order in maintenance models can provide more useful information for the related decision-making problems.

Multiple optimal criteria in maintenance models, for example, such as the joint consideration of cost, reliability and availability, can be studied more, which also makes the problems more complicated. Sometimes, some of the objective functions, for example g_i, g_j, g_k, should be maximized, whereas others, for example g_l, g_m, should be minimized. Then they can be put together as maximal (minimal) objective functions of the form

$$\max(g_i, g_j, g_k, -g_l, -g_m), \text{ or}$$

$$\min(-g_i, -g_j, -g_k, g_l, g_m).$$

Under the unified form, optimizing techniques such as algorithms can be used to find solutions. In this case, the solutions can be divided into four classes as follows.

1. *Optimal (positive-ideal) solution:* simultaneously results in the optimal value of each objective function,
2. *Nondominated (Pareto-optimal) solution:* denotes a noninferior solution and an efficient solution,
3. *Preferred solution:* a nondominated solution chosen by the decision maker through some additional criteria, and
4. *Satisfying solution:* a solution in a reduced subset of the feasible set.

Although several factors related to maintenance models have been discussed, there are some elements we have not mentioned or recognized in practical maintenance problems. The more factors

that are involved in maintenance models, the more applicable the models are, although the complexity, including finding the optimal solutions and description of models, becomes higher. The ideal maintenance model should be at least practically applicable and easily dealt with in mathematical sense. However, what constitutes an ideal maintenance model is a very debatable issue.

48.7 Future Developments

Maintenance models and their related problems have been discussed or reviewed in this chapter. As mentioned previously, the topic receives much attention because it has wide scope for research and study. On the other hand, maintenance models are the basis of any maintenance research. The classification of maintenance models made by the author in this chapter is different from that which has appeared in the literature, because each classification has its own criterion to distinguish the maintenance models. The author believes that some of the most important future developments in the subject of maintenance should be in the following directions.

1. *New models:* New maintenance models, such as those involving probability and fuzzy or vague set theory, can be developed to meet various real situations and extend the range of theoretical applications. On the other hand, as high-tech product applications, such as IC manufacture systems and bio-product manufacturing devices, become widespread, the new situations will bring some new maintenance policies and models naturally. The invention of new maintenance models can extend the old models and stimulate new maintenance techniques.
2. *New processes:* The description of lifetimes of components or a system is an important factor in considering maintenance problems. New distributions or new stochastic processes are definitely needed to meet this requirement. For example, shock models have been paid more attention recently; some new stochastic processes, such as aggregated stochastic processes, are presented in repairable system analysis. It is no doubt that new stochastic processes or newly extended stochastic processes are bringing some new light on the subject of maintenance. Here the author wants to mention that the hazard rate process (for example, Arjas [2]) has provided new understanding for repairable systems in terms of different information levels. This direction may be an interesting future development, although it may need good probability and stochastic process knowledge. Martingale techniques in particular may be used more in this approach.
3. *New techniques/approaches:* The techniques for establishing models and optimization of models are driven by the development of new maintenance models and problems. As new maintenance models are invented, the conventional approaches may not meet the changed situations, and new techniques will be proposed naturally. On the other hand, techniques in other disciplines may be transferred into the subject of maintenance in order to solve maintenance problems, including establishing new models and finding the optimal solutions for new maintenance problems. Here the author emphasizes that some new algorithms may be developed for finding quick solutions and easy handling.
4. *New optimization criteria:* The same problem can obtain totally different optimal solutions under different optimal criteria. New optimal criteria will definitely be developed in the future. Because the targets people aspire are changing, the criteria of problems need to be adjusted; thus new optimal criteria, especially multiple criteria, will be born naturally. In some situations, the optimal criteria are in contradiction with each other, which gives rise to the need to develop new so-called optimal or satisfying solutions. Meta-heuristic algorithms may be developed

further, although in general they cannot guarantee that the real optimal solutions will be obtained. In fact, heuristic algorithms are more versatile, which can fit more problems in various optimal criteria.

5. *Statistical inferences on repairable systems:* So far most research work on the subject of maintenance is on the application of probability and stochastic processes to maintenance problems, with little work on statistical inference on maintenance problems. In practice, maintenance systems have a lot of operation and repair data, which should be used more to analyze the maintenance systems. The author believes that statistical inference work has a large scope for development. Statistical work can correct maintenance models and analyze the properties of maintenance models, such as robustness, goodness-of-fit test, and model selection based on real data. This approach may need much more relation with computer simulation in the subject of maintenance. The difficulty of applying statistical methods may be one of the reasons that statistical inference work on maintenance has not been developed more, so that computer simulation may be a powerful approach in dealing with the data. In theory, any stochastic environment or situation can be simulated properly by computer. Of course, the simulation method can not give a precise solution, but a reasonably accurate one will usually be sufficient—better an approximate answer to the right question than an exact answer to the wrong one!
6. *Analysis of maintenance models:* Thousands of maintenance models have been proposed, but properties such as model robustness, models' sensitivity analysis, models' random properties, *etc*., are often not fully discussed. This kind of work may attract future research. The equivalence property of maintenance models should be studied, because many current maintenance models are equivalent to each other in some sense. For example, the effects of repairs can be described by failure rate, virtual age, reliability, *etc*, but these indexes have some well-known relationships, which reveals that related maintenance models are the same in some sense.
7. *Dependence among the model factors:* Dependence exists in real world maintenance, such as economic dependence, structural dependence, and stochastic dependence, which is pointed out by Dekker *et al.* [18]. In fact, more factors are now considered and the dependence among them can be discussed more too, which is the direction of further research in the subject of maintenance. Here the author emphasizes that modeling stochastic dependence is a very broad subject. One useful tool in this aspect is the Copula.

The author has tried to give a reasonably complete and an advanced chapter. However, inevitably, there will be some points of view of the researchers that have been overlooked, not included, or inadvertently not referenced. However, it is hoped that important points are at least not omitted.

Acknowledgement

The author would like to thank Professor Alan G. Hawkes for his help with the English of this chapter, but the responsibility rests with the author, if some errors still exist.

References

[1] Apeland S, Scarf PA. A fully subjective approach to modeling inspection maintenance. European Journal of Operational Research 2003; 148:410–425.

[2] Arjas E. The failure and hazard process in multivariate reliability systems. Mathematical Methods of Operational Research 1981; 6(4):551–562.

[3] Attardi A, Pulcini G. A new model for repairable systems with bounded failure intensity. IEEE Transactions on Reliability 2005; R54(4):572–582.

[4] Bai J, Pham H. Cost analysis on renewable full-service warranties for multi-component systems.

European Journal of Operational Research 2006; 168:492–508.
[5] Barlow RE, Hunter LC. Optimum preventive maintenance policies. Operations Research 1960; 8:90–100.
[6] Barros A, Bérengur C, Grall A. Optimization of replacement times using imperfect monitoring information. IEEE Transactions on Reliability 2003; R52(4):523–533.
[7] Bergman B. Optimal replacement under a general failure model. Advances in Applied Probability 1978; 10 (2):431–451.
[8] Bloch-Mercier S. A preventive maintenance policy with sequential checking procedure for a Markov deteriorating system. European Journal of Operational Research 2002; 147:548–576.
[9] Bunea C, Bedford T. The effect of model uncertainty on maintenance optimization. IEEE Transactions on Reliability 2002; R51(4):486–493.
[10] Cassady CR, Iyoob IM, Schneider K, Pohl EA. Ageneric model of equipment availability under imperfect maintenance. IEEE Transactions on Reliability. 2005; 54(4):564–571.
[11] Castro IT, Alfa AS. Lifetime replacement policy in discrete time for a single unit system. Reliability Engineering and System Safety May 2004; 84(2):103–111.
[12] Chelbi A, Rezg N. Analysis of a production/ inventory system with randomly failing production unit subjected to a minimum required availability level. International Journal of Production Economics 2006; 99:131–143.
[13] Chien YH, Sheu SH. Extended optimal age-replacement policy with minimal repair of a system subject to shocks. European Journal of Operational Research 2006; 174:169–181.
[14] Chien YH, Sheu SH, Zhang ZG, Love E. An extended optimal replacement model of systems subject to shocks. European Journal of Operational Research 2006; 175(1):399–412.
[15] Crowder M, Lawless J. On a scheme for preventive maintenance. European Journal of Operational Research 2007; 176(3):1713–1722.
[16] Cui Lirong, Kuo W, Loh HT, Xie M. Optimal allocation of minimal and perfect repairs under resource constraints. IEEE Transactions on Reliability 2004; R53(2):193–199.
[17] Dagpunar JS. Some properties and computational results for a general repair process. Naval Research Logistics 1998; 45:391–405.
[18] Dekker R, Schouten FD, Wildeman R. A review of Multi-Component Maintenance models with economic dependence. Mathematical Methods of Operational Research 1997; 45(3):411–435.
[19] Doyen L, Gaudoin O. Classes of imperfect repair models based on reduction of failure intensity or virtual age. Reliability Engineering and System Safety 2004; 84:45–56.
[20] Finkelstein MS. On some models of general repair. Microelectronics and Reliability 1993; 33(5):636–666.
[21] Glazebrook KD, Mitchell HM, Ansell PS. Index policies for the maintenance of a collection of machines by a set of repairment. European Journal of Operational Research 2005; 165:267–284.
[22] Grigoriev A, Klundert J, Spieksma FCR. Modeling and solving the periodic maintenance problem. European Journal of Operational Research 2006; 172:783–797.
[23] Guo R, Ascher H, Love CE. Generalized models of repairable systems–A survey via stochastic processes formalism. ONION 2000; 16(2):87–128.
[24] Guo R, Love CE. Bad-as-old modeling of complex systems with imperfectly repaired subsystems. Proceedings of the International Conference on Statistical Methods and Statistical Computing for Quality and Productivity Improvement, Seoul, Korea; August 17–19, 1995:131–140.
[25] Hsieh CC, Chiu KC. Optimal maintenance policy in a multistate deteriorating standby system. European Journal of Operational Research 2002; 141:689–698.
[26] Jaturonnatee J, Murthy DNP, Boondiskulchok R. Optimal preventive maintenance of leased equipment with corrective minimal repairs. European Journal of Operational Research 2006; 174:201–215.
[27] Jiang ST, Landers TL, Rhoads TR. Assessment of repairable-system reliability using proportional intensity models: A review. IEEE Transactions on Reliability 2006; R55(2):328–336.
[28] Juang MG, Anderson G. A Bayesian method on adaptive preventive maintenance problem. European Journal of Operational Research 2004; 155:455–473.
[29] Kijima M. Some results for repairable systems with general repair. Journal of Applied probability 1989; 26:89–102.
[30] Kim CS. Djamaludin I, Muethy DNP. Warranty and discrete preventive maintenance. Reliability Engineering and System Safety 2004; 84:301–309.
[31] Kuo W, Prasad VR, Tillman FA, Hwang CL. Optimal reliability design fundamentals and applications. Cambridge University press 2001.

[32] Lam Y. Geometric processes and replacement problem. Acta Mathematicae Applicatae Sinica 1988; 4:366–377.
[33] Liao Haitao, Elsayed EA, Chan LY. Maintenance of continuously monitored degrading systems. European Journal of Operational Research 2006; 175(2):821–835.
[34] Makis V, Jardine AKS. A note on optimal replacement policy under general repair. European Journal of Operational Research 1993; 69:75–82.
[35] Moustafa MS, Maksoud EYA, Sadek S. Optimal major and minimal maintenance policies for deteriorating systems. Reliability Engineering and System Safety 2004; 83:363–368.
[36] Murthy DNP, Djamaludin I. New product warranty: a literature review. International Journal of Production Economics 2002; 79:236–260.
[37] Perez-Ocon R, Montoro-Cazorla D. Transient analysis of a repairable system, using Phase-type distributions and geometric processes. IEEE Transactions on Reliability 2004; R53 (2):185–192.
[38] Perez-Ocon R, Montoro-Cazorla D. A multiple system governed by a quasi-birth-and-death process. Reliability Engineering and System Safety 2004; 84:187–196.
[39] Pongpech J, Murthy DNP. Optimal periodic preventive maintenance policy for leased equipment. Reliability Engineering and System Safety 2006; 91: 772–777.
[40] Qu LS, Li LM, Lee J. Enhanced diagnostic certainty using information entropy theory. Advanced Engineering Informatics 2003; 17:141–150.
[41] Quan G, Greenwood GW, Liu Donglin, Hu S. Searching for multiobjective preventive maintenance schedules: Combining preferences with evolutionary algorithms. European Journal of Operational Research 2007; 177(3):1969–1984.
[42] Rajpal PS, Shishodia KS, Sekhon GS. An artificial neural network for modeling reliability, availability and maintainability of a repairable system. Reliability Engineering and System Safety 2006; 91:809–819.
[43] Ribeiro MA, Silveira JL, Qassim RY. Joint optimization of maintenance and buffer size in a manufacturing system. European Journal of Operational Research 2007; 176(1):405–413.
[44] Seo K.K. and Ahn B.J., A learning algorithm based estimation method for maintenance cost of product concepts. Computer and Industrial Engineering 2006; 50:66–75.
[45] Shaked M, Shanthikumar JG. Stochastic orders and their applications. Academic Press, New York, 1994.
[46] Sheu, SH., Extended optimal replacement model for deteriorating systems. European Journal of Operational Research 1999, 112(3):503–516.
[47] Smidt-Destombes KS, Heijden MC, Harten AV. On the availability of a *k*-out-of-*n* system given limited spares and repair capacity under a condition based maintenance strategy. Reliability Engineering and System Safety 2004; 83:287–300.
[48] Smidt-Destombes KS, Heijden MC, Harten A. On the interaction between maintenance, spare part inventories and their capacity for a *k*-out-of-*n* system with wear-out. European Journal of Operational Research 2006; 174:182–200.
[49] Stadje W, Zuckerman D. Optimal maintenance strategies for repairable systems with general degree of repair. Journal of Applied Probability 1991; 28:384–396.
[50] Tang YY, Lam Y. A δ-shock model maintenance model for a deteriorating system. European Journal of Operational Research 2006; 168:541–556.
[51] Vaughan TS. Failure replacement and preventive maintenance spare parts ordering policy. European Journal of Operational Research 2005; 161:183–190.
[52] Wang Dazhi, Trivedi KS. Computing steady-state mean time to failure for non-coherent repairable systems. IEEE Transactions on Reliability 2005; R54(3):506–516.
[53] Wang HZ, A survey of maintenance policies of deteriorating systems. European Journal of Operational Research 2002, 139(3): 469–489.
[54] Wang HZ, Pham H. Availability and maintenance of series systems subject to imperfect repair and correlated failure and repair. European Journal of Operational Research 2006; 174(3):1706–1722.
[55] Wu Shaomin, Clements-Croome D. Optimal maintenance policies under different operational schedules. IEEE Transactions on Reliability 2005; R54(2): 338–346.
[56] Zhang YL. A geometric-process repair-model with good-as-new preventive repair. IEEE Transactions on Reliability 2002; R51 (2):223–228.
[57] Zhang YL. An optimal replacement policy for a three-state repairable system with a monotone process model. IEEE Transactions on Reliability 2004; R53(4):452–457.
[58] Zhang YL. A discussion on a bivariate optimal replacement policy for a repairable system. European Journal of Operational Research 2007; 179(1):275–276.
[59] Zheng Zhihua, Cui Lirong, Hawkes AG. A study on a single-unit Markov repairable system with repair time omission. IEEE Transactions on Reliability 2006; R55 (2):182–188.

49

Replacement and Preventive Maintenance Models

Toshio Nakagawa

Department of Marketing and Information Systems, Aichi Institute of Technology
1247 Yachigusa, Yakusa-cho, Toyota 470-0392, Japan

Abstract: This chapter summarizes concisely optimum maintenance policies for reliability models without detailed mathematical explanations: First, standard replacement models such as age, block, and periodic replacements are taken up, and are converted to modified models with finite operating times and random replacement times. Furthermore, replacement policies for inspection models, cumulative damage models, and a parallel system are proposed. Secondly, preventive maintenances (PMs) of one-unit and two-unit systems are discussed. Modified models with periodic PM times, imperfect PM, and repair limit are proposed. Optimum policies that minimize the expected costs or maximize availabilities are summarized. Finally, as applications of maintenance models, optimum policies for computer systems with intermittent faults, imperfect maintenance, and restart are discussed. These results should be very helpful in applications of maintenance models and studies of reliability theory.

49.1 Introduction

Most units or systems such as parts, equipment, components, devices, materials, structures, and machines are replaced or repaired immediately when they fail. However, *corrective maintenance* of units after failure may be costly, and sometimes requires a long time. It is an important problem to determine when to preventively maintain operating units before failure. However, it is unwise to maintain units very frequently. From this viewpoint, the commonly considered maintenance policies are *preventive replacement* for units without repair and *preventive maintenance* (PM) for units with repair on a specific schedule.

Suppose that a unit has to operate for an infinite or a specified time span. Then, as an objective function, it is appropriate to adopt the expected cost *per* unit of time for an infinite time span, that is called *expected cost rate*, and the total expected cost for a finite time span from the viewpoint of economics. Furthermore, it is appropriate to adopt mean time to failure from reliability and *availability* for units with non-negligible replacement or repair time.

We summarize the theoretical results of optimum policies that minimize or maximize the above quantities without detailed explanations and proofs, which are available in the literature [1, 2]. In Section 49.2, we first introduce simple replacement policies for an operating unit. Next, we take up standard replacement models such as age, block, and periodic replacements, convert them to replacement models for a finite time

interval, and consider extended models in which a unit is replaced at a random time. Furthermore, we propose the replacement policies for inspection models, cumulative damage models, and a parallel redundant system. In Section 49.3, we obtain the availabilities of a one-unit system and a two-unit system with PM, and consider the modified PM models where PMs are done at periodic and sequential times. Furthermore, we propose imperfect PM models, where a unit is not always like new at PM times, and a repair limit model as one modified model of PM models. In Section 49.4, as applications of replacement and PM models, we discuss optimum policies for a computer system with intermittent faults and with imperfect maintenance. Finally, we also derive an optimum number of restarts for a computer system.

The known results of replacement, preventive maintenance, and associated models have been summarized in [1]. Since then, many papers and books have been published and reviewed [3–12].

Recently published books [13–17] have collected many reliability and preventive maintenance models. Some chapters in these books have discussed and applied these models to actual systems [18–21]. Many maintenance policies from standard to advanced ones for system reliability models have been extensively discussed [2, 22].

We use the following notations throughout this chapter: Suppose that a unit has to operate for an infinite time span and a specified time span. The unit fails according to a general distribution $F(t) \equiv \int_0^t f(u)du$ with a finite mean μ and a density function $f(t)$, *i.e.*, $f(t) \equiv dF(t)/dt$ and $\mu \equiv \int_0^\infty \overline{F}(t)dt$, where $\overline{\Phi}(t) \equiv 1-\Phi(t)$ for any function $\Phi(t)$. It is assumed that the *failure rate* is $h(t) \equiv f(t)/\overline{F}(t)$ and the *renewal density* is $m(t) \equiv \sum_{j=1}^\infty f^{(j)}(t)$, where $\Phi^{(j)}(t)$ is the j-fold convolution of $\Phi(t)$ with itself and $\Phi^{(0)}(t) \equiv 1$ for $t \geq 0$. In addition, $H(t) \equiv \int_0^t h(u)du$ and $M(t) \equiv \int_0^t m(u)du$, *i.e.*, $F(t) = 1-e^{-H(t)}$ and $M(t) \equiv \sum_{j=1}^\infty F^{(j)}(t)$ that are called a *cumulative hazard rate* and a *renewal function*, respectively. When the unit fails and undergoes minimal repair at failures [2], it is said that failures occur in a nonhomogeneous Poisson process with a *mean value function* $H(t)$ and an *intensity function* $h(t)$.

49.2 Replacement Models

Suppose that an operating unit is replaced after failure or before failure. Then, replacement is roughly classified into two replacements after failure and before failure that are called *corrective replacement* and *preventive replacement*, respectively.

First, we introduce simple replacement policies [2]. Next, as the preventive replacement policies, we take up three policies for age, block, and periodic replacements, and derive analytically optimum policies that minimize the expected cost rates [1, 2]. We extend these policies to replacement models for a finite time interval and with random replacement interval [2, 23]. Furthermore, we propose the replacement policies for inspection models [2], cumulative damage models [24], and a parallel redundant system [2, 24].

49.2.1 Simple Replacement Models

As simple reliability measures of replacement, there are a mean failure time μ and a characteristic life T_1 such that $H(T_1) = 1$. If we estimate only the mean failure time, we may replace a unit before failure when it operates for a $p\mu$ time interval at the rate of p. Because $H(T_1)$ represents the expected number of failures in $[0, T_1]$, time T_1 is the time until the expected number of failures is equal to 1 and $F(T_1) = 1-e^{-1}$, *i.e.*, T_1 is also the approximate time that the unit fails with a probability of 63.2%.

Next, consider a unit that is replaced at time T: Suppose that an operating unit has some earning per unit of time if it does not fail in time T,

otherwise it has no earning. Then, the average time during $[0,T]$ in which we have some earning is

$$l(T) = 0 \times F(T) + T\overline{F}(T) = T\overline{F}(T).$$

Thus, an optimum time T_2 that maximizes $l(T)$ is given by $h(T_2) = 1/T_2$. In particular, when $F(t) = 1 - e^{-\lambda t}$, $T_1 = T_2 = 1/\lambda$.

Finally, introduce simple preventive replacement policies: The first one is that the unit is replaced before failure at time T_p such that $F(T_p) = p \quad (0 < p \le 1)$, where T_p is called a p th percentile point of $F(t)$. Secondly, let c_1 and c_2 $(c_1 > c_2)$ be the respective replacement costs after failure and before failure. Then, we balance the cost of replacement after failure against that before failure such that $c_1 F(T) = c_2 \overline{F}(T)$. In this case,

$$F(T) = \frac{c_2}{c_1 + c_2},$$

and a solution T_p to satisfy it represents a $p(= c_2/(c_1 + c_2))$ th percentile point of $F(t)$.

49.2.2 Standard Replacement

Suppose that a unit must operate for an infinite time span. Then, we consider the standard three replacement policies; age, block, and periodic replacements.

The unit is replaced at failure or at a planned time $T \quad (0 \le T \le \infty)$, whichever occurs first. Then, the expected cost rate is

$$C_1(T) = \frac{(c_1 - c_2)F(T) + c_2}{\int_0^T \overline{F}(t)dt}, \qquad (49.1)$$

where $c_1 =$ cost of replacement at failure and $c_2 =$ cost of replacement at time T with $c_2 < c_1$. If $T = \infty$, then this corresponds to the replacement only at failures, and the resulting cost rate is $C_1(\infty) = c_1/\mu$. If the failure rate $h(t)$ is strictly increasing and $h(\infty) = \lim_{t\to\infty} h(t) > c_2/[\mu(c_1 - c_2)]$, then there exists a finite and unique $T^* \quad (0 < T^* < \infty)$ that satisfies

$$h(T)\int_0^T \overline{F}(t)dt - F(T) = \frac{c_2}{c_1 - c_2}, \qquad (49.2)$$

and the resulting cost rate is

$$C_1(T^*) = (c_1 - c_2)h(T^*). \qquad (49.3)$$

Next, the unit is replaced at periodic times kT $(k = 1,2,\ldots)$ and is also replaced at any failures between replacements. Then, the expected cost rate is

$$C_2(T) = \frac{1}{T}[c_1 M(T) + c_2], \qquad (49.4)$$

where $c_1 =$ cost of replacement at each failure and $c_2 =$ cost of replacement at time T . A necessary condition for a finite T^* to exist is that T^* satisfies

$$Tm(T) - M(T) = \frac{c_2}{c_1}, \qquad (49.5)$$

and the resulting cost rate is

$$C_2(T^*) = c_1 m(T^*). \qquad (49.6)$$

Further, the unit is replaced at periodic times $kT \quad (k = 1,2,\ldots)$ and undergoes only minimal repair at failures between replacements. Minimal repair means that the failure rate remains undisturbed by any minimal repair. Then, the expected cost rate is

$$C_3(T) = \frac{1}{T}[c_1 H(T) + c_2], \qquad (49.7)$$

where $c_1 =$ cost of minimal repair at each failure and $c_2 =$ cost of replacement at time T . If the failure rate $h(t)$ is strictly increasing and $\int_0^\infty t\, dh(t) > c_2/c_1$, there exists a finite and unique $T^* \quad (0 < T^* < \infty)$ that satisfies

$$Th(T) - H(T) = \frac{c_2}{c_1}, \qquad (49.8)$$

and the resulting cost rate is

$$C_3(T^*) = c_1 h(T^*). \qquad (49.9)$$

Clearly, if $h(t)$ is strictly increasing to infinity, a finite T^* exists uniquely.

Finally, the unit is replaced only at times kT $(k = 1,2,\ldots)$ and remains failed for the time interval from its failure to a planned replacement. Then, the expected cost rate is

$$C_4(T)=\frac{1}{T}\left[c_1\int_0^T F(t)dt+c_2\right], \qquad (49.10)$$

where c_1 = cost for the time elapsed between a failure and the replacement per unit of time. If $\mu > c_2/c_1$, there exists a finite and unique T^* $(0<T^*<\infty)$ that satisfies

$$TF(T)-\int_0^T F(t)dt=\frac{c_2}{c_1}, \qquad (49.11)$$

and the resulting cost rate is

$$C_4(T^*)=c_1F(T^*). \qquad (49.12)$$

49.2.3 Replacement for a Finite Interval

A unit has to be operating for a finite time interval $[0,S]$, *i.e.*, the working time of a unit is given by a specified value S. For the maintenance of an operating unit, an interval S is partitioned equally into N parts in which it is replaced at periodic times kT $(k=1,2,\ldots,N)$, where $NT=S$.

The unit is replaced at periodic times kT $(k=1,2,\ldots,N)$ and any unit is as good as new at each replacement. First, the unit is always replaced at any failures between replacements. Then, the expected cost of one interval $[0,T]$ is, from (49.4),

$$\tilde{C}_2(1)\equiv c_1M(T)+c_2=c_1M\left(\frac{S}{N}+c_2\right).$$

Thus, the total expected cost until time S is

$$C_2(N)\equiv N\tilde{C}_2(1)=N\left[c_1M\left(\frac{S}{N}\right)+c_2\right]$$
$$=\frac{S}{T}\left[c_1M(T)+c_2\right] \quad (N=1,2,\ldots). \qquad (49.13)$$

Therefore, we have the optimum policy [2]:

(i) If $T^*<S$, then we set that $\left[S/T^*\right]\equiv N$ and calculate $C_2(N)$ and $C_2(N+1)$ from (49.13). If $C_2(N)\le C_2(N+1)$, then $N^*=N$, and conversely, if $C_2(N)> C_2(N+1)$, then $N^*=N+1$.

(ii) If $T^*\ge S$, then $N^*=1$.

Next, the unit undergoes only minimal repair at failures between replacements. Then, the expected cost of one interval $[0,T]$ from (49.7) is

$$\tilde{C}_3(1)\equiv c_1H(T)+c_2=c_1H\left(\frac{S}{T}\right)+c_2.$$

Thus, the total expected cost until time S is

$$C_3(N)\equiv N\tilde{C}_3(1)=N\left[c_1H\left(\frac{S}{N}\right)+c_2\right]$$
$$=\frac{S}{T}\left[c_1H(T)+c_2\right] \quad (N=1,2,\ldots). \qquad (49.14)$$

Therefore, by obtaining T^* that satisfies (49.8) and applying it to the optimum policy, we can obtain an optimum number N^* that minimizes $C_3(N)$ in (49.14).

Finally, the unit is replaced only at periodic times kT. Then, from (49.10), the expected cost of one interval $[0,T]$ is

$$\tilde{C}_4(1)\equiv c_1\int_0^T F(t)dt+c_2$$
$$=c_1\int_0^{S/N}F(t)dt+c_2.$$

Thus, the total expected cost until time S is

$$C_4(N)\equiv N\tilde{C}_4(1)=N\left[c_1\int_0^{S/N}F(t)dt+c_2\right]$$
$$=\frac{S}{T}\left[c_1\int_0^T F(t)dt+c_2\right]. \qquad (49.15)$$

Therefore, using the optimum policy, we can obtain an optimum replacement number N^* that minimizes $C_4(N)$ in (49.15).

49.2.4 The Random Replacement Interval

When a unit has a variable working cycle and processing time, it would be better to do some maintenance after it has completed its work and process. It is assumed that a unit is replaced before failure at either a planned time T or a random time Y, where Y is distributed according to a general distribution $G(t)$, where $\overline{G}(t)\equiv 1-G(t)$.

First, the unit is replaced at time T, at random time Y or at failure, whichever occurs first. Then, from (49.1), the expected cost rate is

$$C_1(T) = \frac{(c_1 - c_2)\int_0^T \overline{G}(t)dF(t) + c_2}{\int_0^T \overline{G}(t)\overline{F}(t)dt}. \quad (49.16)$$

If the failure rate $h(t)$ is strictly increasing, and

$$h(\infty)\int_0^T \overline{G}(t)\overline{F}(t)dt - \int_0^\infty \overline{G}(t)dF(t) > \frac{c_2}{c_1 - c_2},$$

there exists a finite an unique T^* $(0 < T^* < \infty)$ that satisfies

$$h(T)\int_0^T \overline{G}(t)\overline{F}(t)dt - \int_0^T \overline{G}(t)dF(t) = \frac{c_2}{c_1 - c_2}, \quad (49.17)$$

and the resulting cost rate is given in (49.3).

Secondly, the unit is replaced at time T or at time Y, whichever occurs first, and is also replaced at any failures between replacements. Then, from (49.4), the expected cost rate is

$$C_2(T) = \frac{c_1\int_0^T \overline{G}(t)dM(t) + c_2}{\int_0^T \overline{G}(t)dt}. \quad (49.18)$$

A necessary condition for a finite T^* to exist is that T^* satisfies

$$m(T)\int_0^T \overline{G}(t)dt - \int_0^T \overline{G}(t)dM(t) = \frac{c_2}{c_1}, \quad (49.19)$$

and the resulting cost rate is given in (49.6).

Further, the unit is replaced at time T or at time Y, whichever occurs first, and undergoes only minimal repair at failures between replacements. Then, from (49.7), the expected cost rate is

$$C_3(T) = \frac{c_1\int_0^T \overline{G}(t)dH(t) + c_2}{\int_0^T \overline{G}(t)dt}. \quad (49.20)$$

If the failure rate $h(t)$ is strictly increasing, and $\int_0^\infty [\int_0^t \overline{G}(u)du]dh(t) > c_2/c_1$, there exists a finite an unique T^* $(0 < T^* < \infty)$ that satisfies

$$h(T)\int_0^T \overline{G}(t)dt - \int_0^T \overline{G}(t)dH(t) = \frac{c_2}{c_1}, \quad (49.21)$$

and the resulting cost rate is given in (49.9).

Finally, when the unit fails between replacements, it remains failed for the time interval from a failure to its replacement. Then, from (49.10), the expected cost rate is

$$C_4(T) = \frac{c_1\int_0^T \overline{G}(t)dF(t) + c_2}{\int_0^T \overline{G}(t)dt}. \quad (49.22)$$

If $\int_0^\infty \overline{G}(t)\overline{F}(t)dt > c_2/c_1$, then there exists a finite and unique T^* $(0 < T^* < \infty)$ that satisfies

$$F(T)\int_0^T \overline{G}(t)dt - \int_0^T \overline{G}(t)F(t)dt = \frac{c_2}{c_1}, \quad (49.23)$$

and the resulting cost rate is given in (49.12). In particular, when $\overline{G}(t) \equiv 1$ for any $t \geq 0$, the above results correspond to those of Section 49.2.2.

Next, suppose that the unit is replaced at a planned time T or at the N th random time $(N = 1, 2, \ldots)$. Then, the expected cost rates of each model can be rewritten as

$$C_1(T,N) = \frac{(c_1 - c_2)\int_0^T [1 - G^{(N)}(t)]dF(t) + c_2}{\int_0^T [1 - G^{(N)}(t)]\overline{F}(t)dt}, \quad (49.24)$$

$$C_2(T,N) = \frac{c_1\int_0^T [1 - G^{(N)}(t)]dH(t) + c_2}{\int_0^T [1 - G^{(N)}(t)]dt}, \quad (49.25)$$

$$C_3(T,N) = \frac{c_1\int_0^T [1 - G^{(N)}(t)]dM(t) + c_2}{\int_0^T [1 - G^{(N)}(t)]dt}, \quad (49.26)$$

$$C_4(T,N) = \frac{c_1\int_0^T [1 - G^{(N)}(t)]F(t)dt + c_2}{\int_0^T [1 - G^{(N)}(t)]dt}. \quad (49.27)$$

49.2.5 Inspection with Replacement

A unit should operate for an infinite time span and is checked at successive times $T_k \quad (k=1,2,\ldots)$, where $T_0=0$. Any failure is detected at the next checking time and is replaced immediately. It is assumed that all times needed for checks are negligible and the failure rate $h(t)$ is unchanged by any check. Then, the total expected cost until the replacement is

$$C_1(T_1,T_2,\ldots)=\sum_{k=0}^{\infty}\int_{T_k}^{T_{k+1}}[c_1(k+1)+c_2(T_{k+1}-t)]dF(t)+c_3, \qquad (49.28)$$

where c_1 = cost of one check, c_2 = loss cost *per* unit of time for the time elapsed between a failure and its detection at the next checking time, and c_3 = replacement cost of a failed unit.

Differentiating $C_1(T_1,T_2,\ldots)$ with T_k and setting it equal to zero,

$$T_{k+1}-T_k=\frac{F(T_k)-F(T_{k-1})}{f(T_k)}-\frac{c_1}{c_2} \quad (k=1,2,\ldots). \qquad (49.29)$$

Algorithm 1 for computing the optimum inspection schedule is [1]:

1. Choose T_1 to satisfy $c_1=c_2\int_0^{T_1}F(t)dt$.
2. Compute $T_2,T_3,\ldots$ recursively from (49.29).
3. If any $\delta_k>\delta_{k-1}$, reduce T_1 and repeat, where $\delta_k\equiv T_{k+1}-T_k$. If any $\delta_k<0$, increase T_1 and repeat.
4. Continue until $T_1<T_2<\cdots$ are determined to the degree of accuracy required.

Next, a unit should operate for a finite time interval $[0,S]$ and is checked at successive times $T_k \quad (k=1,2,\ldots,N)$, where $T_0\equiv 0$ and $T_N=S$. Then, the expected cost is

$$C_2(T_1,T_2,\ldots,T_N)=\sum_{k=0}^{N-1}\int_{T_k}^{T_{k+1}}[c_1(k+1)+c_2(T_{k+1}-t)]dF(t)+c_1N\overline{F}(T_N)+c_3 \quad (N=1,2,\ldots). \qquad (49.30)$$

Setting $\partial C_2(T_1,T_2,\ldots,T_N)/\partial T_k=0$, we have (49.29) for $k=1,2,\ldots,N-1$, and the resulting cost is

$$\begin{aligned}\tilde{C}_2(T_1,T_2,\ldots,T_N)&=C_2(T_1,T_2,\ldots,T_N)+c_2\int_0^S\overline{F}(t)dt-c_3\\&=\sum_{k=0}^{N-1}[c_1+c_2(T_{k+1}-T_k)]\overline{F}(T_k)\end{aligned} \quad (N=1,2,\ldots). \qquad (49.31)$$

Therefore, we may solve the simultaneous equations (49.29) for $(k=1,2,\ldots,N-1)$ and $T_N=S$, and obtain the expected cost $\tilde{C}_2(T_1,T_2,\ldots,T_N)$ in (49.31). Next, comparing $\tilde{C}_2(T_1,T_2,\ldots,T_N)$ for all $N\geq 1$, we can obtain the optimum checking number N^* and times T_k^* $(k=1,2,\ldots,N^*)$.

Finally, suppose that a unit is checked at time T_k and random times $Y_k \quad (k=1,2,\ldots)$, where $Y_0\equiv 0$ and $Z_k\equiv Y_k-Y_{k-1} \quad (k=1,2,\ldots)$ are independently and identically distributed random variables, and also independent of its failure time. It is assumed that Z_k has an identical distribution $G(x)$ and the distribution of Y_k is denoted by the j-fold convolution $G^{(j)}(x)$ of $G(x)$ with itself. Then, the total expected cost until replacement is

$$\begin{aligned}C_3(T_1,T_2,\ldots)&=c_1\sum_{k=0}^{\infty}\overline{F}(T_k)\\&+c_4\sum_{k=0}^{\infty}k\int_0^{\infty}[G^{(k)}(t)-G^{(k+1)}(t)]dF(t)\\&-(c_1-c_4)\sum_{k=0}^{\infty}\int_{T_k}^{T_{k+1}}\{G(T_{k+1})-G(t)\\&+\int_0^t[G(T_{k+1}-x)-G(t-x)]dM_G(x)\}dF(t)\\&+c_2\sum_{k=0}^{\infty}\int_{T_k}^{T_{k+1}}\{\int_t^{T_{k+1}}\overline{G}(y)dy\\&+[\int_0^t(\int_{t-x}^{T_{k+1}-x}\overline{G}(y)dy)dM_G(x)]\}dF(t)\\&+c_3,\end{aligned} \qquad (49.32)$$

where c_4 = cost of the random check and $M_G(x)$ represents the expected number of random checks during $[0,x]$.

In particular, when $G(x) = 1 - e^{-\theta x}$, the total expected cost in (49.32) can be simplified as

$$C_3(T_1, T_2, \ldots) = c_1 \sum_{k=0}^{\infty} \overline{F}(T_k) + c_4 \theta \mu - \left(c_1 - c_4 - \frac{c_2}{\theta} \right) \sum_{k=0}^{\infty} \int_{T_k}^{T_{k+1}} [1 - e^{-\theta(T_{k+1} - t)}] dF(t) + c_3. \quad (49.33)$$

49.2.6 The Cumulative Damage Model

Consider the following cumulative damage model: A unit should operate for an infinite time span. Shocks occur at random times and each shock causes a random amount of damage to the unit. It is assumed that the total damage is additive, and the unit fails when it has exceeded a failure level K.

First, suppose that shocks occur in a renewal process with a general distribution $F(t)$ with finite mean μ. Letting $N(t)$ be the number of shocks in time t, the probability that j shocks occur exactly in $[0, t]$ is

$$\Pr\{N(t) = j\} = F^{(j)}(t) - F^{(j+1)}(t) \quad (j = 0, 1, 2, \ldots).$$

Further, an amount W_j of damage due to the jth shock has an identical distribution $G(x) \equiv \Pr\{W_j \le x\}$.

The unit is replaced before failure at time T, at shock N, or at damage Z, whichever occurs first. Then, the expected cost rate is

$$C(T, N, Z) = \left[c_1 - (c_1 - c_2) \sum_{j=0}^{N-1} [F^{(j)}(T) - F^{(j+1)}(T)] G^{(j)}(Z) - (c_1 - c_3) F^{(N)}(T) G^{(N)}(Z) - (c_1 - c_4) \sum_{j=0}^{N-1} F^{(j+1)}(T) \times \int_0^Z [G(K - x) - G(Z - x)] dG^{(j)}(x) \right] \Big/ \left[\sum_{j=0}^{N-1} G^{(j)}(Z) \int_0^T [F^{(j)}(t) - F^{(j+1)}(t)] dt \right], \quad (49.34)$$

where c_1 = cost of replacement at failure, c_2 = cost of replacement at time T, c_3 = cost of replacement at shock N, and c_4 = cost of replacement at damage Z.

When the unit is replaced at time T $(0 < T \le \infty)$ or at failure, whichever occurs first, the expected cost rate in (49.34) is

$$C_1(T) = \frac{c_1 - (c_1 - c_2) \sum_{j=0}^{\infty} [F^{(j)}(T) - F^{(j+1)}(T)] G^{(j)}(K)}{\sum_{j=0}^{\infty} G^{(j)}(Z) \int_0^T [F^{(j)}(t) - F^{(j+1)}(t)] dt}. \quad (49.35)$$

When the unit is replaced at shock N $(N = 1, 2, \ldots)$ or at failure, whichever occurs first, the expected cost rate in (49.34) is

$$C_2(N) = \frac{c_1 - (c_1 - c_3) G^{(N)}(K)}{\mu \sum_{j=0}^{N-1} G^{(j)}(K)} \quad (N = 1, 2, \ldots). \quad (49.36)$$

Finally, when the unit is replaced at damage Z $(0 < Z \le \infty)$ or at failure, whichever occurs first, the expected cost rate in (49.34) is

$$C_3(Z) = \frac{c_1 - (c_1 - c_4) \left[G(K) - \int_0^Z \overline{G}(K - x) dM_G(x) \right]}{\mu [1 + M_G(Z)]}. \quad (49.37)$$

The optimum policies that minimize the expected cost rates in (49.35), (49.36), and (49.37) have been discussed analytically [24].

For example, an optimum damage level Z^* that minimizes $C_3(Z)$ in (49.37) for $c_1 > c_4$ is given as follows: If $M_G(K) > c_4/(c_1 - c_4)$, then there exists a finite and unique Z^* $(0 < Z^* < K)$ that satisfies

$$\int_{K-Z}^{K} [1 + M_G(K - x)] dG(x) = \frac{c_4}{c_1 - c_4}, \quad (49.38)$$

and the resulting cost rate is

$$\mu C_3(Z^*) = (c_1 - c_4) \overline{G}(K - Z^*). \quad (49.39)$$

Conversely, if $M_G(K) \le c_4/(c_1 - c_4)$, then $Z^* = K$, *i.e.*, the unit should be replaced only at failure, and the expected cost rate is

$$\mu C_3(K) = \frac{c_1}{1 + M_G(K)}. \quad (49.40)$$

Next, suppose that shocks occur in a nonhomogeneous Poisson process with a mean value function $H(t)$, *i.e.*, $p_j(t) \equiv \Pr\{N(t) = j\} = \left[H(t)^j / j!\right] e^{-H(t)}$ $(j = 0,1,2,\ldots)$. Then, the expected cost rate in (49.34) is rewritten as

$$C(T,N,Z) = \frac{\begin{aligned} &c_1 - (c_1 - c_2)\sum_{j=0}^{N-1} G^{(j)}(Z)\, p_j(T) \\ &-(c_1 - c_3) G^{(N)}(Z) \sum_{j=N}^{\infty} p_j(T) \\ &-(c_1 - c_4)\sum_{j=0}^{N-1} \int_0^Z [G(K-x) - G(Z-x)] \\ &\times dG^{(j)}(x) \sum_{i=j+1}^{\infty} p_i(T) \end{aligned}}{\sum_{j=0}^{N-1} G^{(j)}(Z) \int_0^T p_j(t)\,dt}. \quad (49.41)$$

When shocks occur in a Poisson process, the two costs of (49.34) and (49.41) agree with each other.

49.2.7 The Parallel Redundant System

Consider a parallel redundant system that consists of n $(n \geq 2)$ identical units and fails when all units fail. It is assumed that each unit has a failure distribution $F(t)$ with finite μ.

Suppose that the system is replaced at failure or at time T $(0 < T < \infty)$, whichever occurs first. Then, the expected cost rate is

$$C_1(T) = \frac{(c_1 - c_2)F(T)^n + c_2 + c_0 n}{\int_0^T \left[1 - F(t)^n\right] dt}, \quad (49.42)$$

where $\mu_n \equiv \int_0^\infty \left[1 - F(t)^n\right] dt$, c_1 = cost of replacement at system failure, c_2 = cost of replacement at time T with $c_2 < c_1$, and c_0 = acquisition cost of one unit. By a method similar to that in Section 49.2.2, if the failure rate $h(t)$ is strictly increasing, and $h(\infty) > (c_1 + nc_0)/\left[\mu_n (c_1 - c_2)\right]$, then there exists a finite and unique T^* $(0 < T^* < \infty)$ that satisfies

$$\frac{nh(T)\left[F(T)^{n-1} - F(T)^n\right]}{1 - F(T)^n} \int_0^T \left[1 - F(t)^n\right] dt - F(T)^n = \frac{c_2 + nc_0}{c_1 - c_2}, \quad (49.43)$$

and the resulting cost rate is

$$C_1(T^*) = n(c_1 - c_2)h(T^*)\frac{F(T^*)^{n-1} - F(T^*)^n}{1 - F(T^*)^n}. \quad (49.44)$$

If the system is replaced only at failure, then the expected cost rate in (49.42) is

$$C_2(n) \equiv \lim_{T \to \infty} C_1(T) = \frac{c_0 n + c_2}{\int_0^\infty \left[1 - F(t)^n\right] dt} \quad (n = 1,2,\ldots). \quad (49.45)$$

An optimum number n^* is given by a finite unique minimum that satisfies

$$\frac{\int_0^\infty \left[1 - F(t)^n\right] dt}{\int_0^\infty \left[F(t)^n - F(t)^{n+1}\right] dt} - n \geq \frac{c_2}{c_0} \quad (n = 1,2,\ldots). \quad (49.46)$$

In particular, when $F(t) = 1 - e^{-\lambda t}$, an optimum n^* is a unique minimum such that

$$(n+1)\sum_{j=1}^{n} \frac{1}{j} - n \geq \frac{c_2}{c_0} \quad (n = 1,2,\ldots). \quad (49.47)$$

Finally, consider a parallel redundant system with n units in which units fail subject to shocks at a mean interval μ. It is assumed that the probability that each unit fails at shock j is constant p, where $q \equiv 1 - p$. Suppose that the system is replaced before failure when the total number of failed units is $N+1, N+2, \ldots, n-1$, or it is replaced when all units have failed, otherwise it is left alone. Then, the expected cost rate is

$$C_3(N) = \frac{\begin{aligned} &(c_1 - c_2)\sum_{j=0}^{N} \binom{n}{j} (-1)^j p^{n-j} \\ &\times \sum_{i=0}^{j} \binom{j}{i} (-1)^i \left[1/(1 - q^{n-i})\right] + c_2 \end{aligned}}{\mu \sum_{j=0}^{N} \binom{n}{j} (-1)^j \sum_{i=0}^{N-j} \binom{n-j}{i} \left[1/(1 - q^{n-i})\right]} \quad (N = 0,1,\ldots,n-1), \quad (49.48)$$

where c_1 = cost of replacement at system failure and c_2 = cost of replacement before failure with $c_2 < c_1$. In particular, when $n = 2$,

$$C_3(0) = \frac{c_1 p^2 + c_2(1-p^2-q^2)}{\mu},$$

$$C_3(1) = \frac{c_1}{\mu}\frac{1-q^2}{1+2q}. \tag{49.49}$$

Thus, if $c_2/c_1 < q/(1+2q)$, then the system is replaced when one unit fails at some shock, and if $c_2/c_1 \geq q/(1+2q)$, then it is replaced when two units have failed.

49.3 Preventive Maintenance Models

A unit is repaired upon failure. If a failed unit undergoes repair, it needs a repair time that may not be negligible. After the completion of repair, the unit begins to operate again. When the unit is repaired after failure, it may require much time and high cost. To prevent such failure, we need to undergo preventive maintenance before failure, but not to do it too late from the viewpoint of reliability or cost.

First, this section considers a one-unit system and a two-unit system, and derives optimum PM times that maximize the availabilities [2, 25]. Next, we modify the standard model in which the PM is planned at periodic times and it is done at the next time when the number of failures and the total damage have exceeded a threshold level [2, 26]. Furthermore, we consider the PM model, where PM times are done at sequential times, and derive analytically optimum times that minimize the expected cost rate [2, 27]. We propose imperfect PM models, where the unit may be younger at each PM time, and the repair limit model, where the repair of a failed unit is stopped when it is not completed in time T [2, 22, 28, 29].

49.3.1 The Parallel Redundant System

When a unit fails, it undergoes repair immediately, and once repaired it is returned to the operating state. It is assumed that the failure time X has an identical distribution with mean μ, and the repair time Y_1 has an identical distribution $G_1(t)$ with finite mean θ_1. Further, the unit undergoes PM before failure at a planned time T and the time for PM is θ_2. Then, the availability is

$$A(T) = \frac{\int_0^T \overline{F}(t)dt}{\int_0^T \overline{F}(t)dt + \theta_1 F(T) + \theta_2 \overline{F}(T)}. \tag{49.50}$$

Thus, the PM policy maximizing the availability is the same as minimizing the expected cost rate $C_1(T)$ in (49.1).

Next, suppose that the repair of a failed unit is not completed in time T $(0 \leq T \leq \infty)$, which is called a *repair limit policy*, then it is replaced with a new one. Then, the expected cost rate is

$$C(T) = \frac{c_1 \overline{G}_1(T) + \int_0^T \overline{G}_1(t)dc_r(t)}{\mu + \int_0^T \overline{G}_1(t)dt}, \tag{49.51}$$

where c_1 = replacement cost of a failed unit and $c_r(t)$= repair cost during $(0,t]$.

Let $g_1(t)$ be a density function of $G_1(t)$ and $r_1(t) \equiv g_1(t)/\overline{G}_1(t)$ be the repair rate. In particular, when $c_r(t) = c_2 t$, the expected cost rate in (49.51) is rewritten as

$$C(T) = \frac{c_1 \overline{G}_1(T) + c_2 \int_0^T \overline{G}_1(t)dt}{\mu + \int_0^T \overline{G}_1(t)dt}. \tag{49.52}$$

Then, we have the optimum policy when $r_1(t)$ is strictly decreasing: If $r_1(0) \leq k$, then $T^* = 0$, *i.e.*, no repair should be made. If $r_1(0) > k$ and $r_1(\infty) \leq K$, then there exists a finite and unique T^* that satisfies

$$r_1(T)\left[\mu + \int_0^T \overline{G}_1(t)dt\right] + \overline{G}_1(T) = \frac{c_2\mu}{c_1}, \tag{49.53}$$

and the resulting cost rate is

$$C(T^*) = c_2 - c_1 r_1(T^*). \tag{49.54}$$

If $r_1(\infty) \geq K$, then $T^* = \infty$, *i.e.*, no repair should

be made, where

$$k \equiv \frac{c_2\mu - c_1}{c_1\mu}, \qquad K \equiv \frac{c_2\mu}{c_1(\mu+\theta_1)}.$$

49.3.2 The Two-unit System

Consider a two-unit standby system where two units are statistically identical. Suppose that when an operating unit operates for a specified time T without failure, we stop its operation and undergo its PM. It is assumed that an operating unit has a failure distribution $F(t)$ with finite mean μ, a failed unit has a repair distribution $G_1(t)$ with finite mean θ_1, and the time for PM has a general distribution $G_2(t)$ with finite mean θ_2. Then, the availability is

$$A(T) = \frac{\left[\gamma_1 + \int_0^T G_1(t)\overline{F}(t)dt\right]\left[1 - \int_T^\infty G_2(t)dF(t)\right] + \left[\gamma_2 + \int_0^T G_2(t)\overline{F}(t)dt\right]\int_T^\infty G_1(t)dF(t)}{\left[\theta_1 + \int_0^T G_1(t)\overline{F}(t)dt\right]\left[1 - \int_T^\infty G_2(t)dF(t)\right] + \left[\theta_2 + \int_0^T G_2(t)\overline{F}(t)dt\right]\int_T^\infty G_1(t)dF(t)}, \tag{49.55}$$

where

$$\gamma_i \equiv \int_0^\infty \overline{G}_i(t)\overline{F}(t)dt \quad (i=1,2).$$

When $G_1(t) < G_2(t)$ for $0 < t < \infty$ and the failure rate $h(t)$ is strictly increasing, we have the following optimum policy: If $\rho_1\theta_2 > \rho_2\theta_1$ and $h(0) \geq k$, then $T^* = 0$, and the availability is

$$A(0) = \frac{q_2\gamma_1 + (1-q_1)\gamma_2}{q_2\theta_1 + (1-q_1)\theta_2} \tag{49.56}$$

If $\rho_1\theta_2 > \rho_2\theta_1$, $h(\infty) > K$, and $h(0) < k$, or $\rho_1\theta_2 \leq \rho_2\theta_1$ and $h(\infty) > K$, then there exists a finite and unique T^* $(0 < T^* < \infty)$ that satisfies

$$h(T)\left[\int_0^T L(t)\overline{F}(t)dt + \int_0^\infty \overline{L}(t)dt\right] - \int_0^T L(t)dF(t) = \frac{\rho_1\int_0^\infty \overline{L}(t)dF(t) + \rho_2\int_0^T L(t)dF(t)}{\rho_1 - \rho_2}. \tag{49.57}$$

If $h(\infty) \leq K$, then $T^* = \infty$, *i.e.*, no PM is done, and the availability is

$$A(\infty) = \frac{\mu}{\mu + \theta_1 - \gamma_1},$$

where

$$q_i \equiv \int_0^\infty \overline{G}_i(t)dF(t),$$

$$\rho_i \equiv \int_0^\infty \overline{G}_i(t)F(t)dt = \theta_i - \gamma_i \quad (i=1,2),$$

$$L(t) \equiv \frac{\rho_1 G_2(t) - \rho_2 G_1(t)}{\rho_1 - \rho_2},$$

$$k \equiv \frac{\rho_1 q_2 + \rho_2(1-q_1)}{\rho_1\theta_2 - \rho_2\theta_1}, \quad K \equiv \frac{\rho_1}{\mu(\rho_1 - \rho_2)}.$$

49.3.3 The Modified Discrete Policy

Consider a unit that should operate for a certain time span. It is assumed that failures occur in a nonhomogeneous Poisson process with an intensity function $h(t)$ and a mean value function $H(t) \equiv \int_0^t h(u)du$. Then, the expected number of failures during $[0,t]$ is $p_j[H(t)] \equiv \left[H(t)^j / j!\right] \times e^{-H(t)}$ $(j = 0,1,2,\ldots)$. Suppose that the PM is planned at periodic times kT $(k = 1,2,\ldots)$, where a positive T $(0 < T < \infty)$ is given. If the total number of failures has exceeded a specified number N $(N = 1,2,\ldots)$, the PM is done at the next planned time and the unit becomes like new, otherwise the unit is left as it is. The unit undergoes minimal repair at each failure between PMs.

Under the above assumptions, the expected cost rate is

$$C_1(N) = \frac{c_1\sum_{k=0}^\infty [H((k+1)T) - H(kT)] \times \sum_{j=0}^{N-1} p_j[H(kT)] + c_2}{T\sum_{k=0}^\infty \sum_{j=0}^\infty p_j[H(kT)]} \quad (N = 1,2,\ldots), \tag{49.58}$$

where c_1 = cost of minimal repair at each failure and c_2 = cost of planned PM.

When an intensity function $h(t)$ is strictly increasing, if $L_1(\infty) > c_2/c_1$, then an optimum number N^* is given by a finite and unique minimum that satisfies

$$L_1(N) \geq \frac{c_2}{c_1} \qquad (N = 1, 2, \ldots), \qquad (49.59)$$

where

$$L_1(N) \equiv q_1(N) \sum_{k=0}^{\infty} \sum_{j=0}^{N-1} p_j[H(kT)] - \sum_{k=0}^{\infty} [H((k+1)T) - H(kT)] \sum_{j=0}^{N-1} p_j[H(kT)],$$

$$q_1(N) \equiv \frac{\sum_{k=0}^{\infty} [H((k+1)T) - H(kT)]\, p_N[H(kT)]}{\sum_{k=0}^{\infty} [p_N[H(kT)]]}.$$

Next, consider the cumulative damage model where shocks occur in a nonhomogeneous Poisson process with a mean value function $H(t)$ and each damage due to shocks has an identical distribution $G(x)$. The total damage is additive, and the unit fails when it has exceeded a failure level K and the CM is done. If the total damage has exceeded a threshold level Z $(0 \leq Z \leq K)$ during $(kT, (k+1)T]$ $(k = 0, 1, 2, \ldots)$, then the PM is done at time $(k+1)T$. Then, the expected cost rate is

$$C_2(Z) = \frac{\begin{array}{l} c_2 + (c_1 - c_2) \sum_{k=0}^{\infty} \sum_{j=0}^{\infty} p_j[H(kT)] \\ \times \sum_{i=0}^{\infty} p_i[H((n+1)T) - H(nT)] \\ \times \int_0^Z [1 - G^{(i)}(K-x)]\, dG^{(j)}(x) \end{array}}{\begin{array}{l} \sum_{k=0}^{\infty} \sum_{j=0}^{\infty} p_j[H(kT)] \\ \times \int_0^Z G^{(i)}(K-x)\, dG^{(j)}(x) \\ \times \int_{kT}^{(k+1)T} p_i[H(t) - H(nT)]\, dt \end{array}}, \qquad (49.60)$$

where c_1 = CM cost after failure and c_2 = PM cost before failure.

When shocks occur in a Poisson process with rate λ, *i.e.*, $p_j[H(kT)] = [(k\lambda T)^j / j!] e^{-k\lambda T} \equiv p_j(k\lambda T)$ $(j = 0, 1, 2, \ldots)$, an optimum damage level Z^* is given as follows: If $M_G(K) > c_2/(c_1 - c_2)$, then there exists a unique Z^* $(0 < Z^* < K)$ that satisfies

$$\begin{aligned} & q_2(Z) \sum_{k=0}^{\infty} \sum_{j=0}^{\infty} p_j(k\lambda T) \sum_{i=0}^{\infty} \int_0^T p_i(\lambda t)\, dt \\ & \times \int_0^Z G^{(i)}(K-x)\, dG^{(j)}(x) \\ & - \sum_{k=0}^{\infty} \sum_{j=0}^{\infty} p_j(k\lambda T) \sum_{i=0}^{\infty} p_i(\lambda T) \\ & \times \int_0^Z [1 - G^{(i)}(K-x)]\, dG^{(j)}(x) = \frac{c_2}{c_1 - c_2}, \end{aligned} \qquad (49.61)$$

and the resulting cost rate is

$$C_2(Z^*) = (c_1 - c_2) q_2(Z^*), \qquad (49.62)$$

where

$$q_2(Z) \equiv \frac{\sum_{i=0}^{\infty} p_i(k\lambda T)[1 - G^{(i)}(K-Z)]}{\sum_{i=0}^{\infty} \int_0^T p_i(k\lambda T)\, dt\, G^{(i)}(K-Z)}.$$

Conversely, if $M_G(K) \leq c_2/(c_1 - c_2)$, then $Z^* = K$, and the PM is done after failure, and the expected cost rate is

$$C_2(K) = \frac{c_1}{\mu[1 + M_G(K)]},$$

which agrees with (49.40).

49.3.4 Periodic and Sequential Policies

A unit must operate for an infinite time span. The PM is done at successive times $0 < T_1 < T_1 + T_2 < \cdots < T_1 + T_2 + \cdots + T_N$, and the unit is replaced at time $T_1 + T_2 + \cdots + T_N$. It is assumed that the unit has the failure rate $h_k(t)$ in the k-th period of PMs and $h_k(t) < h_{k+1}(t)$ for any $t > 0$, *i.e.*, the failure rate increases with the number of PMs. Further, the unit undergoes minimal repair at failures between PMs. Then, the expected cost rate is

$$C(T_1, T_2, \ldots, T_N) = \frac{c_1 \sum_{k=1}^{\infty} \int_0^{T_k} h_k(t)\, dt + c_2 + (N-1)c_3}{T_1 + T_2 + \cdots + T_N}, \qquad (49.63)$$

where c_1 = cost of minimal repair at each failure, c_2 = cost of replacement, and c_3 = cost of PM with $c_3 < c_2$. When $N = 1$, (49.63) agrees with (49.7). Differentiating $C(T_1,T_2,\ldots,T_N)$ with respect to T_k and setting it equal to zero implies

$$h_1(T_1) = h_2(T_2) = \cdots = h_N(T_N), \qquad (49.64)$$

$$c_1 h_k(T_k) = C(T_1,T_2,\ldots,T_N). \qquad (49.65)$$

Thus, we can specify the following computing procedure for obtaining an optimum PM policy:

1. Solve $h_k(T_k) = A$ and express T_k $(k = 1,2,\ldots,N)$ by a function of A.
2. Substitute T_k in (49.65) and solve it with respect to A.
3. Determine N^* that minimizes A.

Suppose that $h_k(t) = \lambda_k m t^{m-1}$ $(m > 1)$ and $\lambda_k < \lambda_{k+1}$, *i.e.*, the failure rate $h_k(t)$ becomes greater with the number of PMs and is strictly increasing to ∞ as $t \to \infty$. Then, solving $h_k(T_k) = A$, we have

$$T_k = \left(\frac{A}{\lambda_k m}\right)^{1/(m-1)}.$$

Substituting T_k in (49.65) and rearranging it,

$$A\sum_{k=1}^{N}\left(\frac{A}{\lambda_k m}\right)^{1/(m-1)} - \sum_{k=1}^{N}\lambda_k\left(\frac{A}{\lambda_k m}\right)^{m/(m-1)} = \frac{c_2 + (N-1)c_3}{c_1},$$

i.e.,

$$A = \left\{\frac{c_2 + (N-1)c_3}{c_1\left[1-(1/m)\right]\sum_{k=1}^{N}\left[1/(\lambda_k m)\right]^{1/(m-1)}}\right\}^{(m-1)/m}.$$

Next, solve the problem that minimizes

$$B(N) = \frac{c_2 + (N-1)c_3}{\sum_{k=1}^{N}\left(1/\lambda_k\right)^{1/(m-1)}} \quad (N = 1,2,\ldots).$$

An optimum N^* that minimizes *B(N)* is given as follows: If $L(\infty) > c_2/c_3$, then there exists a finite and unique N^* that satisfies

$$L(N) \ge \frac{c_2}{c_3} \qquad (N = 1,2,\ldots),$$

where

$$L(N) \equiv \sum_{k=1}^{N}\left(\frac{\lambda_{N+1}}{\lambda_k}\right)^{1/(m-1)} - (N-1).$$

Therefore, we have the following optimum policy:

$$A = \left\{\frac{c_2 + (N^*-1)c_3}{c_1\left[1-(1/m)\right]\sum_{k=1}^{N^*}\left[1/(\lambda_k m)\right]^{1/(m-1)}}\right\}^{(m-1)/m},$$

$$T_k^* = \left(\frac{A}{\lambda_k m}\right)^{1/(m-1)},$$

and the expected cost rate is $c_1 A$.

49.3.5 Imperfect Policies

Consider four imperfect policies for the same periodic PM model as that in Section 49.3.4, *i.e.*, the PM is done at periodic times kT $(k = 1,2,\ldots)$. It is assumed that the unit undergoes only minimal repair at failures between PMs, and the failure rate is strictly increasing and remains undisturbed by minimal repair.

First, suppose that the unit after PM has the same failure rate as it had before PM with probability p $(0 \le p < 1)$ and that it becomes as good as new with probability $q \equiv 1 - p$. Then, the expected cost rate is

$$C_1(T) = \frac{1}{T}\left[c_1 q^2 \sum_{j=1}^{\infty} p^{j-1}\int_0^T h(t)\,dt + c_2\right], \qquad (49.66)$$

where c_1 = cost of minimal repair at each failure and c_2 = cost of each PM. If $\int_0^T t\,dh(t) > c_2/\left(c_1 q^2\right)$, then there exists a finite and unique T^* that satisfies

$$\sum_{j=1}^{\infty} p^{j-1}\int_0^{jT} t\,dh(t) = \frac{c_2}{c_1 q^2}. \qquad (49.67)$$

Secondly, suppose that the age becomes x $(0 \le x \le T)$ units younger at each PM and is

replaced if it operates for the time interval NT. Then, the expected cost rate is

$$C_2(N) = \frac{1}{NT}\left[\begin{array}{l} c_1 \sum_{j=0}^{N-1} \int_{j(T-x)}^{T+j(T-x)} h(t)dt \\ +c_2 + (N-1)c_3 \end{array}\right] \quad (N = 1, 2, \ldots), \quad (49.68)$$

where c_1 = cost of minimal repair, c_2 = cost of replacement at time NT, and c_3 = cost of each PM with $c_3 < c_2$. Then, an optimum N^* that minimizes $C_2(N)$ is given as follows: If $L_2(\infty) > (c_2 - c_3)/c_1$, then there exists a finite and unique minimum such that

$$L_2(N) \geq \frac{c_2 - c_3}{c_1} \quad (N = 1, 2, \ldots), \quad (49.69)$$

where

$$L_2(N) \equiv \sum_{j=0}^{N-1} \int_0^T \left[h(t + N(T-x)) - h(t + j(T-x))\right] dt.$$

Thirdly, suppose that the age after PM reduces to at $(0 < a \leq 1)$ when it was t before PM, *i.e.*, the age becomes $t(1-a)$ units of time younger at each PM. Then, the expected cost rate is

$$C_3(N) = \frac{1}{NT}\left[c_1 \sum_{j=0}^{N-1} \int_{A_j T}^{(A_j+1)T} h(t)dt + c_2 + (N-1)c_3\right] \quad (N = 1, 2, \ldots), \quad (49.70)$$

where $A_j \equiv a + a^2 + \cdots + a^j$ $(j = 1, 2, \ldots)$, $A_0 \equiv 0$, and the costs are the same ones as those in (49.66). If $L_3(\infty) > (c_2 - c_3)/c_1$, then there exists a finite and unique minimum such that

$$L_3(N) \geq \frac{c_2 - c_3}{c_1} \quad (N = 1, 2, \ldots), \quad (49.71)$$

where

$$L_3(N) \equiv N \int_{A_N T}^{(A_N+1)T} h(t)dt - \sum_{j=0}^{N-1} \int_{A_j T}^{(A_j+1)T} h(t)dt.$$

Finally, when the failure rate after PM reduces to $bh(t)$ $(0 < b \leq 1)$ when it was $h(t)$ before PM, the expected cost rate is

$$C_4(N) = \frac{1}{NT}\left[c_1 \sum_{j=0}^{N-1} b^j \int_{jT}^{(j+1)T} h(t)dt + c_2 + (N-1)c_3\right] \quad (N = 1, 2, \ldots). \quad (49.72)$$

If $L_4(\infty) > (c_2 - c_3)/c_1$, then there exists a finite and unique minimum such that

$$L_4(N) \geq \frac{c_2 - c_3}{c_1} \quad (N = 1, 2, \ldots), \quad (49.73)$$

where

$$L_4(N) \equiv N b^N \int_{NT}^{(N+1)T} h(t)dt - \sum_{j=0}^{N-1} b^j \int_{jT}^{(j+1)T} h(t)dt.$$

Note that the four models are identical and agree with the standard model in (49.7) when $p = 0$ and $N = 1$.

49.4 Computer Systems

A computer system has usually two types of failures: The system stops because of intermittent faults due to transient faults from noise, temperature, power supply variations, and poor electric contacts. Such faults are often automatically detected by the error correcting code and corrected by the error control, and the system begins to operate again. If the faults cannot be corrected, the system is restarted. On the other hand, the system stops subject to hardware failures or software errors, and then, it breaks down and needs corrective maintenance.

First, we apply the inspection policy to intermittent faults where the test is planned at periodic times to detect faults. We obtain the expected cost until fault detection and derive an optimum test time [2, 30, 31]. Next, we consider a computer system that is restarted when it stops, and discuss optimum PM policies that maximize the availabilities [32]. Furthermore, we apply the imperfect PM policy to a computer system with three imperfect cases, and derive an optimum PM time [2, 33].

49.4.1 Intermittent Faults

Suppose that faults occur intermittently, *i.e.*, a computer system repeats the operating state (state 0) and fault state (state 1) alternately. The times of respective operating and fault states are independent and have identical exponential distributions $(1-e^{-\lambda t})$ and $(1-e^{-\theta t})$ with $\theta > \lambda$. The periodic test to detect faults is planned at times kT $(k = 1, 2, \ldots)$. It is assumed that faults are investigated only through test and are always detected at tests when they have occurred.

The transition probabilities from state 0 to state j $(j = 0, 1,)$ are [1]

$$P_{00}(t) = \frac{\theta}{\lambda+\theta} + \frac{\lambda}{\lambda+\theta} e^{-(\lambda+\theta)t},$$

$$P_{01}(t) = \frac{\lambda}{\lambda+\theta}\left[1 - e^{-(\lambda+\theta)t}\right].$$

Thus, the expected number of $M(T)$ of tests to detect a fault is

$$M(T) = \sum_{j=0}^{\infty} (j+1)\left[P_{00}(T)\right]^j P_{01}(T) = \frac{1}{P_{01}(T)}, \tag{49.74}$$

and the mean time $l(T)$ to detect a fault is

$$\begin{aligned} l(T) &= \sum_{j=0}^{\infty} \left[(j+1)T\right]\left[P_{00}(T)\right]^j P_{01}(T) \\ &= \frac{T}{P_{01}(T)} = TM(T). \end{aligned} \tag{49.75}$$

Further, the probability $P(T)$ that the first occurrence of faults is detected at the first test is

$$\begin{aligned} P(T) &= \int_0^T e^{-\theta(T-t)} \lambda e^{-\lambda t} dt \\ &= \frac{\lambda}{\theta-\lambda}\left(e^{-\lambda T} - e^{-\theta T}\right). \end{aligned} \tag{49.76}$$

The total expected cost until fault detection is, from (49.74) and (49.75),

$$C(T) \equiv c_1 M(T) + c_2 l(T) = \frac{c_1 + c_2 T}{P_{01}(T)}, \tag{49.77}$$

where $c_1 =$ cost of one test and $c_2 =$ operational cost rate of a computer system. Then, an optimum test time T_1^* that minimizes $C(T)$ is given by a finite and unique solution of the equation:

$$\frac{1}{\lambda+\theta}\left[e^{(\lambda+\theta)T} - 1\right] - T = \frac{c_1}{c_2}.$$

Furthermore, an optimum time T_2^* that maximizes $P(T)$ is given by

$$T_2^* = \frac{\log\theta - \log\lambda}{\theta - \lambda}. \tag{49.78}$$

49.4.2 Imperfect Maintenance

A computer system begins to operate at time 0 and has to operate for an infinite time span. When the unit fails, it is repaired immediately and its mean repair time is θ_1. To prevent failures, the unit undergoes PM at periodic times kT $(k = 1, 2, \ldots)$. Then, one of the following three cases after PM results:

(1) The system is not changed with probability p_1, *i.e.*, PM is imperfect.

(2) The system is as good as new with probability p_2, *i.e.*, PM is perfect.

(3) The system fails with probability p_3, *i.e.*, PM becomes failure, where $p_1 + p_2 + p_3 = 1$ and $p_2 > 0$. In this case, the mean repair time for PM failure is θ_2.

The probability that the system is renewed by repair upon actual failures is

$$\sum_{j=1}^{\infty} {p_1}^{j-1} \int_{(j-1)T}^{jT} dF(t) = (1-p_1) \sum_{j=1}^{\infty} {p_1}^{j-1} F(jT), \tag{49.79}$$

the probability that it is renewed by perfect PM is

$$p_2 \sum_{j=1}^{\infty} p_1^{j-1} \overline{F}(jT), \tag{49.80}$$

and the probability that it is renewed by repair upon PM failure is

$$p_3 \sum_{j=1}^{\infty} p_1^{j-1} \overline{F}(jT), \tag{49.81}$$

where (49.79) + (49.80) + (49.81) = 1.

Further, the mean time until the unit is renewed by either repair or perfect PM is

$$\sum_{j=1}^{\infty} p_1^{j-1} \int_{(j-1)T}^{jT} t\,dF(t) + (p_2+p_3)\sum_{j=1}^{\infty} p_1^{j-1}\overline{F}(jT)$$
$$= (1-p_1)\sum_{j=1}^{\infty} p_1^{j-1} \int_0^{jT} \overline{F}(t)dt. \quad (49.82)$$

Therefore, from (49.79)–(49.82), the availability is

$$A(T) = \frac{(1-p_1)\sum_{j=1}^{\infty}\int_0^{jT}\overline{F}(t)dt}{(1-p_1)\sum_{j=1}^{\infty} p_1^{j-1}\int_0^{jT}\overline{F}(t)dt + [(1-p_1)\theta_1]\sum_{j=1}^{\infty} p_1^{j-1}F(jT) + (p_3\theta_3)\sum_{j=1}^{\infty} p_1^{j-1}\overline{F}(jT)}. \quad (49.83)$$

Then, an optimum time T^* that maximizes the availability $A(T)$ is given as follows: Suppose that

$$Q(T) \equiv \frac{\sum_{j=1}^{\infty} p_1^{j-1} j f(jT)}{\sum_{j=1}^{\infty} p_1^{j-1} j\overline{F}(jT)}$$

is strictly increasing and $K \equiv (1-p_1)/(p_2\mu)$. Then, if $Q(\infty) > K$ and $(1-p_1)\theta_1 < p_3\theta_2$, there exists a finite and unique T^* that satisfies

$$Q(T)\sum_{j=1}^{\infty} p_1^{j-1}\int_0^{jT}\overline{F}(t)dt - \sum_{j=1}^{\infty} p_1^{j-1}F(jT) = \frac{p_3}{1-p_1}\frac{\theta_2}{(1-p_1)\theta_1 - p_3\theta_2}, \quad (49.84)$$

and the resulting availability is

$$A(T^*) = \frac{1}{1+[\theta_1 - p_3\theta_2/(1-p_1)]Q(T^*)}. \quad (49.85)$$

49.4.3 Optimum Restart

Consider a computer system where restarts due to system failures occur in a nonhomogeneous Poisson process with a mean value function $H(t)$: When the system stops, it is restarted. The restart succeeds with probability q $(0 < q \le 1)$. In this case, the system returns to its initial condition and the intensity function remains undisturbed by restart. Conversely, the restart fails with probability $p \equiv 1-q$. In this case, the system breaks down and undergoes CM with mean time θ_1. The system undergoes PM with mean time $\theta_2 < \theta_1$ at time T. Then, the probability that the system needs CM in time T is

$$F_p(T) \equiv \sum_{j=0}^{\infty}\left(q^j p\right) p_j[H(T)] = 1 - e^{-pH(T)}. \quad (49.86)$$

Thus, replacing $F(t)$ in (49.83) with $F_p(t)$, we can obtain the availability $A_1(T)$.

Next, suppose that the system undergoes PM when the N th restart succeeds. Then, because the mean time to the Nth restart is $\sum_{j=0}^{N-1} q^j \int_0^{\infty} p_j[H(t)]dt$, the availability is:

$$A_2(N) = \frac{\sum_{j=0}^{N-1} q^j \int_0^{\infty} p_j[H(t)]dt}{\sum_{j=0}^{N-1} q^j \int_0^{\infty} p_j[H(t)]dt + (1-q^N)\theta_1 + q^N\theta_2} \quad (N = 1,2,\ldots). \quad (49.87)$$

If $h(t)$ is strictly increasing and $h(\infty)p\int_0^{\infty} e^{-pH(t)}dt > \theta_1/(\theta_1-\theta_2)$, then there exists a finite and unique minimum such that

$$\frac{p\sum_{j=0}^{N-1} q^j \int_0^{\infty} p_j[H(t)]dt}{\int_0^{\infty} p_N[H(t)]dt} - (1-q^N) \ge \frac{\theta_2}{\theta_1-\theta_2} \quad (N = 1,2,\ldots). \quad (49.88)$$

Finally, the PM is planned only at times kT $(k = 1,2,\ldots)$ as shown in Section 49.3.3. If the total number of successful restarts exceeds a specified number N, the PM is done at the next PM time, otherwise no PM is done. Then, the availability is

$$A_3(N) = \frac{\sum_{k=0}^{\infty}\int_{kT}^{(k+1)T}\overline{F}_p(t)dt\sum_{j=0}^{N-1} p_j[qH(kT)]}{\sum_{k=0}^{\infty}\int_{kT}^{(k+1)T}\overline{F}_p(t)dt\sum_{j=0}^{N-1} p_j[qH(kT)] + \theta_2 + (\theta_1-\theta_2)\left[F_p((k+1)T) - F_p(kT)\right] \times \sum_{j=0}^{N-1} p_j[qH(kT)]}. \quad (49.89)$$

In this case, (49.88) is rewritten as

$$\frac{\sum_{k=0}^{\infty}\int_{kT}^{(k+1)T}\overline{F}_p(t)dt\sum_{j=0}^{N-1}p_j\left[qH(kT)\right]}{\sum_{k=0}^{\infty}\int_{kT}^{(k+1)T}\overline{F}_p(t)dt\,p_N\left[qH(kT)\right]}$$

$$\times\sum_{k=0}^{\infty}\left[F_p((k+1)T)-F_p(kT)\right]p_N\left[qH(kT)\right]$$

$$-\sum_{k=0}^{\infty}\left[F_p((k+1)T)-F_p(kT)\right]\sum_{j=0}^{N-1}p_j\left[qH(kT)\right]$$

$$\geq\frac{\theta_2}{\theta_1-\theta_2}\qquad(N=1,2,\ldots).\qquad(49.90)$$

References

[1] Barlow RE, Proschan F. Mathematical theory of reliability. Wiley, New York, 1965.

[2] Nakagawa T. Maintenance theory of reliability. Springer, London, 2005.

[3] Barlow RE, Proschan F. Statistical theory of reliability and life testing probability models. Holt, Rinehart and Winston, New York, 1975.

[4] Gertsbakh I. Models of preventive maintenance. North-Holland, Amsterdam, 1997.

[5] Osaki S, Nakagawa T. Bibliography for reliability and availability of stochastic systems. IEEE Transactions on Reliability 1976; R-25:284–287.

[6] Pierskalla WP, Voelker JA. A survey of maintenance models: The control and surveillance of deteriorating systems. Naval Research Logistics 1976; Q 23:353–388.

[7] Sherif YS, Smith ML. Optimal maintenance models for systems subject to failure - A review. Naval Research Logistics 1981; Q 28:47–74.

[8] Thomas LC. A survey of maintenance and replacement models for maintainability and reliability of multi-item systems. Reliability Engineering 1986; 16: 297–309.

[9] Valdez-Fores C, Feldman RM. A survey of preventive maintenance models for stochastically deteriorating single-unit system. Naval Research Logistics 1989; Q 36: 419–446.

[10] Cho DI, Parlar M. A survey of maintenance models for multi-unit systems. European Journal of Operational Research 1991; 51:1–23.

[11] Dekker R. Applications of maintenance optimization models: A review and analysis. Reliability Engineering and System Safety 1996; 51: 229–240.

[12] Wang H. A survey of maintenance policies of deteriorating systems. European Journal of Operational Research 2002; 139:469–489.

[13] Ozekici S (editor). Reliability and maintenance of complex systems. Springer, Berlin, 1996.

[14] Ben-Daya M, Duffuaa SO, Raouf A. (editors). Maintenance, modeling and optimization.Kluwer, Boston, 2000.

[15] Rahin MA, Ben-Daya M. Integrated models in production planning, inventory, quality, and maintenance. Kluwer, Boston, 2001.

[16] Osaki S (editor). Stochastic models in reliability and maintenance. Springer, Berlin, 2002.

[17] Pham H. Handbook of reliability engineering. Springer, London, 2003.

[18] Jensen U. Stochastic models of reliability and maintenance: An overview. In: Ozekici S, editor. Reliability and maintenance of complex systems. Springer, Berlin, 1996; 3–36.

[19] Ben-Daya M, Duffuaa SO. Maintenance modeling areas. In: Ben-Daya M, Duffuaa SO, Raouf A, editors Maintenance, modeling and optimization. Kluwer, Boston, 2000; 3–35.

[20] Kaio N, Dohi T, Osaki S. Classical maintenance models. In: Osaki S, editor. Stochastic models in reliability and maintenance. Springer, Berlin, 2002; 65–87.

[21] Nakagawa T. Maintenance and optimum policy. In: Pham H, editors Handbook of reliability engineering. Springer, London, 367–395.

[22] Wang H, Pham H. Reliability and optimal maintenance. Springer, London, 2006.

[23] Nakagawa T, Mizutani S. A summary of maintenance policies for a finite interval. To appear in Reliability Engineering and System Safety. 2008.

[24] Nakagawa T. Shock and damage models in reliability theory. Springer, London, 2007.

[25] Nakagawa T. Two-unit redundant model. In: Osaki S, editor. Stochastic models in reliability and maintenance. Springer, Berlin, 2002.

[26] Nakagawa T. Modified discrete preventive maintenance policies. Naval Research Logistics 1986;Q 33:703–715.

[27] Nakagawa T. Periodic and sequential preventive maintenance policies. Journal of Applied Probability 1986; 23:536–542.

[28] Nakagawa T. Imperfect preventive maintenance models. In: Osaki S, editor. Stochastic models in reliability and maintenance. Springer, Berlin 2002; 125–143.

[29] Wang H., Pham H. Optimal imperfect maintenance models. In: H. Pham, editor. Handbook of

reliability engineering. Springer, London 2003; 397–414.
[30] Nakagawa T, Motoori M, Yasui K. Optimal testing policy for a computer system with intermittent faults. Reliability and Engineering System Safety 1990; 27: 213–218.
[31] Nakagawa T, Yasui K. Optimal testing-policies for intermittent faults. IEEE Transactions on Reliability 1989; 38:577–580.
[32] Nakagawa T, Nishi K, Yasui K. Optimum preventive maintenance policies for a computer system with restart. IEEE Transactions on Reliability1984; R-33:272–276.
[33] Nakagawa T, Yasui K. Optimum policies for a system with imperfect maintenance. IEEE Transactions on Reliability 1987; R-36:631–633

50

Effective Fault Detection and CBM Based on Oil Data Modeling and DPCA

Viliam Makis and Jianmou Wu

University of Toronto, Department of Mechanical and Industrial Engineering
5 King's College Rd., Toronto, Canada M5S 3G8

Abstract: This chapter presents two methodologies for effective equipment condition monitoring and condition-based maintenance (CBM) decision-making. The first method is based on multivariate modeling of data obtained from condition monitoring (CM data), dimensionality reduction using dynamic principal component analysis (DPCA), and constructing and using on-line a multivariate statistical process control (MSPC) chart based on the DPCA. The second method is based on vector autoregressive (VAR) modeling of CM data, DPCA, and building a proportional hazards (PH) decision model using the retained principal components as covariates. These methodologies are illustrated by an example using real oil data histories obtained from spectrometric analysis of heavy-hauler truck transmission oil samples taken at regular sampling epochs. The performances of the MSPC chart-based policy and the PH model-based optimal control limit policy are evaluated and compared with the traditional age-based policy.

50.1 Introduction

High complexity and sophistication of modern manufacturing systems has increased the impact of unplanned downtime caused by system failures. Unplanned downtime reduces productivity, increases product or service variability, and results in an increased maintenance spending due to breakdown maintenance. Effectively planned maintenance activities are becoming more and more important in modern manufacturing. Various maintenance schemes have been widely applied in industry, from corrective and time-based maintenance to condition-based maintenance (CBM). CBM is a maintenance strategy based on collected condition data that are related to the system health or status [1]. A CBM policy is based on monitoring an equipment condition on-line (*e.g.*, machine vibration monitoring or spectrometric analysis of oil samples) and making maintenance decisions based on the partial information obtained from the observation process. The concept of CBM has been widely accepted in maintenance practice due to the availability of advanced condition-monitoring technology capable of collecting and storing a large amount of data when the equipment is in operation. Several CBM models have appeared in the maintenance literature, such as a proportional hazards model in [2], a random coefficient regression model in [3], a counting-process model in [4], a state-space model in [5], an optimal-stopping

model in [6], and a hidden Markov model in [7], among others.

This chapter presents two novel methodologies for effective equipment condition monitoring and condition-based maintenance (CBM) decision-making based on multivariate modeling of CM data, dimensionality reduction using dynamic principal component analysis (DPCA), constructing a multivariate statistical process control (MSPC) chart based on the DPCA results, and building a proportional hazards (PH) model using the retained principal components as covariates.

Statistical process control (SPC) concepts and methods are very useful in industrial practice for process condition monitoring and fault detection. SPC uses statistically based methods to evaluate and monitor a process or its output in order to achieve or maintain a state of control [8]. It is still common in many industries to apply univariate SPC methods, such as Shewhart, CUSUM and EWMA charts, to a small number of variables and examine them one at a time. Due to the availability of advanced condition-monitoring technologies that are able to collect and store a large amount of process data, these univariate approaches should be replaced by multivariate methods. The multivariate process data should be used to extract information in an effective manner for monitoring operating performance and failure diagnosis. Various multivariate SPC (MSPC) charts, such as χ^2, T^2, multivariate CUSUM and EWMA have been developed and can be used for this purpose.

Although the MSPC charts have been applied in industrial practice, the main focus has been on multivariate quality control. Little attention has been paid to the implementation of MSPC for fault detection and maintenance decision-making. Considering the similarity between on-line quality control and condition monitoring for maintenance purposes, the application of multivariate SPC tools to CBM seems to be very appealing. The advantage of this approach when compared with the previously developed CBM models is the relative simplicity of the multivariate charting methods and an easy implementation in industrial practice. Some recent attempts to integrate SPC and maintenance control can be found in the literature (see, *e.g.*, [9], [10], [11], and [12]). However, in these studies only relatively simple univariate SPC approaches have been used. To our knowledge, there has been no SPC application based on real data in the maintenance literature.

Using the T^2 control chart, Jackson and Mudholkar [13] investigated PCA as a multivariate SPC tool for the purpose of dimensionality reduction and introduced residual analysis. The PCA-based (T_A^2, Q) control charts are very useful for monitoring multivariable industrial processes, but they cannot be directly applied in CBM because PCA assumes independence of successive samples, whereas the maintenance data typically exhibit both cross and auto-correlation. Dynamic PCA, an extension of PCA, can be successfully applied to such data, and therefore a DPCA version of the combined T_A^2 and Q, charts would be appropriate for a maintenance application. In this chapter, we apply the DPCA-based (T_A^2, Q) charts to the CM data and illustrate the method using real heavy hauler truck transmission oil data for failure prevention and CBM decision-making.

PHM, first proposed by Cox in 1972, has become very popular to model the lifetime data in biomedical sciences, and recently also in reliability and maintenance applications. In CBM modeling, PHM integrates the age information with the condition information to calculate the risk of failure (hazard rate) of a system. In the paper by Makis and Jardine [2], a PH decision model was considered and the structure of the optimal replacement policy minimizing the total expected average maintenance cost was obtained. The computational algorithms for this PH decision model were published by Makis and Jardine [14].

In this chapter, the CBM modeling is based on the above PH model. The sampling data gained from condition monitoring can be represented in a vector form and the components in a data vector are termed as covariates in PH modeling. Usually the covariates are both cross-correlated and auto-correlated because they are related to the same deterioration process. The amount of data collected at a sampling epoch is usually very large and it is therefore important to reduce data dimensionality and capture most of the information contained in the original data set. Therefore, we first apply the

multivariate time series methodology to fit a vector autoregressive (VAR) model to the whole oil data histories. Then, a DPCA is performed and the principle components capturing most of the data variability are selected. These principal components are then used as the covariates to build a PH model for CBM purposes.

50.2 Fault Detection Using MSPC, VAR Modeling and DPCA

50.2.1 Hotelling's T^2 Chart and PCA-based (T_A^2, Q) Charts

The best-known control charts for monitoring multivariate processes are Hotelling's χ^2 and T^2 charts [15]. Assume that when the process is in control, a *k*-dimensional vector Y_t of measurements has a multivariate normal distribution with mean vector μ and covariance matrix Σ. The following statistic

$$\chi_t^2 = (Y_t - \mu)'\Sigma^{-1}(Y_t - \mu) \qquad (50.1)$$

is plotted on the chart for which the upper control limit (UCL) is $\chi_{\alpha,k}^2$, where α is the selected probability of false alarm.

When the in-control mean vector μ and covariance matrix Σ are unknown and must be estimated from a sample of data, the Hotelling's T_t^2 statistic is used:

$$T_t^2 = (Y_t - \hat{\mu})'S^{-1}(Y_t - \hat{\mu}), \qquad (50.2)$$

where $\hat{\mu}$ and S are the estimates of the process mean μ and the covariance matrix Σ, respectively. The upper control limit T_{UCL}^2 is obtained from the *F* distribution with k and $N-k$ degrees of freedom, where N is the size of the sample used to estimate μ and Σ,

$$T_{UCL}^2 = \frac{(N^2-1)k}{N(N-k)}F_\alpha(k, N-k). \qquad (50.3)$$

Principal component analysis (PCA) is a linear transformation method that can obtain a set of uncorrelated variables, termed principal components (PCs), from the original set of variables. The obtained PCs have special properties in terms of variances. For example, the first PC is the standardized linear combination with maximum variance. The second PC has maximum variance of all linear combinations uncorrelated with the first PC, *etc.* [16]. When the PCA is used to characterize the multivariable observation process, Hotelling's T^2 can also be expressed in terms of PCs:

$$T_t^2 = \sum_{a=1}^{k}\frac{z_{t,a}^2}{l_a}, \qquad (50.4)$$

where $z_{t,a}$ are the PC scores from the principal component transformation and l_a, $a = 1, 2, \cdots, k$, are the eigenvalues of the correlation matrix estimate of the original data.

Furthermore, the PC score vector Z_t can be expressed as Y_t

$$Z_t = (z_{t,1}, z_{t,2}, \cdots z_{t,k})' = (u_1, u_2, \cdots u_k)' \cdot O_t, \qquad (50.5)$$

where $u_1, u_2, \cdots, u_k$ are the eigenvectors of the correlation matrix estimate of the original data set Y_t and the vector O_t is the standardized vector obtained from $O_t = (\frac{Y_{t,1}-\bar{Y}_1}{s_1}, \frac{Y_{t,2}-\bar{Y}_2}{s_2}, \cdots, \frac{Y_{t,k}-\bar{Y}_k}{s_k})'$, with $\bar{Y}_i$ and s_i denoting the sample mean and standard deviation for variable $i, (i = 1, \cdots, k)$.

When PCA is used to reduce dimensionality, the T^2 chart based on the first A selected principal components is constructed as follows:

$$T_{A,t}^2 = \sum_{a=1}^{A}\frac{z_{t,a}^2}{l_a} = \sum_{a=1}^{A}\frac{(u_a' \cdot O_t)^2}{l_a}. \qquad (50.6)$$

Then, based on the above formula, we can rewrite the T_t^2 statistic as follows [8], [17]

$$T_t^2 = \sum_{a=1}^{A}\frac{z_{t,a}^2}{l_a} + \sum_{a=A+1}^{k}\frac{z_{t,a}^2}{l_a^2} = T_{A,t}^2 + \sum_{a=A+1}^{k}\frac{z_{t,a}^2}{l_a^2}. \qquad (50.7)$$

The T_A^2 statistic based on the first A uncorrelated PCs provides a test for deviations in the condition monitoring variables that contribute most to the variance of the original data set Y_t. The upper control limit of T_A^2 can be calculated from (50.3) with k replaced by A [17].

However, only monitoring the process via T_A^2 is not sufficient. This method can only detect whether the variation in the condition monitoring variables in the space defined by the first A principal components exceeds UCL or not. In case a totally new type of special event occurs, which can cause the machine failure and was not presented when developing the in-control PCA model, then new PC's will appear and the new observation will move off the space defined by the in-control PCA model. Such new events can be detected by monitoring the squared prediction error (SPE) of the observation residuals, which gives a measure of how close an observation is to the A-dimensional space defined by the in-control PCA model:

$$SPE_t = \sum_{i=1}^{k} (O_{t,i} - \hat{O}_{t,i})^2 , \qquad (50.8)$$

where $\hat{O}_t = \sum_{a=1}^{A} Z_{t,a} \cdot u_a$ is computed from the in-control PCA model.

The SPE statistic is also referred to as a Q statistic [18]. The upper control limit for the Q statistic can be computed using approximate results for the distribution of quadratic forms [18], [19]. With significance level α, the UCL can be computed from the following formula:

$$Q_\alpha = \theta_1 [1 - \theta_2 h_0 (1 - h_0) / \theta_1^2 + z_\alpha (2\theta_2 h_0^2)^{1/2} / \theta_1]^{1/h_0} \qquad (50.9)$$

where z_α is the $100(1-\alpha)$ normal percentile, $\theta_i = \sum_{j=A+1}^{k} l_j^i, i = 1, 2, 3,$ and $h_0 = 1 - 2\theta_1\theta_3 / 3\theta_2^2$ [20]. When the process is in control, Q represents unstructured fluctuations (noise) that cannot be accounted for by the PCA model. When an unusual event occurs that results in a change in the covariance (or correlation) structure of the original data set, it will be detected by a high value of Q. In this case, the PCA model may no longer be valid.

A T_A^2 chart on the A dominant orthogonal PCs plus a Q chart is an effective set of multivariate SPC charts. On one hand, because the T_A^2 statistic is not affected by the smaller eigenvalues of the correlation matrix, it provides a more robust fault detection measure. T_A^2 can be interpreted as measuring the systematic variation in the PCA subspace, and a large value of T_A^2 exceeding the threshold would indicate that the systematic variation is out of control [20]. On the other hand, the T^2 chart is overly sensitive in the PCA space because it includes the scores corresponding to the small eigenvalues representing noise which may contribute significantly to the value of the T^2 statistic. The Q (SPE) statistic represents the squared perpendicular distance of a new multivariate observation from the PCA subspace and it is capable of detecting a change in the correlation structure when a special event occurs.

50.2.2 The Oil Data and the Selection of the In-control Portion

The data used in this chapter are the histories of the diagnostic oil data obtained from the 240-ton heavy hauler truck transmissions. Oil samples are taken roughly every 600 hours and the results of the spectrometric analysis consisting of the measurements of 20 metal elements in ppm are recorded. The total number of oil data histories considered is 51, 20 of them ended with a failure and the remaining 31 were suspended. A preliminary analysis by using EXAKT software (http://www.mie.utoronto.ca/labs/cbm) and also the results obtained previously [21] indicate that it is sufficient to consider only 6 out of the total of 20 metal elements, namely potassium, iron, aluminum, magnesium, molybdenum and vanadium for maintenance decision-making.

Since it is a set of six-dimensional data and the in-control covariance matrix is unknown, we decided to calculate and plot the T^2 statistic in order to determine the portions of the histories when transmission was in a healthy state. Before plotting the T^2 statistic and selecting the in-control portion of the oil data, it was necessary to pre-process the raw oil data. To satisfy the equal sampling interval condition, we discarded six histories that have sampling intervals far greater than 600 hours. In the remaining 45 histories, the sampling records were excluded when the sampling intervals were far less than 600 hours. There were also nine short histories that have less than six records. Since it does not make much sense to select the in-control portions from these short histories, we discarded them too. Finally, we considered 36 histories that are long enough and equally spaced. The total number of the oil data records is 527. The T^2 statistic was calculated and plotted and the in-control portion of the data was identified.

The sample mean and covariance matrix were estimated from the data and the T_t^2 values were calculated using (50.2). For the upper control limit T_{UCL}^2, we set k=6 and N=527 in (50.3) because our oil data is 6-dimensional and we have totally 527 observations in the remaining 36 histories. Choosing the significance level $\alpha = 0.025$, we found $F_\alpha(k, N-k) = 2.4325$ and $T_{UCL}^2 = 14.763$.

On selecting the healthy portion of the oil data, the following three working states of the transmissions were considered: initial state, healthy state and deteriorating state. Also, we note that the transmission oil was changed every 1200 hours, which dramatically affected the cumulative increasing trend of the T_t^2 series. We have decided to apply the following criteria to find out the in-control portion of the oil data. When the T_t^2 value exceeded the upper control limit T_{UCL}^2 during the first three observations of a history, we assumed the transmission was in the initial run-in state before reaching the normal operating state. We excluded all the initial records in the histories up to and including the ones that exceeded the upper control limit. On the other hand, when an abnormal value of T_t^2 appeared later in the history ($t \geq 6$), it was assumed that the transmission reached a deteriorating state and all the following observations were excluded. The remaining observations are the portions of the histories when transmission was in a healthy state. Following this procedure, we selected 409 out of 527 records as the healthy portion of the oil data histories.

50.2.3 Multivariate Time Series Modeling of the Oil Data in the Healthy State

We assume that the evolution of the observation process is described by a VAR model which proved to be a good representation of the oil data obtained from condition monitoring in our previous research [22], [23]. Using the in-control portion of the oil data, we can build a stationary VAR model to describe the observation process.

We have applied the Yule–Walker estimation method to calculate the model parameter estimates. The model order was determined by a test using Wald statistic. After fitting the VAR model, we also checked the model stationarity condition in order to confirm that our method of selecting the in-control portion of the data histories is appropriate. The details of the Yule–Walker methodology, Wald statistic and the stationarity condition check can be found in [24].

By extending the Yule–Walker estimator formulae and the Wald statistic formula to a multi-history case and applying them to the in-control portion of the oil data, we have the following modeling results. For m = 2, 3, 4, 5 the order test Wald statistic values are W_2 = 59.6080, W_3 = 29.8101, W_4 = 21.8461, and W_5 = 13.6612. We can see that there is a clear drop in these values between W_2 and W_3. By setting the significance level $\alpha = 0.025$, we find the critical value $C = X_{36,0.025}^2 = 54.437$ from the chi-square distribution with $k^2 = 36$ degrees of freedom. Since $W_2 > C$ and $W_3 < C$, we reject $H_0 : \Phi_{22} = 0$ and fail to reject $H_0 : \Phi_{33} = 0$. Thus, we conclude that an AR(2) model is adequate to model the in-control portion of the oil data. The order of the AR

model is also used in the dynamic principle component analysis (DPCA) later in the chapter as the time lag value.

For the fitted AR(2) model $(Y_t - \mu) = \Phi_{12}(Y_{t-1} - \mu) + \Phi_{22}(Y_{t-2} - \mu) + \varepsilon_t$, the estimates of the parameters are as follows,

$$\hat{\mu}_6 = (2.3899 \quad 8.9342 \quad 1.3215 \quad 8.2506 \quad 0.5114 \quad 0.1038)'$$

$$\hat{\Phi}_{12} = \begin{bmatrix} 0.7150 & -0.0237 & 0.1045 & 0.0008 & -0.1016 & -0.0433 \\ 0.2618 & 0.4857 & -0.8588 & -0.0211 & 0.4640 & -0.3494 \\ 0.0145 & 0.0082 & 0.2323 & 0.0003 & -0.0942 & 0.0196 \\ -0.2546 & -0.0100 & 0.9894 & 0.4606 & 0.7465 & -1.2370 \\ 0.0142 & 0.0012 & -0.0081 & -0.0025 & 0.0996 & -0.0034 \\ -0.0149 & 0.0023 & 0.0546 & -0.0012 & -0.0493 & 0.0625 \end{bmatrix}$$

$$\hat{\Phi}_{22} = \begin{bmatrix} -0.1385 & 0.0003 & -0.2326 & 0.0014 & 0.0591 & 0.2485 \\ -0.1378 & 0.1302 & 0.7855 & 0.0099 & 0.0037 & 0.7663 \\ -0.0300 & -0.0039 & 0.2115 & -0.0031 & -0.0626 & -0.0538 \\ 0.2238 & -0.0209 & 0.1360 & -0.0063 & 0.3450 & -0.9185 \\ -0.0119 & -0.0062 & -0.0377 & -0.0001 & 0.1411 & -0.0023 \\ 0.0143 & -0.0057 & -0.0188 & 0.0006 & 0.0899 & 0.0384 \end{bmatrix}$$

$$\hat{\Sigma}_2 = \begin{bmatrix} 6.6044 & 1.1622 & 0.0802 & -2.8131 & 0.0168 & 0.1088 \\ 1.1622 & 25.3816 & 0.2222 & 1.9658 & 0.4041 & 0.0739 \\ 0.0802 & 0.2222 & 0.2333 & -0.3565 & 0.0974 & 0.0245 \\ -2.8131 & 1.9658 & -0.3565 & 75.2260 & 0.0304 & -0.1669 \\ 0.0168 & 0.4041 & 0.0974 & 0.0304 & 0.2686 & 0.0211 \\ 0.1088 & 0.0739 & 0.0245 & -0.1669 & 0.0211 & 0.2239 \end{bmatrix}$$

The eigenvalues of Φ_2 are (−0.4261, −0.2512 + 0.1343*i*, −0.2512 − 0.1343*i*, −0.1792, −0.0000, 0.2915 + 0.2170*i*, 0.2915 −0.2170*i*, 0.6724, 0.6135, 0.4358 + 0.0667i, 0.4358 −0.0667*i*, 0.4230), where Φ_2 is described as $\Phi_2 = \begin{bmatrix} \Phi_{12} & \Phi_{22} \\ I & 0 \end{bmatrix}$. Since the eigenvalues are all less than one in absolute value, the fitted AR(2) model is stationary. This result indicates that choosing the relatively simple Yule–Walker method for the AR model parameters estimation and Wald statistic for the model order selection is appropriate.

50.2.4 Dynamic PCA and the DPCA-based $(T^2_{4,t}, Q_t)$ Charts for the Oil Data

The readings of the six metal elements representing the oil data are both cross and auto-correlated. Since the oil data does not satisfy the assumption of independence of samples collected at different time epochs, the original PCA method is not suitable here. Directly applying PCA to the oil data will not reveal the exact relations between the variables of the process. DPCA, an extension of the PCA method, is used to process the oil data. The correlation relationship in the oil data is represented by the cross-covariance and the auto-covariance matrices. The correlation relationship can be represented by the covariance matrices $\Gamma(0), \Gamma(1)$ and $\Gamma(2)$. $\Gamma(0)$ is the cross-covariance matrix and $\Gamma(i)$ is the auto-covariance matrix of time lag $i, i = 1, 2$. These covariance matrices are used when applying DPCA to the oil data. Unlike the PCA method, when DPCA is applied, the data matrix is composed of the time-shifted data vectors (see, *e.g.*, [25]).

DPCA is based on conducting singular value decomposition on an augmented data matrix containing time lagged process variables. It is essentially the same as PCA except that the data vectors of the variables consist of the current data vector Y_t and the time-shifted vectors $Y_{t-1}, Y_{t-2}, \cdots$. For example, in the case of our oil data, the process dynamics is described by a vector AR(2) model so that the data vector considered in the DPCA is $(Y'_t, Y'_{t-1}, Y'_{t-2})'$ instead of Y_t which would be considered in the PCA.

The starting point for DPCA is to obtain the sample covariance matrix $\hat{\Gamma}$. In our vector AR(2) model, the covariance matrix Γ consists of $3 \times 3 = 9$ blocks, each of dimension 6×6, where the $(i, j)th$ block matrix is $\Gamma(i - j)$, $\Gamma(i - j) = \Gamma(j - i)'$ if $i - j < 0$, for $i, j = 1, 2, 3$. In this section, $\Gamma(i)$ denotes the sample covariance matrix of time lag i. If the original variables are in different units, or their means vary widely, as is the case for our oil data, it is more appropriate to use the correlation matrix rather than the covariance

matrix. The lag i correlation matrix can be obtained from the covariance matrix directly by $R(i) = D^{-1}\Gamma(i)D^{-1}, i = 0,1,2$, where D is the diagonal matrix of standard deviations of the original variables. The structure of the sample correlation matrix used in DPCA is the same as the structure of the sample covariance matrix Γ, *i.e.*, the $(i, j)th$ block matrix is $R(i-j)$, where $R(i-j) = R(j-i)'$ if $i-j<0$, $i, j = 1,2,3$. Replacing O_t by $D_t = (O'_t, O'_{t-1}, O'_{t-2})'$ in (50.5), we can obtain the PC scores from the original oil data.

The eigenvalues $\{l_i\}$ of the sample correlation matrix R ordered from the largest to the smallest are the sample variances of the (sample) principal components. The purpose of DPCA is to generate a reduced set of variables (PCs) that accounts for most of the variability in the original oil data. A number of procedures for determining how many components to retain have been suggested in [26]. Here we apply the scree test, an approach first proposed by Cattell [27]. In the scree test, the eigenvalues are plotted in successive order of their extraction and then an "elbow" in the curve is identified such that the bottom portion of the eigenvalues after the "elbow" forms an approximate straight line. The points above the straight line in the curved portion of the plot correspond to the retained PCs. The result of the scree test for the in-control oil data DPCA is shown in Figure 50.1. The eigenvalues obtained after applying DPCA are listed in Table 50.1.

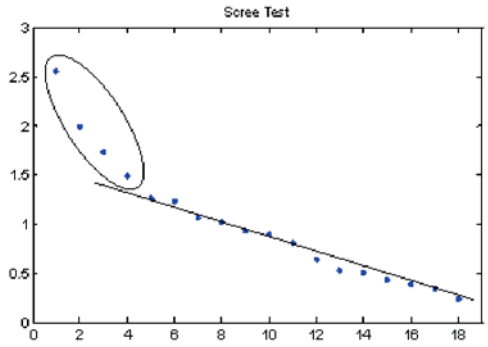


Figure 50.1. Scree test of DPCA for the oil data

The scree test plot in Figure 50.1 clearly shows that there is a break (an elbow) between the first four and the remaining 14 eigenvalues that form approximately a straight line. This result indicates that we should retain the first four PCs to construct our DPCA model.

After applying the DPCA and selecting the principle components accounting for most of the process variation, we obtained a four-dimensional PC scores series. Putting $A = 4$ in (50.6) and (50.8), we calculated the $T^2_{4,t}$ and Q_t values. Setting the significance level as $\alpha = 0.025$, we obtained: $T^2_{4,UCL} = 11.4305$, $Q_{UCL} = 23.2147$ from (50.3) and (50.9). We then plotted the $T^2_{4,t}$ and the Q_t values on the corresponding charts. The T^2_4 chart shows too many false alarms and misses most of the impending failures. The reason is that the four-dimensional PC score series is still highly serially correlated, which makes the T^2_4 chart in-

Table 50.1. Successive eigenvalues l_i and eigenvalues diffenerce l_i-l_{i+1}

	***i*=1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
l_i	2.5504	1.9820	1.7287	1.4809	1.2588	1.2259	1.0655	1.0203	0.9268
l_i-l_{i+1}	0.5684	0.2533	0.2478	0.2221	0.0329	0.1604	0.0452	0.0935	0.0339
	10	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
l_i	0.8929	0.8020	0.6396	0.5292	0.5025	0.4326	0.3852	0.3398	0.2369
l_i-l_{i+1}	0.0909	0.1624	0.1104	0.0267	0.0699	0.0474	0.0454	0.1029	–

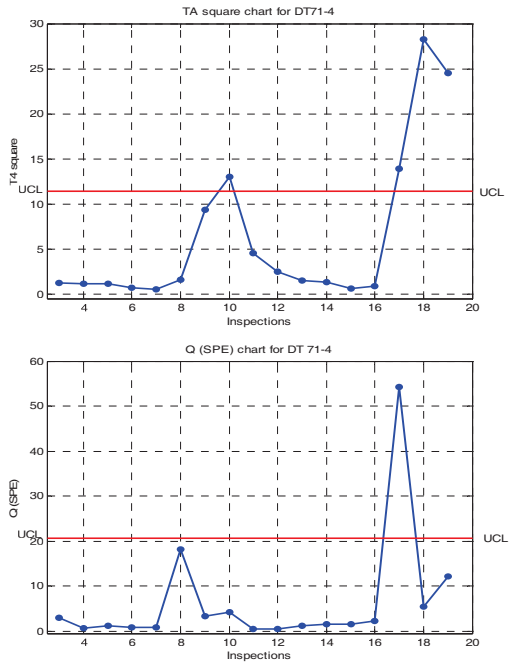


Figure 50.2. An example of the DPCA-based T_4^2 chart and Q chart

effective. On the other hand, the Q chart is based on the residuals of the DPCA model and serial correlation is not significant when the process is in control. In the Q chart, false alarms are significantly reduced and the true alarms coincide with the impending transmission failures.

For example, Figure 50.2 compares the DPCA-based T_4^2 chart and Q charts applied to history DT 71-4 which ended with suspension. On the T_4^2 chart, out-of-control alarms appear at the 10th, 17th, 18th and 19th sampling points. It is clear that the 17th sampling point alarm in the T_4^2 chart has an effect on the next two $T_{4,t}^2$ values because of the high serial correlation of the PC scores and two subsequent alarms appeared that should not be there. On the Q chart, only one alarm appears at the 17th sampling point. Because this history ended with suspension, which means the transmission worked properly until it was suspended, all these alarms are false alarms although the alarm generated by the Q chart is much closer to the suspension time than the alarms on the T_4^2 charts. Therefore, it is obvious that the T_4^2 chart is not appropriate for transmission condition monitoring due to the serial correlation of the oil data, and the Q chart shows a better performance. Note that the T_4^2 chart and the Q chart begin with the third sample because the time shift in DPCA makes the first two $T_{4,t}^2$ and Q_t values unavailable.

50.2.5 Performance Comparison of Fault Detection and Maintenance Cost

In this section, we check the fault detection performance of the DPCA-based Q chart, denoted as Q_{DPCA} chart and perform a maintenance cost comparison between the Q_{DPCA} chart-based policy and the age-based policy.

By setting the significance level $\alpha = 0.025$, we first applied the Q_{DPCA} chart to the 23 histories that ended with suspension. In these cases, the histories ended with suspensions and the transmissions were replaced applying the age-based policy after about 12,000 working hours regardless of their actual conditions. Thus, we only focused on the false alarms in the chart. One can assume that the out-of-control signals occurring at the first three samplings are run-in period alarms. After the run-in period any subsequent signals can be considered to be false alarms. The out-of-control signals and the false alarms (in bold font) are summarized in Table 50.2. Totally, there are only 6 false alarms in the Q_{DPCA} chart for the 23 suspended histories.

For the failure histories, our main goal is to compare the failure detection capability of the two charting methods. If the out-of-control signal occurs just before failure, *i.e.*, at the last sampling point, the SPC chart indicates the impending failure perfectly and triggers a preventive replacement which avoids failure. Furthermore, in case the Q_{DPCA} statistic value dramatically

Table 50.2. Application of the Q_{DPCA} chart to the suspended data histories

Histories	Number of samples	Alarms on Q_{DPCA} chart
DT 65-1	11	–
DT 65-2	20	–
DT 65-3	13	–
DT 66-2	21	–
DT 66-3	17	–
DT 67-2	20	**15th**
DT 67-3	22	–
DT 68-1	20	–
DT 69-3	17	–
DT 70-1	20	–
DT 70-2	20	**10th, 17th**
DT 70-3	13	–
DT 71-4	19	**17th**
DT 71-5	10	–
DT 72-1	20	3rd
DT 72-3	8	–
DT 74-1	20	**18th**
DT 74-3	13	–
DT 75-1	20	–
DT 76-2	17	–
DT 77-3	17	**5th**
DT 78-1	15	–
DT 79-3	7	–

increases, even if it does not exceed the control limit, this can also be considered as an alarm indicating the impending failure. Examples of the Q_{DPCA} chart applied to the failure histories, DT 68-2 and DT 72-2, are given in Figure 50.3. The trends of the Q_{DPCA} are increasing in both plots and engineers can easily figure out that the signals indicate transmission impending failures.

The alarms which occur in the middle part of the failure histories (excluding the first three samples) are treated as false alarms and the significance level is $\alpha = 0.025$. The results for the Q_{DPCA} chart applied to the failure histories are

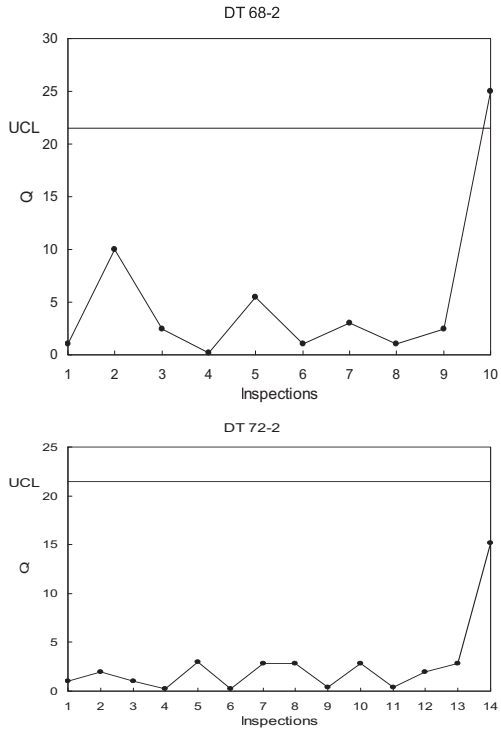


Figure 50.3. Examples of Q_{DPCA} chart applied to the failure histories

given in Table 50.3. The Q_{DPCA} chart triggers 7 preventive replacements without giving any false alarm for the 13 failure histories.

From the results in Tables 50.2 and 50.3, we can conclude that the Q_{DPCA} chart is an effective SPC charting method which can prevent considerable number of failures in a timely manner without generating an excessive number of false alarms. Next, we perform a maintenance cost analysis between the Q_{DPCA} chart-based policy and the age-based policy in order to confirm the effectiveness of the Q_{DPCA} chart.

When the chart signals, the transmission is inspected by a technician to find out whether it is a false alarm or an indication of impending failure. Therefore, every alarm incurs a sampling cost, which includes also the cost related to machine downtime. In case the alarm occurs at the last sampling point before failure, preventive replacement is considered. The preventive replacement

Table 50.3. Application of the Q_{DPCA} chart to the failure histories

Histories	Number of samplings	Alarms in Q_{DPCA} chart
DT 66-1	18	18th
DT 67-1	13	13th (Q increases)
DT 68-2	10	10th
DT 68-3	–	–
DT 68-4	–	–
DT 69-2	16	16th
DT 71-1	9	3rd
DT 71-2	9	9th
DT 72-2	14	14th (Q increases)
DT 73-1	–	–
DT 74-2	–	–
DT 77-1	7	7th
DT 79-2	–	–

cost includes inspection cost, downtime cost, a transmission re-installation cost and so on. Therefore, in the maintenance cost analysis, only the alarms in the middle of the histories will result in incurring a false alarm cost since the sampling cost is included in the preventive replacement cost.

The following parameters are needed to calculate the total maintenance cost for a particular policy: the preventive replacement cost C, the failure replacement cost $C+K$, and the false alarm cost F. For this study, we consider the estimates used in our previous research [22], [23], namely C=\$1,560 and $C+K$=\$6,780. In this chapter, the false alarm cost F is considered to be \$450. A comparison of the two maintenance policies (the currently used age-based policy and the Q_{DPCA} chart-based policy) is in Table 50.4.

From Table 50.4, the chart-based maintenance policy can avoid 7 out of 13 transmission failures. Considering the transmission oil changes that eliminate any cumulative increase in the control

Table 50.4. Comparison of maintenance policies using oil data histories

Policy	Age-based	Q_{DPCA} Chart-based
Sample size	36	36
Failures	13	6
Preventive replacements	23	30
Prev. repl.	63.89%	83.33%
Total false alarms	–	6
Total maintenance cost	\$124020	\$90180
Savings	–	\$33840
Savings %	–	27.29%

statistics, which makes it very difficult to indicate impending failures in condition monitoring, the fault detection capability of the Q_{DPCA} chart is excellent. On the other hand, the Q_{DPCA} chart gives only six false alarms. Thus the Q_{DPCA} chart based policy leads to significant cost savings, \$33840 or 27.29%.

50.3 CBM Cost Modeling and Failure Prevention

50.3.1 The Proportional Hazards Model and the CBM Software EXAKT

The CBM model presented in this chapter is the PH decision model considered by Makis and Jardine [2], controlled by the optimal replacement policy. It was proved in [2] that the average cost optimal policy is a control limit policy, *i.e.* the system is replaced (overhauled) when the value of the hazard function exceeds some optimal limit.

In the general PHM [28], the hazard rate is assumed to be the product of a baseline hazard rate $h_0(t)$, and a positive function $\psi(z,\gamma)$ representing

the effect of the operating environment on the system deterioration, where z is a covariate vector and γ is the vector of the unknown parameters.

In maintenance and reliability applications, some covariates are usually time-dependent stochastic processes and a dynamic PHM is more appropriate to describe the time-to-failure distribution. Thus, the hazard function for the dynamic PHM has the form: $h(t, z_t) = h_0(t, \omega)\psi(z_t, \gamma)$, where z_t is a covariate vector process and (ω, γ) is a vector of unknown parameters. In real applications, the system condition is usually monitored at regular sampling epochs and it is thus assumed that the values of $\{z_t\}$ are available only at these discrete sampling times. The system deterioration process is assumed to be continuous and the system can fail at any time. The covariate vector process $\{z_t\}$ is assumed to be a continuous time Markov process. Each replacement costs C and the failure replacement cost is C+K, C>0, K>0. The optimal policy minimizes the long-run expected average cost per unit time.

The condition-based maintenance (CBM) modeling is conducted by using the software called EXAKT, which was developed by the CBM lab at the Department of Mechanical and Industrial Engineering, University of Toronto.

EXAKT is a software package for CBM data pre-processing, PH modeling and maintenance decision-making. It utilizes recent oil or vibration data histories obtained from an equipment condition monitoring to build a Weibull PH model off-line, calculates the average cost optimal preventive replacement policy and then processes the data obtained from an on-line condition monitoring system to make optimal maintenance decisions.

The PH model in EXAKT uses the Weibull hazard function, which has the form:

$$h(t, Z(t)) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1} Exp(\gamma_1 z_1(t) + \gamma_2 z_2(t) + \cdots + \gamma_k z_k(t)) \tag{50.10}$$

where β and η are unknown shape and characteristic life parameters, respectively, and $\gamma = (\gamma_1, \gamma_2, \cdots, \gamma_k)'$ is the vector of unknown regression coefficients, $Z(t) = (z_1(t), z_2(t), \cdots, z_k(t))'$ is the vector of covariates assumed to be a multivariate non-homogeneous Markov process. The decision model in EXAKT calculates the average-cost optimal preventive replacement policy using the PH model fitted to recent data histories. It was proved in [2] that the structure of the optimal replacement policy is a control-limit policy, *i.e.*, a preventive replacement is recommended when the calculated value of the hazard function in (50.10) exceeds some optimal critical value.

50.3.2 Multivariate Time Series Modeling of the Oil Data

The oil data set used here is the same as what was used in the previous section. However, in this section, the modeling is not based on the healthy portion of the histories but using the whole data histories. Thus, we only discard the histories with the sampling interval far greater than 600 hours or much smaller than 600 hours in the multivariate time series modeling. There were two other data histories with only two records, which were too short for time series modeling and they were also discarded. Thus, our time series modeling is based on the 43 of the original 51 histories (totally 563 sampling records).

We have applied the least-square (LS) estimation method to calculate the model parameter estimates. The model order was determined by a test using likelihood ratio (LR) statistic. After fitting the VAR model, we also checked the model stationarity condition. The details of the LS estimation method, LR statistic and the stationarity condition check can be found in [24].

Based on the 43 of the selected oil data histories, we have the following modeling results. For m=2,3, the order test LR statistic M_2= 87.938, M_3=50.286. From the chi-squared distribution, with k^2=36 degrees of freedom and taking the significance level as 0.05, we find

$X^2_{36,0.05} = 50.998 = C$. Since $M_2 > C$ and $M_3 < C$, we reject H_0: $\Phi_{22} = 0$ and fail to reject H_0: $\Phi_{33} = 0$. Thus, we conclude that an AR(2) model is adequate for the oil data. Thus, the correlation relationship is represented by the covariance matrices $\Gamma(0), \Gamma(1)$ and $\Gamma(2)$. $\Gamma(0)$ is the cross-covariance matrix while $\Gamma(1)$ and $\Gamma(2)$ are the auto-covariance matrices of time lag one and two respectively. For the fitted AR(2) model $Y_t = \Phi_{12} Y_{t-1} + \Phi_{22} Y_{t-2} + \delta + \varepsilon_t$, the estimates of the parameters are as follows:

$$\hat{\delta}' = [0.6217,\ 2.3614,\ 0.8288,\ 5.9734,\ 0.5074,\ 0.3047]$$

$$\hat{\Phi}_{12} = \begin{bmatrix} 0.3946 & -0.5443 & 0.0175 & -0.3526 & -0.0060 & 0.1368 \\ -0.0000 & 0.6668 & 0.0052 & -0.1179 & 0.0044 & -0.0034 \\ 0.0285 & -0.2587 & 0.1776 & 7.1550 & -0.0733 & -0.0517 \\ 0.0020 & -0.0100 & 0.0007 & 0.2410 & -0.0008 & 0.0036 \\ -0.1571 & 0.6021 & -0.0498 & -5.0252 & 0.2169 & -0.1450 \\ 0.0040 & -0.0516 & 0.0041 & 0.9885 & -0.0206 & 0.0378 \end{bmatrix}$$

$$\hat{\Phi}_{22} = \begin{bmatrix} 0.1613 & 0.5135 & -0.0301 & 0.0774 & 0.0016 & -0.0357 \\ -0.0111 & 0.0617 & -0.0048 & 0.0479 & -0.0006 & 0.0049 \\ -0.0923 & 0.1459 & 0.2555 & -2.6052 & -0.0730 & -0.1901 \\ 0.0014 & 0.0132 & -0.0004 & 0.0742 & 0.0009 & 0.0051 \\ 0.0748 & 0.0051 & -0.0263 & 3.0802 & 0.2134 & 0.1781 \\ -0.0791 & -0.1721 & -0.0002 & -1.1693 & 0.0113 & -0.0601 \end{bmatrix}$$

$$\hat{\Sigma}_2 = \begin{bmatrix} 2.6322 & 1.4876 & 0.1178 & 0.4422 & 0.0237 & 0.1261 \\ 1.4876 & 78.4428 & 0.1926 & 3.5132 & 0.4981 & 1.8616 \\ 0.1178 & 0.1926 & 0.2697 & 0.9228 & 0.0901 & 0.1233 \\ 0.4422 & 3.5132 & 0.9228 & 715.5363 & 0.2702 & 3.2791 \\ 0.0237 & 0.4981 & 0.0901 & 0.2702 & 0.3806 & 0.1079 \\ 0.1261 & 1.8616 & 0.1233 & 3.2791 & 0.1079 & 2.7440 \end{bmatrix}$$

To check the stationarity condition for this fitted AR(2) model, we found that the eigenvalues of Φ_2 are (−0.4755, −0.3717, −0.2068 + 0.0647i, −0.2068 − 0.0647i, 0.0040 + 0.1866i, 0.0040 − 0.1866i, 0.0500, 0.7449, 0.6766, 0.6474, 0.3539, 0.5145), where Φ_2 is described as $\Phi_2 = \begin{bmatrix} \Phi_{12} & \Phi_{22} \\ I & 0 \end{bmatrix}$. Since the eigenvalues are all less than one in absolute value, the fitted AR(2) model is stationary.

50.3.3 Application of DPCA to the Oil Data

The readings of the six metal elements representing the oil data are both cross and auto-correlated. The correlation relationship among them is represented by the cross-covariance and the auto-covariance matrices. It follows from the analysis in the previous section that the correlation relationship can be represented by the covariance matrices $\Gamma(0), \Gamma(1)$ and $\Gamma(2)$. $\Gamma(0)$ is the cross-covariance matrix and $\Gamma(i)$ is the auto-covariance matrix of time lag $i, i = 1, 2$. These covariance matrices are used when applying DPCA to reduce the dimensionality of oil data. DPCA is an extension of the original PCA method applied to the matrix composed of the time-shifted data vectors (see, *e.g.*, [25] for an application of DPCA to a chemical process data analysis).

Following the DPCA procedures described in the previous section and using the new VAR modeling results in this section, we obtain the following DPCA results: the eigenvalues $\{l_i\}$ of the sample correlation matrix R in Table 50.5 and scree plot in Figure 50.4. The plot in Figure 50.4 clearly shows that there is a break (an elbow) between the first three and the remaining fifteen eigenvalues which form approximately a straight line. This indicates that we should retain the first three PCs for the subsequent CBM model building.

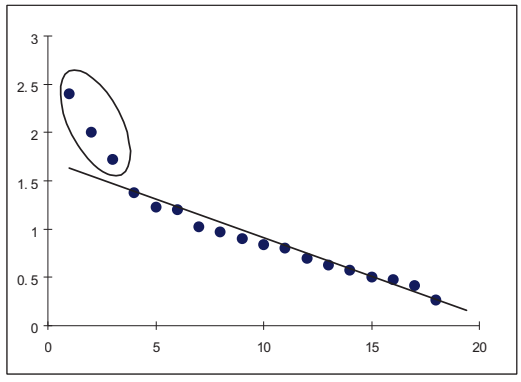


Figure 50.4. Scree test of DPCA for the oil data

Table 50.5. Successive eigenvalues l_i and eigenvalues diffenerce l_i-l_{i+1}

	***i*=1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
l_i	2.3964	1.9148	1.7196	1.3578	1.2133	1.1984	1.0107	0.966	0.8879
l_i–l_{i+1}	0.4816	0.1952	0.3618	0.1445	0.0149	0.1877	0.0447	0.0781	0.0571
	10	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
l_i	0.8308	0.7955	0.6972	0.6101	0.5691	0.5034	0.4804	0.4128	0.2578
l_i–l_{i+1}	0.0353	0.0983	0.0871	0.041	0.0657	0.023	0.0676	0.155	–

50.3.4 CBM Model Building Using DPCA Covariates

It follows from the analysis in the previous sub-sections that the three selected principal components calculated at each sampling epoch are uncorrelated, but since it is an AR(2) model, the resultant multivariate time series consisting of the three PCs at different time epochs is autocorrelated. To represent the covariate vector $Z(t)$ in (50.10) for PH modeling as a multivariate Markov process, we define

$$Z(t) = (pc1_t, pc2_t, pc3_t, pc1_{t-1}, pc2_{t-1}, pc3_{t-1}). \tag{50.11}$$

It follows from (50.5) that the portion of the U matrix needed for the calculation of the selected three PCs at each sampling epoch has the form $U = [u_1, u_2, u_3]$, where (u_1, u_2, u_3) are the eigenvectors corresponding to the first three largest eigenvalues of the sample correlation matrix R. For the oil data, the matrix U was calculated in the previous sub-section.

In EXAKT, in order to represent the covariate process as a discrete state Markov process, the covariate values are discretized and EXAKT provides routines for determining the covariate bands automatically. The covariate Markov process is generally assumed to be non-homogeneous. The length of the process histories is divided into several intervals and the process is assumed to be homogeneous within an interval, fully determined by the transition rates, which are estimated from the data together with the vector of the unknown PH model parameters. For the oil data considered in this chapter, two time intervals were suggested in [21], namely $[0, 2000)$ and $[2000, +\infty)$, and the covariate Markov process is assumed to be homogeneous in each interval.

The following three parameters are needed to calculate the average cost optimal replacement policy: the preventive replacement cost C, the failure replacement cost C+K, and the length of the interval between two subsequent samplings, Δ. For this study, we consider the estimates obtained in [21], namely C=\$1,560, C+K=\$6,780, and $\Delta = 600$ hours. After estimating the PH model parameters and the transition rates for the covariate Markov process, EXAKT builds a PH model by testing two kinds of hypotheses. The first null hypothesis states that the shape parameter β in the hazard function given by (50.10) is equal to one, *i.e.*, the baseline hazard function is a constant, indicating that the time effect is not significant and an exponential baseline hazard function is appropriate. The second set of hypotheses tests the significance of the individual covariates, *i.e.*, if the null hypothesis $H_0^i : \gamma_i = 0$ is rejected, the *i*th covariate $Z_i(t)$ is retained in the model. The summary of the PH model building using EXAKT is in Table 50.6.

From the results of the analysis, as presented in Table 50.6, only $PC1_t$, $PC1_{t-1}$ and $PC2_t$ are significant covariates to be retained in the model. Also, the estimate of the shape parameter β equal to 1.723 is considerably different from the hypothesized value of one, indicating that the time effect is significant and the exponential baseline model is not appropriate. A comparison of the

Table 50.6. The results of the PH model building using EXAKT

Parameter	Estimate	Significant	Standard Error	P-value
Scale (η)	1.755e+004	–	3564	–
Shape (β)	1.723	Y	0.3326	0.02982
pc1 (γ_1)	−1.12	Y	0.2519	0
pc1_1 (γ_2)	0.9909	Y	0.2584	0.0001253
Pc2 (γ_3)	0.545	Y	0.2526	0.03093

Table 50.7. Policy comparison

	Cost [$/hr]	Prev. repl. Cost [$/hr]	Failure repl. cost [$/hr]	Prev. repl. [%]	Failure repl. [%]
DPCA PHM optimal policy	0.258752	0.121589 (47.0%)	0.137162 (53.0%)	79.4	20.6
Failure replacement only	0.474628	0 (0.0%)	0.474628 (100%)	0	100
Savings	0.215876 (45.5%)	-0.121589	0.337466	−79.4	79.4

optimal maintenance policy for the fitted PH model summarized in Table 50.6, and the policy which replaces only upon failure is in Table 50.7. From Table 50.7, 79.4% of the replacements are preventive replacements and only 20.6% are failure replacements, *i.e.*, a substantial portion of failure is avoided by preventive maintenance actions. Also, the average cost per hour is substantially reduced by applying the optimal policy, resulting in the savings of 45.5% when compared with the average cost associated with the failure replacement policy.

50.3.5 Failure Prevention Performance and the Maintenance Cost Comparison

Next, we will check the failure prevention performance of the CBM model using DPCA covariates by applying the optimal policy to the oil data histories. The results will also be compared with the current maintenance policy of the company, which is a simple age-based replacement policy, *i.e.*, a transmission is replaced after 12,000 working hours, or upon failure, whichever occurs first. The results are summarized in Table 50.8.

From the results in Table 50.8, we can again conclude that when applied to the 48 real data histories (18 ended with failure and 30 ended with suspension), the optimal policy for the DPCA PHM gives the lower average cost (0.349 *vs*, 0.432), smaller number of failures, and the higher percentage of preventive replacements, compared to the simple age-based policy. Since only 8 out of the 18 failures occurred when applying the DPCA PHM optimal policy, it is clear that the optimal policy correctly suggested 10 preventive replacements before the machine failure. Thus, in the 21 “replaced” histories of the PHM policy, there are 10 cases for which impending failures were avoided and in the other 11 cases preventive replacement decision was suggested before suspension. The remaining 19 histories ended with suspension when applying the age-based policy, but the optimal DPCA PHM policy suggested that these transmissions should continue operating and the suspension was possibly performed too early.

Table 50.8. Policy comparison using real data histories

Policy	Current age-based	DPCA PHM
Sample size	48	48
Failed	18	8
Replaced	30	21
Undecided	0	19
Cost per unit time	0.432	0.349
Prev. repl.	62.50%	83.33%

These 19 cases are marked as "undecided" in Table 50.8. When we compute the average cost and preventive replacement percentage, these 19 "undecided" histories are treated as suspensions followed by a preventive replacement.

For further failure prevention performance check, we applied the optimal policy for the DPCA PHM model to all the 20 data histories that ended with failure out of the whole 51 histories considered. As shown in Table 50.9, the optimal policy using DPCA PHM recommends 8 preventive replacements to be made at a sampling time before the actual failure occurred. If the decision is not to replace immediately, the software calculates the expected replacement time. For the three histories (ID 69-2, ID 77-2 and ID 79-2), the policy recommended replacements 30 hours after taking the sample. Since 30 hours is a very short time compared to the roughly 600 hours sampling interval, the transmissions will be replaced immediately before the actual failure occurs. To summarize, the policy which uses the DPCA PHM recommends ten preventive replacements for 20

Table 50.9. Replacement recommendation for failure histories using DPCA PHM

ID	Failure time [h]	Last Sampling time [h]	Recommend replace (Y or N)?	Expected to replace in [h]
66-1	10524	10320	**Y**	***0***
67-1	7532	7378	**Y**	**0**
68-2	6134	5947	**Y**	**0**
68-3	5556	5062	N	2235.93
68-4	4428	3987	N	4888.98
68-5	1311	725	**Y**	**0**
69-2	9598	9598	***N***	**30**
71-1	4986	4982	**Y**	**0**
71-2	5577	5329	**Y**	**0**
71-3	3154	3009	N	873.59
72-2	8043	7863	N	5490.09
73-1	7788	7457	N	2046.46
74-2	5013	4595	N	3569.74
76-1	1660	1276	**Y**	**0**
76-3	3124	2901	N	3981.39
76-4	2357	2082	N	3118.7
77-1	4274	4052	**Y**	**0**
77-2	2672	2278	**N**	**30**
79-1	9468	9055	N	4013.77

histories which ended with failure. Compared with the current policy used by the company, the policy which uses the DPCA PHM can avoid 50% of failures.

50.4 Conclusions

In this chapter, we have applied the multivariate time series modeling and DPCA to the transmission oil data. The models have been used for maintenance decision-making using a DPCA-based Q chart and the optimal policy for a DPCA PHM-based CBM model. The effectiveness of both methodologies was demonstrated by evaluating the fault detection capability and cost benefit when compared with the currently used age-based maintenance policy.

First, we presented the methodology which uses the DPCA-based Q chart for maintenance decision-making and used the real truck transmission oil data for testing its performance. Since the transmission oil data exhibits both cross and auto-correlation, the PCA-based (T_A^2, Q) charts cannot be used and we considered the DPCA-based (T_A^2, Q) charts. After applying the DPCA transformation, serial correlation still exists in the PC scores, which considerably reduces the effectiveness of the DPCA-based T_A^2 chart. On the other hand, for the DPCA-based Q chart, no such autocorrelation effect exists. It has been demonstrated that the fault detection ability of the Q_{DPCA} chart is excellent and the application of the Q_{DPCA} chart-based policy resulted in a significant maintenance cost savings compared with the currently used age-based policy.

Next, based on the results of the multivariate time series modeling of transmission oil data and subsequent dimensionality reduction using DPCA, we have built a proportional hazards-based CBM model using the significant three PCs as the covariates. The theoretical results showed that the optimal policy for the CBM model leads to considerable maintenance cost savings compared to the "replace only upon failure" policy. When applied to the oil data histories, the CBM model based policy resulted in a significant cost reduction compared to the current age-based policy.

From the two case studies presented in this chapter and summarized above, we have demonstrated effectiveness of the multivariate time series modeling and DPCA applied to CM data and used for an on-line maintenance decision-making.

References

[1] Lin D, Banjevic D, Jardine AKS. Using principal components in a proportional hazards model with applications in condition-based maintenance. Journal of the Operational Research Society 2006; 57:910–919.

[2] Makis V, Jardine AKS. Optimal replacement in proportional hazard model. INFOR 1992; 30(1):172–183.

[3] Lu CJ, Meeker WQ. Using degradation measures to estimate a time-to-failure distribution. Technometrics 1993; 35(2):161–174.

[4] Aven T. Condition-based replacement policies – A counting process approach. Reliability Engineering and System Safety 1996; 51:275–281.

[5] Christer AH, Wang W, Sharp JM. Case study a state space condition monitoring model for furnace erosion prediction and replacement. European Journal of Operational Research 1997; 101(1):1–14.

[6] Makis V, Jiang X, Jardine AKS. A condition-based maintenance model. IMA Journal of Mathematics Applied in Business and Industrial 1998; 9:201–210.

[7] Makis V, Jiang X. Optimal replacement under partial observations. Mathematics of Operations Research 2003; 28(2):382–294.

[8] MacGregor JF, Kourti T. Statistical process control of multivariate processes. Control Engineering Practice 1995; 3:403–414.

[9] Duffuaa SO, Ben-Daya M. Improving maintenance quality using SPC tools. Journal of Quality and Maintenance Engineering 1995; l.01:25.

[10] Cassady CR, Bowden RO, Liew L, Pohl EA. Combining preventive maintenance and statistical process control: a preliminary investigation. IIE Transactions 2000; 32: 471–478.

[11] Ivy JS, Nembhard HB. A modeling approach to maintenance decisions using statistical quality control and optimization. Quality and Reliability Engineering International 2005; 2:355–366.

[12] Linderman K, Mckone-Sweet KE, Anderson JC. An integrated systems approach to process control and maintenance. European Journal of Operational Research 2005; 164:324–340.
[13] Jackson JE, Mudholkar GS. Control procedures for residuals associated with principle component analysis. Technometrics 1979; 2:341–349.
[14] Makis V, Jardine AKS. Computation of optimal policies in replacement models. IMA Journal of Mathematics Applied in Business and Industry 1992; 3:69–175.
[15] Hotelling H. Multivariate quality control. In: Eisenhart C, Hastay MW, Wallis WA, editors. Techniques of statistical analysis. McGraw-Hill: New York, 1947.
[16] Dillon WR, Goldstein M. Multivariate analysis methods and applications. Wiley, New York, 1984; 23–52.
[17] Kourti T, MacGregor JF. Multivariate SPC methods for process and product monitoring. Journal of Quality Technology 1996; 28:409–428.
[18] Jackson JE. A user's guide to principle components analysis. Wiley, New York, 1991.
[19] Nomikos P, MacGregor JF. Multivariate SPC charts for monitoring batch process. Technometrics 1995; 37:41–59.
[20] Chiang LH, Russell EL, Braatz RD. Fault detection and diagnosis in industrial systems. Springer, London, 2001.
[21] Banjevic D. Case study: CBM model and optimal policy for 240-Ton haul truck transmissions obtained from Syncrude data. Research Report. Department of Mechanical and Industrial Engineering, University of Toronto, Toronto, 1999.
[22] Makis V, Wu J, Gao Y. An application of DPCA to oil data for CBM modeling. European Journal of Operational Research 2006; 174(1):112–123.
[23] Wu J, Makis V. A CBM model based on VAR modeling of oil data and SPE. The 2005 IIE Annual Conference Proceeding, Atlanta, Georgia 2005; May 14–18.
[24] Reinsel GC. Elements of multivariate time series analysis. Springer, New York, 1997.
[25] Ku W, Storer RH, Georgakis C. Disturbance detection and isolation by dynamic principal component analysis. Chemometrics and Intelligent Laboratory Systems 1995; 30(1):179–196.
[26] Jolliffe IT. Principal component analysis. Springer-, New York, 1984.
[27] Cattell RB. The SCREE test for the number of factors. Journal of Multivariate Behavior Research 1996; 1:245–276.
[28] Cox DR. Regression models and life tables (with discussion). Journal of Royal Statistics Society 1972; B34:187–220.

51

Sustainability: Motivation and Pathways for Implementation

Krishna B. Misra

RAMS Consultants, Jaipur, India

Abstract: Sustainability is a characteristic of a process or state that can be maintained at a certain level indefinitely. Sustainability focuses on providing the best outcomes for both human and natural environments now, and indefinitely into the future. In recent years, academic interest and public discussion has led to the use of the word sustainability in reference to how long human ecological systems can be expected to be usefully productive. This chapter first examines the threats and then provides how the environmental threats can be assessed and mitigated.

51.1 Introduction

There is no industrial activity that is entirely free from risks and it is not possible to eliminate every eventuality of mishap by safety precautions. However, when risks are high, system designers must consider the possibilities of additional preventive or protective measures to reduce the risk, and judge whether it would be worthwhile to implement these additional measures, particularly when consequences affect the environment. The industrial accidents that have "*environmental consequences*" for man in some way or the other and are transmitted through the air, water, soil or biological food chains, are known as *environmental risks*. Their causes and characteristics, however, can be very diverse. Some are created by man through the introduction of new technology; product or chemicals while others, such as natural hazards, result from natural processes, which happen to interact with human activities and settlements. Some of these, such as pollution from a smelter, can be anticipated, others, such as the possible effects on the Earth's ozone layer of fluorocarbon sprays or nitrogen fertilizers, have wholly unsuspected effects at the time the technologies or activities were developed.

With chemical industries [8], there is always the risk of toxic substances, fluids or gases getting released to the surrounding environment due to and accident. Therefore it is necessary to assess the risks in all such cases where environmental consequences are possible incase of any mishap. Moreover, there are other sources of environmental degradation due to their even normal operation such as in mining industry where landspoils occur in abundance or in the case of vehicular exhaust where air gets polluted constantly. In such cases, environmental impact assessment [3] should be carried out to plan preventive measures for the public.

In addition to having a common feature of being transmitted through environmental media, environmental risks can cause harm to people who have voluntarily or specifically not chosen to suffer their consequences; therefore they require control or

management. Environmental risk management involves the search for a "*best route*" between social benefit and environmental risks. It is actually a trade-off between various combinations of risks and social and economic gain that usually decides the acceptability of a technological development or a system.

51.2 Environmental Risk Assessment

Environmental risk assessment has acquired importance and emphasis over the past few decades after the public experienced several industrial and nuclear accidents and realized that the actions of humans can have adversely affect the environment. It was due to this realization that the once widely-used pesticide DDT was banned when it was found to have negative effects on the environment (including humans). The 1970s saw the passing of environmental protection legislation such as the Clean Water Act, the Clean Air Act and the Superfund environmental cleanup regulations (the Comprehensive Environmental Response, Compensation and Liability Act). All these legislations required risk assessments.

Two types of approaches are applied to environmental risk assessment, *viz.*, *predictive* and *retrospective*. Predictive assessments deal with proposed actions, such as the introduction of new chemicals, new sources of environmental releases, or possible accidents.

In general, the predictive approach follows a four-step paradigm, *viz.*, *hazard identification, dose-response assessment, exposure assessment,* and *risk characterization*. Hazard identification includes selecting the endpoints, describing the environment under consideration, and determining the pollutant sources. Dose-response assessment replaces effects assessment, which includes the use of models to project the effects of stresses on selected endpoints. Exposure assessment and risk characterization follow.

51.2.1 Hazard Identification

This is the recognition that a hazard with definable characteristic exists. It is a step to ascertain if there is the potential for an exposure of an organism (including a human) or ecosystem [4] to an environmental stressor; the identification of what is at risk. Hazard identification involves the use of exposure and effects data from the laboratory and the field to determine whether the agent of concern can cause a particular adverse health effect. The breadth and complexity of most ecological systems may initially require considerable effort to define the scope of the problem, including identifying the stresses involved (whether chemical or non-chemical), the type of ecosystem(s) involved (aquatic, terrestrial, wetlands, *etc*.), and spatial and temporal scaling factors.

The identification of what is at risk, also referred to as endpoint (or receptor) selection, is critical to the environmental risk assessment process. Ecological endpoints can be chosen at any of several organizational levels, from biochemical and cellular level through individuals, populations, communities, and ecosystems. Endpoint selection is dependent upon both the ecosystem and stresses of concern. Thus, it is important to define these endpoints at the beginning of an environmental risk assessment.

51.2.2 Dose-response Assessment

Dose-response assessment characterizes the relationship between administered dose to a receptor (organism or ecosystem), and the incidence of an adverse effect on that receptor. In human health risk assessment, when administered doses are plotted against the measured responses, extrapolation methods are typically used to estimate the response at low doses. *Stress-response* may be a better term than *dose-response* when dealing with environmental risk assessment, since ecosystems can be adversely affected by many different types of anthropogenic stresses, not only toxic chemicals. A stress response assessment can be conducted once the appropriate assessment and measurement endpoints have been selected. Data used can vary widely depending upon the test protocol; whether the experimental design includes structure-activity relationship analysis, laboratory tests with single species, laboratory microcosms, or full-scale field tests.

51.2.3 Exposure Assessment

An exposure assessment is done to measure or estimate the magnitude, frequency, and duration of exposure, and to characterize the human populations that are subject to exposure. In an ecological context, exposure more frequently refers to the concentration or magnitude of a contaminant or stress in the environment currently or may be present in the future. Characterization of the exposed population is particularly problematic in ecological risk assessments. While demographics and activity patterns are frequently available for human populations, ecological risk assessment generally deals with a diverse group of species, about which relatively little is known. There is also a tremendous diversity of habitats, ranging from aquatic environments (sediment, freshwater, and marine) to wetland and terrestrial environments.

Ecological exposure assessments are generally based on the frequency and duration of inputs of a chemical, its fate and transport in the environment, and any chemical transformations. One can integrate the probabilistic properties of pollutant release into transports and fate models that would give estimates of the concentrations and persistence of the pollutant in different environmental media (soil, water, *etc*.).

The ability of ecosystem to recover from stress is another important factor that must be considered. The ultimate effects of stress on an ecosystem depend not only upon the strength and duration of the initial stress, but also the ecosystem's ability to regenerate.

51.2.4 Risk Characterization

In characterizing risk, one estimates the incidence of adverse human health effect under conditions stated in the exposure assessment. In an environmental risk assessment, the probabilities of adverse effects at estimated exposure levels are not usually determined.

Retrospective risk assessment: In addition to predicting the potential effects of proposed actions, one is frequently faced with the problem of determining whether adverse ecological effects have occurred as a result of previous actions, through a *retrospective risk assessment*. For example, a retrospective risk assessment can be used at an abandoned hazardous waste site to determine whether ecological impacts have occurred. On the other hand, in retrospective assessments both the sources of pollution and the polluted environment may be observed directly. The purpose of a retrospective study is to define the relationship between pollution source, ecosystem exposure, and ecosystem effects.

Each of the steps mentioned in the foregoing sections requires the collection of data (such as the collection of lead concentrations in soil or water) and/or the use of mathematical models (such as ones that describe the movement of contaminants in the environment or define the cancer incidence from exposure to levels of uranium). Risk assessments have now become part of the analysis that a proposed new chemical or other product must undergo before it may be placed on the market.

As is obvious, the successful environmental risk assessment will require the experts from several disciplines, *viz.,* chemistry, physics, biology, ecology, geology, hydrology and engineering. Because of their skills in analyzing data and computations including risk and handling uncertainties, statisticians will play a key role in each one of the above steps. Data or modeling uncertainty in any one of the steps may have a significant effect on the results and meaning of the assessment.

51.3 Ecological Risk Assessment

Ecological risk from chemicals is much more difficult to assess than the estimation of risks to humans. In the first place, we are dealing with only one kind of living creature, humans, while in ecological risk assessment, we must consider the whole range of organisms that exists in nature from the very small to the very large; all those which live in water or in the air or on the ground; and those which have very long or very short life spans. These organisms vary not only in size and life span but also in sensitivity to particular chemicals and to how these chemicals are broken down after being absorbed into the organism.

The goal of ecological risk assessment [4] is not as clearly defined. While some scientists suggest that the focus should be on the individual organism, others think that the focus should be on the survival of the population of animals rather than any single organism. Still others have another view that the larger body of ecosystem, such as a lake or river, should be protected.

Therefore, there is no standard procedure for assessing overall ecological risk. There are intense efforts currently underway to improve upon this situation, but it will undoubtedly take some time before such procedures are standardized and are applicable to all contaminants and sites of interest. However, a large number of studies have been done on the adverse effects that specific chemicals can have on the environment. In addition, there are many studies that have investigated other adverse effects, especially changes in reproductive capacity. Besides the research on PCBs and terrestrial organisms, other investigations have shown a relationship between reproduction and tributyltin, a pesticide often added to marine paints. Other work relating fish tumors to contaminants is not as well advanced, and many tumors have been shown to be caused by naturally occurring viruses. A number of these effects, especially death and decreased reproductive capacity, have impacts on populations as well as individuals and also have the potential to affect ecosystem health.

While these studies provide a great deal of important information, there are a variety of uncertainties associated with the results. When the studies are done in the field one significant source of uncertainty is determining the degree of exposure of the animal to various agents, both chemical and physical, as it moves from place to place and as the environment around it changes. This can be especially problematical when dealing with animals that migrate and so face radically different environments at different times of the year.

To best manage the environment, it is necessary to assess the extent of current and future risks to the biota of the environment and to characterize the causative agents. Increased understanding by public is critical to the development and implementation of policies that are responsive to the concerns of the people inhabiting the ecosystem.

51.4 Sustainability

We have seen in Chapter 1, how in our effort to make the Earth to yield more for the increasing human population through industrialization, we degraded the environment of the planet that we live on and our future generations have to survive on. Unless some urgent drastic steps are taken to contain further deterioration and to maintain *status quo*, if not to regenerate the spoiled environment, the situation is likely to get out of control, and we may be leading our planet towards the doomsday. Ever-increasing deforestation, large scale mining, depletion of mineral resources and fossil fuel reserves, green house gases, ozone layer depletion, waste dumps including radio-active waste, air pollution due to vehicular exhaust, acidification, pollution of water bodies (lakes, rivers, sea, *etc.*), noise, and energy losses are all leading to increase our woes and disrupt the delicate ecological balance that existed on Earth to sustain life on this planet. Thoughtless planning, execution and use have also added to ecological problems. Thus the only pathway that is feasible and practicable seems to lie in the strategy of pollution prevention of all kinds and in sustainable development. Unless all our industrial activities conform [32] to sustainability principles and all products, systems, and services are redesigned to be sustainable, we cannot possibly stop the march to doomsday and future generations will hold the present generation responsible for this lapse if we do not act while there is still time.

The United Nations has taken an initiative in this direction by declaring a *Decade of Education for Sustainable Development* that started in January of 2005. In the US also a non-partisan multi-sector group called the *U.S. Partnership for the Decade of Education for Sustainable Development* has been constituted. Any organization and individuals or groups of youth, business, religion, *etc.*, can join and share resources and success stories for creating a sustainable future.

However, there are lots of impediments in the way of achieving an environmentally sustainable future. A new sustainability paradigm is possible, if all progressive elements of civil society, governments, and businesses, share the information and work together to create an alternative vision of globalization centered on the quality of life, human solidarity, and environmental resilience. The Tellus Institute [26, 34] has brought out some useful publications like "Great Transition" to examine these aspects.

51.4.1 Definition

The simplest definition of sustainability that can be given is: It is a characteristic of a process or state that can be maintained at a certain level indefinitely. The oft-cited definition of sustainability is the one given by the Brundtland Commission [5], which defined *sustainable development* as development that "meets the needs of the present without compromising the ability of future generations to meet their own needs". Sustainability can be defined as: "Humanity's investment in a system of living, projected to be viable on an ongoing basis that provides quality of life for all individuals of sentient species and conserves natural ecosystems".

Sustainability focuses on providing the best outcomes for both the human and natural environments now, and into the indefinite future. In recent years an academic and public discourse has led to the use of the word sustainability in reference to how long human ecological systems can be expected to be usefully productive.

Sustainability relates to the continuity of economic, social, institutional and environmental aspects of human society, as well as the non-human environment. Sustainability is one of the four Core Concepts behind the 2007 Universal Forum of Cultures. Sustainability can be defined both qualitatively in words, as an ethical/ecological proposition such as the Brundtland definition above, and quantitatively in terms of system life expectancy and the trajectory of certain factors or terms in the system. Quantitative analysis in sustainability thinking typically uses system dynamics modeling, as systems are often non-linear and so-called feedback loops are key factors. So, for instance, important human ecological sub-systems that could be analyzed or modeled in this way might include the nitrogen cycle in sustainable agriculture, or the depletion of oil reserves.

In order to distinguish quantitatively and qualitatively which human economic activities are destructive and which are benign or beneficial, various definitions/models of sustainability have been developed. The following list is not exhaustive but contains the major points of view:
In 1996, the International Institute for Sustainable Development, Canada, proposed a *Sample Policy Framework,* according to which a sustainability index need to be developed to provide decision-makers tools to compare various alternative policies and programs and to establish measurable entities or metrics that can be used to assess progress towards sustainability. Accordingly, there have been several efforts [23, 24, 30, 35] in that direction.

51.4.2 The Social Dimension to Sustainability

It may be worthwhile to mention that values vary considerably within and between cultures, as well as between economists and ecologists [6]. The introduction of social values to sustainability goals is a much more complex aspect and the non-ecological interpretations are strongly opposed by those focused on the side of ecological impacts. However, one may like to interpret sustainability in the light of value set which gives "parallel care and respect for the ecosystem and for the people within the ecosystem". From this value set emerges the social goal of sustainability*, i.e.,* to achieve the well-being of human and ecosystem, together. In this context, the concept of sustainability becomes much wider than just a means for environmental protection. It is a positive concept that has as much to do with achieving well-being of people and of ecosystems by reducing ecological stresses or environmental impacts.

At its least, sustainability implies paying attention to comprehensive outcomes of events and actions insofar as they can be anticipated at present. This is known as *full cost accounting*, or *environmental accounting*. This kind of accounting

assumes that all aspects of a system can be measured and audited (*environmental audits*).

Environmental accounting can have a limited biological interpretation as in ecological footprint analysis, or may include social factors as in the case of urban and community accounts.

At most, sustainability is intended as a means of configuring civilization and human activity so that society, its members, and its economies are able to meet their needs and realize their greatest potential in the present, while preserving biodiversity and natural ecosystems, and planning and acting for the ability to maintain these ideals over a very long period – typically, at least seven generations.

However, no one has ever underestimated the importance of the ecological interpretation of sustainability. All advocates of sustainability accept that ecological, not social factors, can be effectively measured and are universal indicators of sustainability. Sustainability outcomes can be investigated at every level of organization, from the local neighborhood to the entire planet.

51.4.3 Sustainability Assessment

Sustainability requires an integrated view of the world, in which close links between environment, economy, and society exist. The natural resources provide the raw materials for production on which jobs and stockholder profits depend. Jobs affect the poverty rate and the poverty rate affects crime. Air quality, water quality, and materials used for production have an effect on health and on stockholder profits: if a process requires clean water as an input, cleaning up poor quality water prior to processing is an extra expense, which reduces profits. Likewise, health is related to general air quality or exposure to toxic materials, and will have an effect on worker productivity and contribute to the rising costs of health insurance. Therefore, sustainability requires multidimensional indicators that show the links between a community's economy, environment, and society. Ness *et al* [36] discuss in detail the assessment tools for sustainability which may be based on indicators, or product related assessment or integrated assessment. The first set of sustainability assessment tools consists of indicators and indices. Indicators are simple measures representing quantitatively a state of economic, social and/or environmental development in a specified region-often the national level. If indicators are aggregated in some manner, the resulting measure is called an index. Indicators and indices, which are continuously measured and calculated, allow for the tracking of longer-term sustainability trends from a retrospective point of view. Understanding these trends allows us to make short-term projections and relevant decisions for the future. The tools in the category of indicators and indices are either *non-integrated*, meaning they do not integrate nature–society parameters, or *integrated*, meaning the tools aggregate the different dimensions. There is also a subcategory of non-integrated tools that focuses specifically on regional flow indicators. An example of non-integrated indicators is environmental pressure indicators (EPIs), developed by the Statistical Office of the European Communities (Eurostat). EPIs consist of 60 indicators, six in each of the ten policy areas under the Fifth Environmental Action Program. Another example is the set of 58 national indicators used by the United Nations Commission on Sustainable Development (UNCSD). These indicators are not integrated or aggregated in any manner. UNCSD indicators include water quality levels for the environmental category, national education levels, and population growth rates as social determinants, GNP per capita for the economic sphere, and the number of ratified global agreements in the category of institutional sustainability. Recently, considerable attention has been paid to *composite* indicators. Chapter 54 in this handbook deals with this aspect.

51.4.4 Metrics of Sustainability

Just as we have indicators in every field to show how well a particular system is working, we also have indicators for sustainability. Indicators are as varied as the types of systems they monitor. Very many indicators have been suggested by organizations and experts. However, there are certain characteristics that effective indicators must have in common. An effective indicator should be based on accessible data so that checks are possible

and should be relevant, easy to understand, and reliable.

Based on Brundtland's definition of sustainability [5], Robèrt [25] described the conditions of sustainability in the *natural step framework* that a sustainable society is one which does not systematically increase concentrations of substances extracted from the Earth's crust, or substances produced by society, does not degrade the environment, and in which people have the capacity to meet their needs worldwide.

Another composite measure of sustainability is through life cycle assessment. It analyses the environmental performance of products and services through all phases of their life cycle; extracting and processing raw materials, manufacturing, transportation and distribution; use, re-use, maintenance; recycling, and final disposal.

Yet another way to look at the sustainability index is through ecological footprint analysis, which is the estimate of the amount of land area a human population, based on existing technology, would need if the current resource consumption and pollution by the population were matched by the sustainable (renewable) resource production and waste assimilation by such a land area. Zhao *et al.* [31] developed algorithms based on ecological footprint model in combination with the emergy methodology and a sustainability index has been derived from the latter. They have also been combined with an index of quality of life (Marks *et al.* [33]), and an index called the *(Un)Happy Planet Index* (HPI) was derived for 178 nations.

Very often a country's economic power and success is judged by the *gross domestic product* (GDP) and is an indicator of prosperity, as it is defined as the total value of a country's annual output of goods and services. However, it is obvious that the welfare of a nation can hardly be judged from the national income. For example, GDP reflects only the amount of economic activity, regardless of the effect of that activity on the community's social and environmental health, it is possible for GDP to go up when overall community health actually goes down. A comparable sustainability indicator is the Index of Sustainable Economic Welfare, which subtracts from the GDP corrections for harmful bases or consequences of economic activity and adds to the GDP corrections for significant activities such as unpaid domestic labor in order to get a more complete picture of the economic progress. For instance, the ISEW accounts for air pollution by estimating the cost of damage per ton of five key air pollutants. It accounts for depletion of resources by estimating the cost to replace a barrel of oil equivalent with the same amount of energy from a renewable source. It estimates the cost of climate change due to greenhouse gas emissions per ton of emissions. The cost of ozone depletion is also calculated per ton of ozone depleting substance produced. Additionally, adjustments are made to reflect concern about unequal income distribution. The correction for unpaid domestic labor is based on the average domestic pay rate. Some health expenses are considered as not contributing to welfare, as well as some education expenses.

The Living Planet Report 2002 by WWF shows that humans are currently using over 20% more natural resources each year than can be regenerated and this deficit is growing each year. Projections based on likely scenarios of population growth, economic development and technological change, indicate that by 2050, humans will consume between 180% and 220% of the Earth's biological capacity, which means that unless governments take urgent action, by 2030, human welfare, as measured by average life expectancy, educational level, and world economic product will go into decline.

Another indicator of sustainability is the *Living Planet Index,* which actually indicates the state of Earth's biodiversity. It tracks populations of 1,313 vertebrate species (fish, amphibians, reptiles, birds, mammals) from all around the world. Separate indices are produced for terrestrial, marine, and freshwater species, and the three trends are then averaged to create an aggregated index. Although vertebrates represent only a fraction of known species, it is assumed that trends in their populations are typical of biodiversity overall. By tracking wild species, the Living Planet Index is also monitoring the health of ecosystems. Between 1970 and 2003, the index fell by about 30%. This global trend suggests that we are degrading natural

ecosystems at a rate unprecedented in human history.

Several other indicators of development to GDP exist such as UN's *Human Development Index* (HDI), but this also fails to assess the success at achieving the ultimate aim of people's happiness in terms of health and happiness for themselves and their families. It is important that the resources provided by our planet also be available to future generations. HPI estimates the ecological efficiency with which nations ensure happy and long lives for their people. The wealthiest nations according to this index are grossly inefficient and no nation scores well on all counts. In actual fact,, HPI involves three distinct indicators, *viz.,* ecological foot prints, self-reported life satisfaction, and life expectancy. It is defined as:

$$HPI = \frac{LifeSatisfaction \times LifeExpectancy}{EcologicalFootprint}$$

Thus HPI is a measure of the ecological efficiency of delivering human well-being. It indicates the average years of happy life produced by a given society or nation per unit of planetary resources consumed. The startling conclusion from ecological footprint analyses was that it would be necessary to have four or five back up planets exclusively engaged in agriculture to sustain the current population to maintain a Western lifestyle.

In 1997, Brown and Ulgiati [17, 20] defined a new sustainability index (SI) called *emergy sustainability index* (ESI) as a ratio of the emergy (embodied energy) yield ratio (EYR) to the environmental loading ratio (ELR). This index accounts for yield, renewability, and environmental load. It is the incremental emergy yield compared to the environmental load.

$$SustainableIndex = \frac{EmergyYieldRatio\,(EYR)}{EnvironmentalLoadingRatio\,(ELR)}$$

It may be noted here that the numerator is not *energy yield ratio*, but *emergy yield ratio*, which is a different concept. This method of valuation, called emergy accounting [15, 19, 23] uses the thermodynamic basis of all forms of energy and materials, but converts them into equivalents of one form of energy, usually sunlight. Emergy accounting is a technique of quantitative analysis, which determines the values of non-monied and monied resources, services, and commodities in common units of the solar energy that it took to make them. The units of emergy are emjoules, to distinguish them from joules. Most often emergy of fuels, materials, services, *etc*., is expressed in solar emjoules (abbreviated *sej*). Emergy then, is a measure of the global processes required to produce something expressed in units of the same energy form. To derive solar emergy of a resource or commodity, it is necessary to trace back through all the resources and energy that are used to produce it and express each in the amount of solar energy that went into their production

51.4.5 The Economics of Sustainability

The World Business Council for Sustainable Development was founded in 1995. It came about through the merging of the Business Council for Sustainable Development and the World Industry Council for the Environment and is based in Geneva, Switzerland, has a North American Office in Washington DC, and has the membership of leading companies like DuPont, General Motors, 3M, Deutsche Bank, Coca-Cola, Sony, Oracle, BP, *etc*.). The World Business Council for Sustainable Development has advocated a business case for sustainable development and advises companies that "sustainable development is good for business and business is good for sustainable development". This view is also shared by proponents of industrial ecology. The theory of industrial ecology suggests that industry should be viewed as a series of interlocking man-made ecosystems interfacing with the natural global ecosystem.

According to some economists [7], it is possible for the concepts of sustainable development and competitiveness to merge if enacted wisely, so that there is no inevitable trade-off. This merger is motivated by the following facts put forward by Hargroves and Smith [28]:

1. Throughout the economy there are widespread untapped potential resource productivity improvements to be made to be coupled with effective design.

2. There has been a significant shift in understanding over what creates the lasting competitiveness of a firm.
3. There is now a critical mass of enabling technologies in eco-innovations that make integrated approaches to sustainable development economically viable.
4. Since many of the costs of what economists call "environmental externalities" are passed on to governments, in the long-term sustainable development strategies can provide multiple benefits to the tax payer.
5. There is a growing understanding of the multiple benefits of valuing social and natural capital, for both moral and economic reasons, and these are being included now in measures of national well-being.
6. There is mounting evidence to show that a transition to a sustainable economy, if done wisely, may not harm economic growth significantly; in fact it could even help it.

However, according to The *Stern Review on the Economics of Climate Change*, which is a 700-page report released on October 30, 2006 by economist Nicholas Stern for the British government, discusses the effect of climate change and global warming on the world economy. This is the most widely known and discussed report of its kind. Its main conclusions are that 1% of the global gross domestic product (GDP) *per annum* is required to be invested in order to avoid the worst effects of climate change, and that failure to do so could risk global GDP being up to 20% lower than it might otherwise be. Stern's report suggests that climate change threatens to be the greatest market failure ever seen, and it suggests prescriptions including environmental taxes to minimize the economic and social disruptions. Stern states that "our actions over the coming few decades could create risks of major disruption to economic and social activity, later in this century and in the next, on a scale similar to those associated with the great wars and the economic depression of the first half of the 20th century".

The debate currently focuses on the sustainability between economy and the environment, which can in other words be considered as between "natural capital" and "manufactured/man-made capital". This is also captured in the "*weak*" versus "*strong*" *sustainability* discussions. Weak sustainability is explained by Hartwick's rule [2], which states that under certain conditions, the amount of investment in produced capital (buildings, roads, knowledge stocks, *etc*.) is needed to exactly offset declining stocks of non-renewable resources. This investment is undertaken so that the standard of living of society does not fall as society moves into the indefinite future. In other words, Hartwick's rule states that so long as total capital stays constant, sustainable development can be achieved.

As long as the diminishing natural capital stocks are being substituted by gains in the man-made stock, total capital will stay constant and the current level of consumption can continue. The proponents believe that economic growth is beneficial as increased levels of income lead to increased levels of environmental protectionism. This is also known as the "substitutability paradigm". Conversely, strong sustainability, as supported by Herman Daly [16], believes that natural capital and man-made capital are only complementary at best. In order for sustainable development to be achieved, natural capital has to be kept constant independently from man-made capital. This is known as the "non-substitutability paradigm".

51.4.6 Resistance to Sustainability

There is a strong resistance to adopting sustainable practices. According to Unruh [21, 22], this is primarily due to the fact that today's technological systems and governing institutions were designed and built for permanence and not to change. In the case of fossil fuel-based systems, this is termed "carbon lock-in" and inhibits many efforts to change.

The whole world is aware that it must live sustainably. There are numerous practical, proven ways to do this, which is the *technical side* of the problem. However, society does not want to take the final step and adopt these practices, which is the resistance to change or the *social side* of the problem. *Therefore, the social side of the problem* prevails. Meadows *et al.* [27] in *Limits to Growth*

have put it very appropriately: "*Beyond the Limits* was published in 1992, the year of the global summit on environment and development in Rio de Janeiro. The advent of the summit seemed to prove that global society had decided to deal seriously with the important environmental problems. But we now know that humanity failed to achieve the goals of Rio. The Rio plus ten conferences in Johannesburg in 2002 produced even less; it was almost paralyzed by a variety of ideological and economic disputes, by the efforts of those pursuing their narrow national, corporate, or individual self-interests. … humanity has largely squandered the past 30 years…"

The failure of governments and individuals to act on the available information can be attributed to personal greed (deemed to be inherent in human nature) especially on the part of international capitalists. However, two things seem to be obvious from our discussion:

1. It is necessary to follow up the study of the socio-cybernetic, or systems processes, which, seem to control what happens in society.
2. We should use social-science-based insights to evolve forms of public management that will act on information in the long term public interest.

51.5 Pathways to Sustainability

With the ever-growing world population, we must have efficient mass production systems. At the same time people must have better life style and living standards. This imposes severe strain on the health of Earth's environment. Therefore, it is time that motivation for performance improvement must also change from economic compulsion to environmental compulsion. It is also true that no development activity for the benefit of human beings can possibly be carried out without incurring a certain amount of risk. This risk may be in terms of environmental degradation in terms of pollution of land, water, air, depletion of resources, and cost of replenishment or restoration to acceptable levels both during normal operating conditions and under the conditions of sudden hazardous releases on account of catastrophic failures or accidents. In the past, we have witnessed several technological (man-made) disasters, which had their origin in our underscoring the importance of ensuring the best level of system performance and its linkages with environmental risk**.**

There is a severe requirement of material conservation, waste minimization energy efficient systems than before. Instead of mining; recycling, recovery, and reuse should become more and more common, as these are not only cost effective but less energy intensive and less polluting. Recycling and reuse must be given serious consideration if nonrenewable resource consumption is to be minimized or energy use associated with material extraction is to be conserved. Use of renewable energy sources has to become the order of the day. The same is true about the prevention of pollution of *free resources* like water and air, which are also required for sustaining life support system of the planet we live on.

One of the important strategies of implementing sustainability is to prevent pollution (*rather than control* it) and this by itself cannot be viewed in isolation with the system performance. A better system performance would necessarily imply less environmental pollution on account of system longevity and optimum utilization of material and energy for limited resources scenario that governs the development of future systems. It is also naturally an economic proposition. In other words, sustainability depends very heavily on the performance characteristic of a system. Therefore, the objective of a system designer should be to incorporate the strategy of sustainability in all future system performance improvement programmes and designs.

The other pathways to achieve sustainable development and to minimize environmental impacts would be to use the concept of *industrial ecology* [18], which would entail to cluster a set of industries and have their *inputs* and *outputs* interlinked and mutually supported in order to preserve energy and materials including wastes. We have to work out methods of efficient energy generation and utilization, cleaner transportation, improved materials. Use of biotechnology for improving products and cleanup process for taking

care of effluents, molecular manufacturing, extensive use of biodegradable materials and plastics would have to become quite common in future.

In summary, the key issues associated with the implementation of sustainability characteristic appear to revolve around:

- The need to conserve essential natural resources, minimize the use of materials, develop renewal energy sources, and avoid over exploitation of vulnerable resource reserves.
- The need to minimize the use of processes and products that degrade or may degrade the environmental quality.
- The need to reduce the volume of waste produced by economic activities entering the environment.
- The need to conserve and minimize the use of energy
- The need to reduce or prevent activities that endanger the critical ecological processes on which life on this planet depends.

In this Handbook, we have tried to include Chapters 52, 53, 54 and 55 to cover the several important facets of sustainability problem.

51.6 Sustainable Future Technologies

As of now, two technologies appear to hold promise to revolutionize the way products and systems would be designed, built or used in the near future (within one or two decades), which will not only be highly dependeable but also sustainable. They are nanotechnology or molecular manufacturing and biotechnology. In the opinion of the author one is going to inflence the other and *vice versa.* As of today, nanotechnology is parallel to bioprocesses, which instead of consuming fossil fuels and emitting CO_2, uses CO_2 and sunlight to convert them into products and thus act as a net CO_2 consumer.The parallelism does not go beyond this and nonotechnology should not be considered a form of biotechnology, and molecular technology would not use ribosomes but robotic assembly; not veins but conveyors; not muscles but motors; not genes but computers; not cells dividing but small factories making products including factories. What molecular nanotechnology has in common with biology is the use of system of molecular machinery to guide molecular aasembly with clean and rapid precision.

51.6.1 Nanotechnology

Nanotechnology comes from the word nanometer, which is 10^{-9}. The idea behind nanotechnology is to custom design atom by atom. Feynman [1] in his classic talk in 1959 (at the annual meeting of American Physical Society at Caltech, on December 29, 1959) said: “The principles of physics, as far as I can see, do not speak against the possibility of maneuvering things atom by atom”. Nanotechnology just aims to achieve that. All manufactured products are made from atoms. The properties of those products depend on how those atoms are arranged. For example, if we can rearrange the atoms in coal in a definite way, we probably will make diamond.

Nanotechnology will achieve to:

- Get essentially every atom in the right place.
- Make almost any structure consistent with the laws of physics that we can specify in molecular detail.
- Have manufacturing costs not greatly exceeding the cost of the required raw materials and energy.

There are two more concepts commonly associated with nanotechnology:

- Positional assembly.
- Massive parallelism.

However, without using some form of positional assembly (to get the right molecular parts in the right places) this seems difficult and we need some form of massive parallelism (to keep the costs down). The need for positional assembly implies an interest in molecular robotics, *e.g.,* robotic devices that are molecular in their size and precision. These molecular scale positional devices are likely to resemble very small versions of their everyday macroscopic counterparts. Positional assembly is frequently used in normal macroscopic

manufacturing today, and provides tremendous advantages. Nanotechnology will require complete control of the structure of matter building complex objects with molecular precision. The research at present falls in two categories, *viz.*, theoretical and enabling technologies.

The problems of atomically-precise and nanometer-scale electronic systems, which includes studies of assemblers, replicators and nanocomputers need to be addressed. One robotic arm assembling molecular parts is going to take a long time to assemble anything large, so many robotic arms are required: this is what is meant by massive parallelism. While earlier proposals achieved massive parallelism through self replication, today's "best guess" is that future molecular manufacturing systems will use some form of convergent assembly. One of the concepts that is essential to molecular manufacturing is that of a self-replicating manufacturing system. And that concept has lagged behind in its acceptance even though it is fairly obvious that such things are feasible. So in order to produce the economies that we are talking about, in order to economically produce complex products we are basically going to adopt a strategy that has been demonstrated by agricultural products.

Molecular manufacturing [10, 12, 14] is the ultimate goal of nanotechnology. The benefits that will flow from the use of nanotechnology in making products or systems sustainable are as follows:

Less material, higher performance capabilities, low cost, waste minimization, and less energy requirement. The products would be lighter and stronger. For example, a diamond is light and strong. The strength-to-weight ratio of a diamond is over 50 times that of steel. Great strength and light weight is not exclusive to diamonds; graphite can also be strong. Aeroplanes or rockets would benefit immensely from having lighter and stronger materials. This would reduce the cost of air travel, and it would reduce the cost of rockets and allow space travel or exploration at literally orders of magnitude lower cost. Lighter computers and lighter sensors would enable more functions for a given weight, Today's computers are made of semiconductors, and the semiconductor of choice is silicon. This is not because silicon is the ideal semiconductor from which to make computers, but because we know how to make devices from it. Diamond [9] will make better computers than silicon [11]. Diamond has a wider band gap, hence electrical devices will work at higher temperatures. It has greater thermal conductivity, so devices can be more easily cooled. It has a greater breakdown field, hence devices can be smaller. It has higher electron and hole mobility, which, when combined with higher electric fields, would result in higher speed. However, there are many problems that do not make diamond a practical alternative. In fact, the use of molecular manufacturing [13] for the computer industry is quite tempting as it would allow us to build computers at a manufacturing cost of less than a dollar per pound, operating at frequencies of tens of gigahertz or more, with linear dimensions for a single device of roughly 10 nanometres, high reliability, and energy dissipation (using conventional methods) of roughly 10^{-18} joules per logic operation. A factor of crucial importance in the design of molecular-scale positional devices is the accuracy with which the tip can be positioned, particularly in the face of thermal noise. Finally, we would need a source of control signals for the molecular arm. One general approach would be to use a molecular computer and it is generally expected that some type of very small computational device will be feasible in a few decades [10]. There will be many additional advantages from the off-shoots of this technology in other application areas. The long term goal of molecular manufacturing is to build exactly what we want at low cost.

Nanomaterials and nanodevices are becoming quite useful in many areas of application. In this handbook, Chapter 57 discusses nanotechnology and its applications are provided in Chapters 58 and 59.

51.6.2 Biotechnology

Biotechnology is defined as any technological application that uses biological systems, living organisms, or derivatives thereof, to make or modify products or processes for specific use. Modern biotechnology is only 50 years old and in

the last decades it has witnessed tremendous developments. Bioengineering is a science upon which all biotechnological applications are based. Before the 1970s, the term, biotechnology, was primarily used in the food processing and agriculture industries. Since the 1970s, it has been used to refer to laboratory-based techniques being developed in biological research, such as recombinant DNA or tissue culture-based processes. It can also be defined as the application of indigenous and/or scientific knowledge to the management of (parts of) micro-organisms, or of cells and tissues of higher organisms, so that these supply goods and services of use to human beings. Biotechnology combines disciplines like genetics, molecular biology, biochemistry, embryology and cell biology, which are in turn linked to practical disciplines like chemical engineering, information technology, and robotics.

Biotechnology has applications in four major industrial areas, including health care, crop production and agriculture, non-food uses of crops (*e.g.,* biodegradable plastics, vegetable oil, biofuels), and environmental uses. For example, one application of biotechnology is the directed use of organisms for the manufacture of organic products (examples include beer and milk products). Another example is using naturally present bacteria by the mining industry in bioleaching to reclaim land spoils. Biotechnology is also used to recycle, treat waste, clean up sites contaminated by industrial activities (bioremediation), and has a military application in the production of biological weapons. *Red biotechnology* is applied to medical processes. The examples are the designing of organisms to produce antibiotics, and the engineering of genetic cures through genomic manipulation. Modern biotechnology can be used to manufacture existing drugs more easily and cheaply. The first genetically engineered products were medicines designed to combat human diseases. There are also applications to increase nutritional qualities of food crops. Proteins in foods may be modified to increase their nutritional qualities. There are very many applications of biotechnology in the medicinal use and in preparing human insulin to cure diabetes and in developing genetic engineered crops and high yielding and diseases resistant crops. However, here our main concern is with those applications that help in making sustainable products and systems (or in manufacturing) and help environmental clean up or pollution prevention.

White biotechnology, also known as *grey biotechnology*, is biotechnology applied to industrial processes. An example is the designing of an organism to produce a useful chemical. Another example is the using of enzymes as industrial catalysts to either produce valuable chemicals or to destroy hazardous/polluting chemicals [29] (using oxidoreductases). Biological leaching can be used in extracting metals from ore particularly when the grades of ore are becoming poorer and poorer day by day as we keep satisfying the need of the world for nonrenewable resources. Plastic, which has very high industrial and domestic use, was considered as the source of pollution since it was not biodegradable. Using biotechnology, we can produce biodegradable plastic. We can also use it to remove heavy metals and sulfates from water. Chlorine bleaching in pulp and paper industry is being replaced by biotechnology processes. White biotechnology tends to consume less in resources than traditional processes used to produce industrial goods.

Green biotechnology is biotechnology applied to agricultural processes. Most of the current commercial applications of modern biotechnology in agriculture are on reducing the dependence of farmers on agrochemicals. The term *blue biotechnology* has also been used to describe marine and aquatic applications of biotechnology, but its use is relatively rare.

In this handbook Chapter 56 deals with biotechnology.

References

[1] Feynmann R. There's plenty of room at the bottom miniaturization. Gilbert Reinhold (ed.). Reinhold, New York, 1961: 282–296.

[2] Hartwick John M. Intergenerational equity and the investment of rents from exhaustible resources. American Economic Review; 1977, Dec.:67:972–974.

[3] Rau JG, Wooten DC. Environmental impact assessment analysis handbook. Mc Graw-Hill, New York, 1980.
[4] Westman WE. Ecology, impact assessment and environmental planning. Wiley, New York, 1985.
[5] Brundtland GH (ed.). Our common future: The World Commission on Environment and Development. Oxford University Press, 1987.
[6] Tisdell C. Sustainable development: Differing perspectives of ecologists and economists, and relevance to LDCs. World Development; 1988:16(3): 373–384.
[7] Daly H, Cobb J. For the common good: Redirecting the economy toward community, the environment, and a sustainable future. Beacon Press, Boston, 1989.
[8] Greenberg HR, Cramer JJ (eds.). Risk assessment and risk management for the chemical process industry. Van Nostrand Reinhold, New York, 1991.
[9] Keyes RW. Limits and Challenges in Electronics. Contemporary Physics; 1991: 32(6): 403–419.
[10] Drexler KE. Nanosystems: Molecular machinery, manufacturing, and computation. Wiley, New York, 1992.
[11] Geis MW, Angus JC. Diamond Film semiconductors. Scientific American; 1992: Oct.:84.
[12] Merkle RC. Self replicating systems and molecular manufacturing. Journal of the British Interplanetary Society; 1992: 45: 407–413.
[13] Merkle RC. Reversible electronic logic using switches. Nanotechnology; 1993: 4: 21–40.
[14] Drexler KE. Molecular manufacturing: A future technology for cleaner production. In: Clean production: Environmental and economic perspectives. Misra KB (ed.). Springer, Berlin, 1996.
[15] Odum HT. Environmental Accounting: Emergy and environmental decision making. Wiley, New York, 1996.
[16] Daly H. Beyond Growth: The economics of sustainable development. Beacon Press, Boston, 1996.
[17] Brown MT, Ulgiati S. Emergy-based indices and ratios to evaluate sustainability: Monitoring economies and technology toward environmentally sound innovation. Ecological Engineering; 1997: 9: 51–69.
[18] Esty DC, Porter ME. Industrial ecology and competitiveness: Strategic implications for the firm. Journal of Industrial Ecology; Winter 1998: 2(1): 35–43.
[19] Ulgiati S, Brown MT. Emergy accounting of human-dominated, large scale ecosystems. In Jorgensen and Kay (eds.). Thermodynamics and Ecology. Elsevier, New York, 1999.
[20] Brown MT, Ulgiati S. Emergy evaluation of natural capital and biosphere services. Ambio; 1999: 28(6): 486–493.
[21] Unruh G. Understanding carbon lock-in. Energy Policy; 2000: 28(12): 817–830.
[22] Unruh G. Escaping carbon lock-in. Energy Policy; 2002: 30(4): 317–325.
[23] Yi Heui-seok, Hau Jorge L, Ukidwe Nandan U. Bakshi Bhavik R. Hierarchical Thermodynamic Metrics for Evaluating the Environmental Sustainability of Industrial Processes. Environmental Progress; 2004:23(4): 65–75.
[24] Shields DJ, Solar SV, Martin WE. The role of values and objectives in communicating indicators of sustainability. Ecological Indicators; 2002: 2 (1–2):149–160.
[25] Robèrt, K.H. The natural step story: Seeding a quiet revolution. New Society Publishers, Gabriola Island, BC, Canada, 2002.
[26] Raskin P, Banuri T, Gallopin G, Gutman P, Hammond A, Kates R, Swart R. Great transition: The promise and lure of of the times ahead. Tellus Institute, Boston, 2002.
[27] Meadows DH. Limits to growth: The 30-year update. Chelsea Green Publishing Company, White River Junction, VT, 2004.
[28] Hargroves Karl, Smith M. (eds.). The natural advantage of nations: Business opportunities, innovations and governance in 21st century. Earthscan/ James and James, London, 2005.
[29] Feng Xu. Applications of oxidoreductases: Recent progress, Industrial Biotechnology; 2005: 1: 38–50.
[30] Jain Ravi. Sustainability: metrics, specific indicators and preference index. Clean Technologies and Environmental Policy; 2005: 7: 71–72.
[31] Zhao S, Li Z, Li W. A modified method of ecological footprint calculation and its application. Ecological Modelling; 2005: 185 (1): 65–75.
[32] Richardson BJ and Wood S. (eds.) Environmental law for sustainability: A reader, Hart Publishing, Oxford, 2006.
[33] Marks N, Simms A, Thompson S, Abdallah S. The (Un)happy planet index. New Economics Foundation, London, 2006.
[34] Kriegman O. Dawn of the cosmopolitan: The hope of a global citizens movement. Tellus Institute, Boston, 2006.
[35] Hezri A, Dovers SR. Sustainability indicators, policy and governance: Issues for ecological economics. Ecological Economics; 2006: 60(1):86–99.
[36] Ness B, Urbel-Piirsalu E, Anderberg S, Olsson L. Categorizing tools for sustainability assessment. Ecological Economics; 2007: 60(3): 498–508.

52

Corporate Sustainability: Some Challenges for Implementing and Teaching Organizational Risk Management in a Performability Context

Rod S. Barratt

Department of Environmental and Mechanical Engineering, Faculty of Technology, The Open University, Walton Hall, Milton Keynes, MK7 6AA, UK

Abstract: This chapter discusses some pressures to ensure that 21st century products, systems and services are not only dependable but are also sustainable. Failure in any of these aspects may threaten an organization. So companies should ensure that they have a sound system of internal control and effective risk management processes. This includes measures to prevent emergencies arising or escalating, and emergency planning is essential to allow the organization to survive a crisis. Then it is essential to address the problem quickly, openly and effectively. Experience increasingly shows that risk management decisions made in collaboration with stakeholders are more effective and more durable, and so aspects of stakeholder engagement through corporate disclosure are discussed.

52.1 Introduction

Risk and hazard are commonplace words, but risk is an ambiguous word in business. To the investor, risk may be associated with the potential for financial gain, whereas an engineer may focus on the potential for loss or harm. Nevertheless, the latter has economic implications, and the trick is to manage processes to minimize their loss potential but equally to ensure that if an incident occurs, appropriate contingency measures are in place. For the educator, there are numerous incidents that may be used to illustrate a variety of technical failures which have had varying impact on investor value. There are also issues about increasing corporate disclosure to stakeholders that provide demanding educational challenges. Some of these issues are outlined and case studies explored to illustrate the failure mechanisms, the impacts and possible lessons to learn as well as opportunities to build these into educational programmes involving corporate sustainability. Examples from various industries reflect the breadth of performability considerations.

52.2 Pressure for Change

Organizations everywhere are continually changing the way they do business, their relationships between customers and suppliers, and also in the way they organize themselves through mergers, acquisitions, *etc*. There are also changes in the way organizations interface with the society

in which they operate, through growth, contraction, response to government policies, responses to new processes, new materials and so on. At the level of an organization, three areas of environmental risk may be identified:

- Risks to the environment from manufacturing processes with routine process releases into the environment. Accidents or incidents may also cause loss of containment and consequent release into the environment.
- Risks associated with purchase or inheritance of a contaminated site.
- Risks from the environment on a business arising from such problems as extreme weather conditions or long-term environmental changes, for example, through the greenhouse effect and climate change. There are also risks from other activities in the surrounding areas.

The first issue is readily apparent with clear performability linkages, while the other two may be less obvious and may be considered irrelevant. However all are important to organizations and environmental risk assessment techniques can be applied to all of them. Organizations need to look critically at all risks facing their business, and this goes wider than environmental health and safety risks. This assessment needs an understanding of the business and its processes, the market, the environment and the legislation.

Environmental risks to an organization are associated with contingent liabilities that may arise from its normal economic activity. Internationally, cost recovery legislation creates the potential for civil liability in the face of environmental damage by potentially allowing regulators and others to recover costs incurred in environmental clean-up as well as payment for natural resource damages. As corporations are increasingly responsible for the financial consequences of environmental contingencies, environmental risk assessments are a growing part of both financial and environmental management and are becoming more central to corporate governance at the board level.

So there are many pressures on organizations to address environmental issues. In the past, these pressures have all too often been considered as constraints. Organizations limited themselves to correcting negative aspects as each problem arose, and the cost of corrective action by end-of-pipe controls was emphasized. Short term remedies were favoured without consideration of the root cause of the problems. Building taller chimneys, using landfill sites further and further from cities, and installing gas cleaning plant are merely procrastination and underlying problems are not addressed. The evolution of awareness and the underpinning of legal and social pressures now present the environment as a business opportunity with the global environmental goods and services market being forecast to grow to $688 billion by 2010 and just under $800 billion by 2015 [1]. From a situation in which organizations limited themselves to correcting negative aspects of each problem with an emphasis on costs, an active environmental management phase evolved, with the environment being recognized as an area of opportunity. It is increasingly recognized that it is better not to contribute to pollution than to combat it. The next evolutionary phase integrates the behaviour of an enterprise with the environment, and the solution of environmental problems is recognized as the result of healthy management. This step by step improvement of environmental performance may be approached as suggested in Figure 52.1.

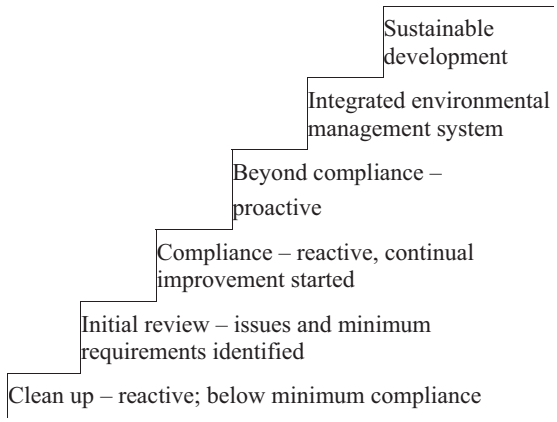


Figure 52.1. Steps of environmental management

There may be legal pressures to promote this progression, particularly through legislation. The early emphasis was on control of emissions of pollutants rather than their prevention. That idea came much later. In the UK, it was not until the Environmental Protection Act 1990 that there was an objective that processes use techniques:

> *(i) for preventing the release of substances prescribed for any environmental medium into that medium or, where that is not practicable by such means, for reducing the release of such substances to a minimum and for rendering harmless any such substances which are so released.*
>
> Section 7(2)(a) of the Environmental Protection Act 1990 in the UK (emphasis added)

This shows a clear hierarchy indicated of prevention before control that is also evident in the subsequent Integrated Pollution Prevention and Control (IPPC) Directive from the EU (Council Directive 96/61/EC). This was modeled to a large extent on the UK system, and became effective in the UK from October 1999 with subsequent UK regulations introduced in August 2000. In working to comply with this, organizations should use the best available techniques, which mean:

> *... the most effective and advanced stage in the development of activities and their methods of operation which indicate the practical suitability of particular techniques for providing in principle the basis for emission limit values designed to prevent and, where that is not practicable, generally to reduce emissions and the impact on the environment as a whole:*
>
> *– "techniques" shall include both the technology used and the way in which the installation is designed, built, maintained, operated and decommissioned,*
>
> *– "available" techniques shall mean those developed on a scale which allows implementation in the relevant industrial sector, under economically and technically viable conditions, taking into consideration the costs and advantages, whether or not the techniques are used or produced inside the Member State in question, as long as they are reasonably accessible to the operator,*
>
> *– "best" shall mean most effective in achieving a high general level of protection of the environment as a whole.*
>
> Council Directive 96/61/EC 24 September 1996

It is clear that waste minimization is a key component of the modern approach to environmental protection, and waste minimization is achieved *inter alia* by the efficient use of all resources, including energy, materials and, of course, personnel.

Good environmental management is often regarded as part of total quality management, and that an organization with effective quality systems in place should minimize problems and may not require environmental inspection as frequently as an organization without such systems. Proven good environmental management systems supported by audit data may also be demanded before an organization can secure a bank loan, by investors before they will invest in and it may be required by its customers before they will buy from it. Public liability insurance policies normally have not included pollution, and the underwriting of potential claims may present major problems in the future. Insurers are therefore likely to seek audit data before taking new risks. Few can now believe that good environmental performance is an optional extra: what was once regarded as offering a market advantage is becoming a prerequisite to entering the market-place.

Amongst the concepts and tools that help improve environmental performance is "eco-efficiency", which:

> *... is reached by the delivery of competitively priced goods and services that satisfy human needs and bring quality of life, while progressively reducing ecological impacts and resource intensity throughout the life cycle, to a level at least in line with the earth's estimated carrying capacity*. [2]

In simple terms, eco-efficiency means "doing more with less", using environmental resources more efficiently in economic processes by engineering techniques, clearly demonstrating performability principles.

One of the ways of achieving eco-efficiency is through cleaner production. This is:

> *"…the continuous application of an integrated preventative environmental strategy applied to processes, products and services. It embodies the more efficient use of natural resources and thereby minimises waste and pollution as well as risks to human health and safety. It tackles these problems at their source rather than at the end of the production process; in other words it avoids the "end-of-pipe" approach…. For processes, Cleaner Production includes conserving raw materials and energy, eliminating the use of toxic raw materials and reducing the quantity and toxicity of all emissions and wastes…For products, it involves reducing the negative effects of the product throughout its life-cycle, from the extraction of the raw materials right through to the product's ultimate disposal…. For services, the strategy focuses on incorporating environmental concerns into designing and delivering services…"* [2]

In the past, emphasis tended to be on environmental releases from the main "point" sources; nowadays the emphasis is increasingly on the control of accidental or "unauthorized releases" from industrial processes. In part this is due to increasing controls over point releases, although, ironically, this may have resulted in the environment becoming relatively more susceptible to risks from non-routine process emissions caused by equipment failure or maloperation. The public and other stakeholders are becoming less tolerant of such releases. Currently, all major companies operating within the EU must have a documented and rehearsed emergency plan. Senior management's interest in failure should not only be limited to major incidents; the treatment of smaller, less serious incidents should be of utmost concern especially in terms of the relevance or appropriateness of existing working practices.

Many improvements can be made in production processes at no or very little cost. This improves both an organization's profitability and its environmental performance, whatever the business sector. Some other "tools" for eco-efficiency and cleaner production include:

- Economic instruments such as taxes, refunds, *etc.,* that encourage optimal resource use.
- Environmental accounting to integrate environmental costs into decision making.
- Environmental audits are designed to identify an organization's environmental impacts.
- Environment management systems (EMS) offer a structured approach to measure their environmental performance, and then regularly evaluate their performance and improvement.
- Public environmental reporting is the process whereby an organization examines its environmental performance over a specified reporting period and disseminates that information to a wide audience.
- Life cycle assessment (LCA) is the collection and evaluation of quantitative data on the inputs and outputs of material, energy and waste flows associated with a product or service over its entire life cycle. This enables its environmental impacts to be determined.
- Design for the environment (DFE) or "ecodesign" examines a product's entire lifecycle and proposes changes to how the product is designed to minimize its environmental impact during its lifetime.

Several of these tools are supported by guidelines from the International Standards Organization (ISO), and some current documents are listed in Table 52.1. An integral part of an organization's environmental management system is the commitment to continual improvement and in accord with this principle, the standards are regularly reviewed.

Table 52.1. Some current standards relating to environmental management

ISO 14001:2004	Environmental management systems. Requirements with guidance for use
ISO 14015:2001	Environmental management. Environmental assessment of sites and organizations
ISO 14031:1999	Environmental management. Environmental performance evaluation – Guidelines
ISO 14040:2006	Environmental management. Life cycle assessment – Principles and framework
ISO 14044:2006	Environmental management. Life cycle assessment – Requirements and guidelines
ISO/TR 14062:2002	Environmental management. Integrating environmental aspects into product design and development
ISO 14063:2006	Environmental management. Environmental communication – Guidelines and examples
ISO 14064 -1:2006	Greenhouse gases. Part 1: Specification with guidance at the organization level for quantification and reporting of greenhouse gas emissions and removals. Parts 2 and 3 also relate.
ISO/FDIS 14065	Greenhouse gases. Requirements for greenhouse gas validation and verification bodies for use in accreditation or other forms of recognition
ISO 19011:2002	Guidelines for quality and/or environmental management systems auditing
ISO/WD 26000	Guidance on social responsibility

52.3 Internal Control

"Performability" reflects an "holistic" view of designing, producing and using a product, system or a service which will satisfy the requirements of a customer to the best possible extent without creating an adverse effect on our environment. This implies that the 21st century products, systems and services not only have to be dependable but must be sustainable [3]. Failure in any of these aspects may threaten an organization.

In September 1999 publication of "Internal Control: Guidance for Directors on the Combined Code", often called the "Turnbull report" [4], after its chairman (Nigel Turnbull, Executive Director of Reed Plc), marked a landmark in corporate governance. The guidance is based on the adoption by a company's board of a risk-based approach to internal control, and on reviewing its effectiveness. This should be incorporated by a company within its normal management and governance processes.

The span of internal control contemplated by Turnbull stretches wider than financial controls, to encompass social and environmental issues, which are often considered under the generic heading of "reputational risk". The Turnbull report [4] noted that:

> *A company's objectives, its internal organisation and the environment in which it operates are continually evolving and, as a result, the risks it faces are continually changing. A sound system of internal control therefore depends on a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed. Since profits are, in part, the reward for successful risk-taking in business, the purpose of internal control is to help manage and control risk appropriately rather than to eliminate it.*

In an appendix suggesting ways for assessing the effectiveness of the company's risk and control processes, the Turnbull report posed several questions on risk assessment including:

> *Does the company have clear objectives and have they been communicated so as to provide effective direction to employees on risk assessment and control issues? For example, do objectives and related plans*

include measurable performance targets and indicators?

Are the significant internal and external operational, financial, compliance and other risks identified and assessed on an ongoing basis? (Significant risks may, for example, include those related to market, credit, liquidity, technological, legal, health, safety and environmental, reputation, and business probity issues.)

Is there a clear understanding by management and others within the company of what risks are acceptable to the board? ...

Does the company communicate to its employees what is expected of them and the scope of their freedom to act? This may apply to areas such as customer relations; service levels for both internal and outsourced activities; health, safety and environmental protection; security of tangible and intangible assets; business continuity issues; expenditure matters; accounting; and financial and other reporting.

Do people in the company (and in its providers of outsourced services) have the knowledge, skills and tools to support the achievement of the company's objectives and to manage effectively risks to their achievement?

How are processes/controls adjusted to reflect new or changing risks, or operational deficiencies?

Conventional measurement, management and quality assurance tools are not totally adequate for assessing and managing risk associated with emerging social and environmental factors that can affect financial performance. Organizations therefore seek new tools and approaches that allow them to meet the requirements set out in the Turnbull report, and that are consistent with good business practice. Tools such as those in Table 52.1 help address some of the risks.

Clearly risk is an important business issue, so it is appropriate to start by considering its meaning(s). The concepts of risk and risk management are used in many diverse fields, but their meaning differs in different disciplines. When we say we are going to take a risk we mean that we are prepared to take a chance of an adverse consequence in the expectation of a benefit. Implicit in that interpretation is that risk reflects both a likelihood of "harm" and a measure of the consequence. In everyday life, however, it is consequence that may be paramount in our mind rather than likelihood. Commonly we associate risk with some aspect of "loss", but it is important to recognize that in financial management, risk attempts to quantify the probability of loss as contrasted to the probability of gain. The emphasis is on a potential benefit.

To achieve the full benefit of embedding risk management, not only should the risks being managed be more visible, but also the resultant attention those risks receive must result in managing risks more effectively. This pressure raises the profile of risk management on the business agenda.

The Turnbull report confirms that the management of companies may be held accountable for risks beyond traditional financial threats. It establishes risk management as a "top down" process based on the management's analysis of key threats to success as diverse as consumer behaviour, supplier failure, or obsolete products as well as environmental health and safety issues. However, any review of risks should concentrate on the significant ones. These aspects of top level commitment and a focus on significant risks are similar to risk management issues from other aspects of business, particularly environmental and health and safety management.

52.4 Risk Assessment and Management

The increased complexity since the second half of the 20th century brought sources of risk with high real and perceived profiles: environmental pollution, nuclear hazards, transport accidents, financial market instabilities, toxicology and terrorism. At the business level, operational risk,

mergers, acquisitions, downsizing, technology innovations, the introduction of e-business processes, information security, market forces, economic pressures, natural disasters, competitor and business partner behaviour, regulatory and legislative changes all involve risks and the prospect and challenge of change. Organizations have always needed a philosophy and structure that not only enables them to plan for future changes but to recognize opportunities and profit from them.

We live in a period of increasing pace of change, and any organization that is unwilling or unable to adapt will lose its profitability, competitive edge, or even fail altogether. Business change alters the overall profile of risk any organization faces and the specific risks to each business process. It should also result in review and updating of business continuity plans. Unlike health and safety legislation, environmental legislation has not been so explicit in demanding risk assessments for environmental protection. However, regulatory agencies are increasingly recognising the benefits from the use of risk assessment techniques in dealing with environmental problems. Such risk assessments also serve as the basis for determining the frequency of inspections by regulators. The role of risk assessment in pollution prevention and control is also being increasingly recognized by legislators. For example, regulations on contaminated land stipulate the use of risk assessment for prioritising remediation work.

Companies themselves are also recognising the benefits of applying formal environmental risk assessment techniques to minimize their environmental liabilities and reduce the frequency of environmental incidents. These can lead to adverse publicity, and also engender significant costs from incident investigation, cleaning up the environment, prosecutions and fines. All may have an impact on the company and its "value" to stakeholders.

In general the management approach requires hazards to be identified, the risks they give rise to assessed and appropriate control measures taken to address the risks.

Risk assessment also provides a means of prioritising resources so as to ensure the most efficient use of the capital available. It can also improve the robustness of decisions on best available techniques for preventing or minimizing pollution and on the best practicable environmental option (BPEO) for minimizing the impact on the environment as a whole.

Formal risk assessment techniques offer an approach for organizations to address their risks. Many risks can be identified instinctively, or by using qualitative methods, without recourse to more detailed and time consuming quantitative risk assessment methods. However, quantitative techniques may be more appropriate when:

- there are concerns that qualitative approaches may overlook important issues;
- there are uncertainties over the likelihood or consequence (or both) of a system going wrong and where quantifying these may reduce uncertainty,
- qualitative assessments indicate a significant number of risks in a system, hence there is a need to prioritize risk reduction or mitigation work using more robust techniques. This is especially important when high levels of spending are required.

With environmental risk we have seen that the concern is with the probability of an event causing a potentially undesirable effect. It involves the separate consideration of the likelihood and the consequences of an event, for the purposes of making decisions about the nature and significance of any risks, and how best to manage any unacceptable risks. Quantitative risk assessment is thus a statistical approach, because probability is the mathematical measure of risk, but it also concerns hazard assessment that relates to the nature of the undesirable effect. Environmental agencies, use risk assessment as an objective tool to set standards, set priorities and provide assistance in decision making. It has long been applied in this way to evaluate the risks to human health arising from chemicals in the environment, for example.

Having identified the main risks to the environment it is equally important that the site environmental management systems give due recognition to them. These systems must then be audited regularly to check that they remain effective, thus ensuring a complete and up-to-date risk management system is in place, in accordance with the requirements for corporate governance.

All of these pressures lead to better environmental protection through better management of risk and planning for emergency scenarios. As noted earlier, the requirements for internal control demand that organizations address these issues.

A risk present in an organization, which has the influence to cause damage of any type, must be effectively managed to reduce it and mitigate subsequent liability and/or damage. The same applies to potential risks. Before expending valuable resources in managing the risk, senior management must first set about identifying all possible risks facing the organization and then carry out an assessment process to decide which risks are most relevant and significant to it. Once the significant risks have been identified, management systems can then be improved or established to reduce them. All areas of the business should be looked at to identify sources of risks within the company (operational). Other areas where the business impacts must also be analysed include upstream processes (supply chain), downstream processes (product end-of-life) and external areas (societal).

If significant risks to a company are managed effectively, the probability of them occurring will reduce, thus removing them from the "critical zone". Management systems such as the ISO 14000 series and OHSAS 18001, an international occupational health and safety management system specification embracing BS8800, AS/NZ 4801, NSAI SR 320 and others may mitigate many risks facing an organization [5].

Having identified risks to the environment and implemented measures to reduce or mitigate these risks it is equally important that the management systems give due recognition to them. Failure to make all relevant staff aware of these systems and the need to monitor and maintain them will give rise to more frequent incidents and greater environmental impact. In fact it defeats the objective if risk reduction or mitigation techniques are installed and the required management systems including emergency planning are not also put in to ensure they are properly operated, monitored or maintained.

Hence measures installed need to be addressed in staff training programmes, in operating instructions, in plant troubleshooting guides and in operator log sheets. They should also be given the correct priorities in any site preventative maintenance system. All of these elements form part of the management systems.

Central to approaches to understanding and managing risk more effectively is stakeholder dialog. When handled effectively, this dialog can influence views and behaviour of stakeholders and the company itself in ways that enable performance improvements in both the short and the longer term. These concerns have led to a growing number of accountability standards that provide a basis for optimising stakeholder dialog for risk assessment and management by linking it to a broad framework of measurement, accounting, auditing, verification and public disclosure. The recent standard, ISO 14063:2006, gives guidance to an organization on general principles, policy, strategy, and activities relating to both internal and external environmental communication and addresses the important "reputational risk" referred to previously.

52.5 Stakeholder Involvement

A stakeholder is anyone who has a "stake" in a risk management situation. Stakeholders typically include groups that are affected or potentially affected by the risk, the risk managers, and groups that will be affected by any efforts to manage the source of the risk. Who the stakeholders are depends entirely on the situation. The objectives, interests and responsibilities of stakeholders may be varied and contradictory.

Questions that can help identify potential stakeholders include:

- Who might be affected by the risk management decision? (They may not know it.)
- Who has information and expertise that might be helpful?
- Who has been involved in similar risk situations before?
- Who has expressed interest in being involved in similar decisions before?
- Who might be reasonably angered if not included?

Experience increasingly shows that risk management decisions made in collaboration with stakeholders are more effective and more durable. Stakeholders bring to the table important information, knowledge, expertise, and insights for developing workable solutions. They are more likely to accept and implement a risk management decision they have participated in shaping. One reason for this is differences in the perceptions of risk.

52.5.1 Perceptions of Risk

The opinions of the public have to be taken account of in the evaluation of risk. It involves interactions across many domains of the environment, and despite massive financial investment, political action and steady improvements in health, safety and the quality of life, the threats posed by technology are still perceived by many as large. Social structures and the processes of risk experience, the resulting repercussions on individual and group perceptions, and the effects of these responses on communities, societies and the economy have been termed "the social amplification of risk". This framework describes how both social and individual factors act to modify perceptions of risk and through this create secondary effects such as stigmatization of technologies, economic losses or regulatory impact as will be discussed shortly.

Sometimes, there is a discrepancy between the risks perceived by experts and the way in which risks are reported and perceived by the public. For example, studies have shown that the public often rank the risks from hazardous waste sites as most serious, whereas the experts rank the risks from these sites as medium/low on the basis of an understanding of the engineered precautions taken to manage such sites. At the other end of the scale, the public may rank the seriousness of indoor air pollution and global warming as relatively low, while experts rank them as high. In other areas there can be agreement between public and experts. Experts may use a calculation based on objective data to generate the actual risk. The perceived risk, or subjective risk, is the risk estimate obtained by surveying the public either for their estimate of the hazard involved (very safe, safe, marginal, dangerous, very dangerous) or for their estimate of the number of accidents or whatever else is the issue.

To a certain extent it is impossible to provide a truly objective measure of risk. Choosing numbers from a table of data involves a subjective decision. A combination of small probabilities and large possible outcomes are known to cause problems with perception of the risks involved, and research has shown that people tend to overestimate the risk of death from low probability causes, and underestimate the risk of death from high probability causes.

People also rank risks based on how well the process is understood, how equitably the danger is distributed, how well individuals can control their exposure and whether risk is voluntarily assumed. These items can be combined into three major factors. The first is an event's degree of dreadfulness, as determined by features such as the scale of its effects and the degree to which it affects innocent bystanders; the second is a measure of how well the risk is understood; and the third is the number of people exposed.

Dread and understanding can be used to understand perceptions. The location within a space defined by these "values" indicates a likely public response. Risks carrying a high level of dread, for example, provoke more concern than do some more familiar risks that actually cause more deaths or injuries.

The concept of risk involves interactions across many domains of the environment, and despite massive financial investment, political action and steady improvements in health, safety and the

quality of life, the threats posed by technology are still perceived by many as large. In the context of "the social amplification of risk" [6], signals about a risk may emerge from direct personal experience or through receiving information, and these signals may be processed by social and individual "amplification stations". These "amplification stations" might include:

- the scientist conducting the technical risk assessment and communicating it,
- the news media,
- pressure groups,
- opinion leaders within social groups,
- personal networks,
- public agencies.

The amplification of risks is likely to result ultimately in effects such as:

- enduring perceptions and attitudes not in favour of technology,
- impact on business sales, property values and economic activity,
- political and social pressure,
- changes in the nature of the risk through feedback,
- changes in education and training,
- social disorder such as protests or even sabotage,
- regulatory changes,
- impact on other technological advances, for example the generation of low public acceptance or trust.

The impacts may spread further to other groups, locations or generations, not unlike the ripple effect when a stone drops into a pond.

It is important to recognize that amplification and attenuation hold equal place in the framework. While instances of amplification captured the headlines in scares, addressing performability failures may involve changing behaviour, and here it is attenuation that may rule.

It is clear, then, that a growing numbers of stakeholders want to integrate environmental and social information in their decision making processes [7]. With the increased information flow across the world that increases the visibility of an organization's activities, organizations are themselves voluntarily choosing to be more transparent. The stepwise trend is suggested in Figure 52.2.

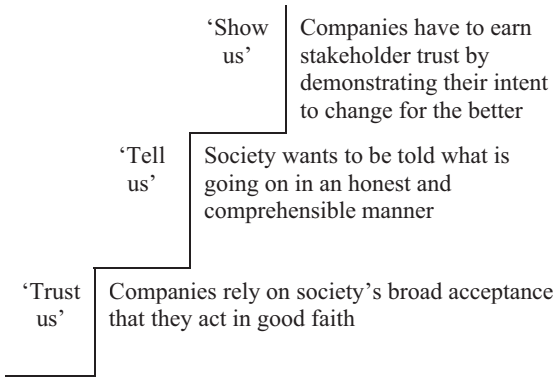


Figure 52.2. Evolution of corporate responsibility

Adverse criticism on environmental and social performance can put at risk the significant economic value of good corporate reputation and a well-regarded brand, as will be considered shortly. However, organizations that demonstrate commitment to good performance can earn the trust from society if a disaster does occur.

52.5.2 Stakeholder Dialog

Central to the approaches to understanding and managing risk more effectively is stakeholder dialog. Dialog can serve the purpose of assessing and more effectively managing aspects of risk by building trust with key stakeholders; acquiring critical information about future societal and market trends; and reaching greater consensus with stakeholders as to what they think constitutes appropriate business purpose and behaviour.

Ultimately, dialog, when handled effectively, can influence views and behaviour of stakeholders and the company itself in ways that enable performance improvements in both the short and the longer term. Poor quality dialog can reduce its value, and indeed can actually damage reputation. These concerns have led to a growing number of accountability standards and management systems developed through partnerships between business, governments and international agencies.

Public environmental reporting, sometimes referred to as "disclosure" is the communication of environmental performance information by an organization to its stakeholders. Increasingly, organizations are choosing to publish such reports, some in response to mandatory requirements, others in accordance with emerging business requirements or changing stakeholder expectations.

As an aspect of performability, pollution prevention in companies has changed from a rather narrow and technical focus on optimization of the existing production processes to a more organizational focus on environmental management. Growing emphasis on the environmental impacts from products over their life cycles, globalization with international product chains and the focus on environmental impacts from products increase the need for environmental communication in and between companies. In this regard it has been said that a preventive environmental effort in a company is a social and distributed process, where environmental communication is "the glue" keeping the process together [8]. Its importance has been recognized by ISO 14063:2006, listed in Table 52.1, which gives guidance to an organization on general principles, policy, strategy and activities relating to both internal and external environmental communication. However, as Table 52.2 indicates, there are many approaches.

While environmental and social disclosures are on the increase in annual reporting, the principal customers for the annual report package may not be directly concerned with the finer details of environmental performance, but with high-level risk, governance and assurance issues. For such users, environmental issues may be amalgamated into a general concern over so-called reputational risk. Investors require assurance that a company is meeting all necessary obligations arising from its stated environmental and social policies.

In particular, it should manage its operations in ways that meet relevant legal regulations and minimize its exposure to any potential environmental liabilities or reputational risk. These changes form part of a paradigm shift towards corporate transparency and public accountability.

Table 52.2. Approaches to environmental reporting

Compliance based	Report level of compliance against external regulations and consents. This is often a feature of heavily regulated organizations such as utilities and chemicals.
Toxic release inventory based reporting	Under US law, many companies are obliged to publish data on emissions of specific toxic substances. Such mandatory disclosure takes precedence over voluntary disclosure.
Eco-balance reporting	Some companies, especially from Europe, construct a formal eco-balance – detailed account of inputs and outputs from which performance indicators are derived.
Performance based reporting	This is probably the most common type of reporting used by most organizations. Significant areas of environmental impact are considered, performance targets set , indicators developed and progress disclosed regularly.
Product reporting	The environmental attributes of a product are evaluated, and in this case the producer responsibility goes beyond the production process itself. You see an example of this in the video case study "What's in a car?"
Environmental and social reporting	Increasing pressure to widen the scope of corporate public accountability drives many organizations to include social data such as employee statistics and working conditions in their reports.
Sustainability reporting	This stage beyond environmental and social reporting involves integrating environmental, social and economic disclosure in a single report.

Worldwide, stand-alone environmental reports or broader sustainability/social responsibility reports are becoming increasingly important as a tool in communicating with and engaging stakeholders.

The concept of public environmental reporting originated from the 1992 United Nations

Conference on Environment and Development (UNCED), the Rio Earth Summit. The Earth Summit was the first major international discussion of sustainable development as a serious global issue. Agenda 21, the "action agenda", which emerged from the Earth Summit, identified "community right-to-know" as a matter for consideration in developing environmental policy.

It recommended that organizations be transparent in their operations and report annually on their environmental performance. An organization is essentially a function of its stakeholder groups, including its employees, shareholders, the public, regulators, contractors/suppliers, customers and other interested external parties, who have varying objectives and expectations that need to be satisfied. The measurement and reporting of environmental performance is becoming increasingly important in order to satisfy the expectations of such stakeholder groups. Managers in a business activity with major incident potential have to respond to emergencies within their own organization. In effect, if an incident occurs, the organization is itself in a crisis, with functionality impaired. Corporate governance embraces all of this.

Companies should ensure that they have a sound system of internal control and effective risk management processes which are regularly reviewed by the board. The entire system, including risk management processes, must be specifically reviewed for effectiveness by the board at least on an annual basis. Time and effort spent on emergency planning may not make an immediate contribution to profits, even though in the long term it may be essential to allow the organization to survive a crisis. Planning also includes measures to prevent emergencies arising or escalating. These will certainly limit the ability of managers to take short cuts or override procedures to overcome temporary difficulties in order to maintain production. Such restrictions are often seen as unnecessary nuisances – until something goes wrong. Then it is essential to address the problem quickly, openly and effectively.

Various incidents with significant negative impact on shareholder value are indicated in Table 52.3. The Open University distance-learning course "Integrated Safety, Health and Environmental Management" includes several of these incidents as video case studies and deals extensively with emergency preparedness.

The Perrier incident is a classic example of a performability failure in which a product fails to "satisfy the requirements of a customer", and the way this failure is managed can affect company value. At the Mecklenburg County Environmental Protection Department in North Carolina, scientists used bottles of Perrier sparkling mineral water as a "pure" standard for water analysis rather than purifying water themselves. On January 19, 1990 an anomalous mass spectrometer reading indicated a corrupt sample. Perrier water had consistently been a reliable source and so faulty instrumentation was suspected, but it was found that the Perrier contained between 12.3 and 19.9 ppb of benzene. This was above the 5 ppb limit specified by America's Food and Drug Administration (FDA) but below levels that might present a health risk. Perrier were alerted to the problem, and while the concentrations of benzene did not pose "a significant short-term health risk" according to the FDA, nevertheless the company acted to protect its brand image of purity. Initially, Perrier claimed that the contamination was an isolated incident due to cleaning fluid containing benzene used on a production-line machine and only drinks in the US were affected. It recalled over 70 million bottles from US shops and restaurants. Unfortunately, the real cause was found three days later when contaminated bottles appeared in Denmark and the Netherlands, and Perrier revised its explanation, admitting that benzene was naturally present in carbon dioxide (the gas that makes Perrier effervescent) but filtered out.

The normal processing method for Perrier was to remove such impurities by passing the mineral water through carbon filters. A faulty warning light on a control panel went either undetected or unreported by employees for more than six months, allowing the filters to become blocked and no longer function. Amid growing consumer mistrust, a further 90 million bottles were withdrawn globally at an estimated loss of $263 million. Through 1991, Perrier struggled to recover. Its overall sales had declined for a second year together with the share price, around half from a high of nearly FF2000 per share prior to the benzene affair (Figure 52.3).

Table 52.3. The costs of some performability failures to businesses

Date	Company	Incident	The costs
1982	Johnson & Johnson	Product tamper and recall of 31 million bottles of Tylenol capsules (known in the UK as paracetamol) after an employee injected cyanide into some capsules, resulting in seven deaths. Advertizing and product distribution were halted. A tamper-resistant pack was designed and the product was relaunched a few months later.	In 1991, the families of the seven victims reached an out of court settlement with the company. The cost of the recall was estimated at $100 million and $50 million for business interruption losses. The company sued its insurers for $67,4 million in 1986, but lost the case.
1984	Union Carbide	Liability from the Bhopal incident.	Over $527 million
1986	Sandoz*	Fire and pollution Rhine	$85 million
1987	P&O*	Liability Zeebrugge	over $70 million
1988	Occidental*	Fire and explosions Piper Alpha	$1,400 million
1989	Exxon	On March 24, the Exxon Valdez oil tanker ran aground, spilling more than 10 million gallons, of oil into Prince William Sound, Alaska. Efforts to contain the spill were slow as was Exxon's response. The Exxon name tends to this day to be synonymous with an environmental disaster.	The cleanup cost the company $2.5 billion with $1.1 billion in various settlements. A 1994 court case also fined Exxon a further $5 billion for its recklessness, which Exxon later appealed. In addition to the direct costs of the disaster, Exxon's image was tarnished, perhaps permanently.
1990	Source Perrier	Product recall benzene carbon filters intended to remove benzene, a carcinogen, became clogged, and this went undetected for six months. No one suffered as a result of drinking the benzene-contaminated water, but Perrier was forced to recall 160 million bottles from 120 countries. There were contradictory statements from management on the extent and cause of the contamination.	Eighteen months after the incident, Perrier's share of the sparkling water market fell from 13% to 9% in the US, and from 49% to less than 30% in the UK. The cost of the recall was $263 million. The share price fell (see Figure 52.3) and the company became a takeover target. In July 1992 it was taken over by Nestle.
2001	Bridgestone/ Firestone Inc./ Ford	The recall of 16 million Firestone Wilderness AT tires in August 2000 was followed in 2001 by the US government requesting another 3.5 million Firestone tires to be recalled for safety checks by Ford, which used them on sports utility vehicles. Treads on several models were found to be separating from the tires. The tires were believed to be the cause of rollover crashes resulting in 203 deaths and over 700 injuries.	Firestone spent more than $350 million for the recall with potentially more in legal cases and a loss in public confidence of the product. The Bridgestone share price dropped from over Y2500 to below Y1000.

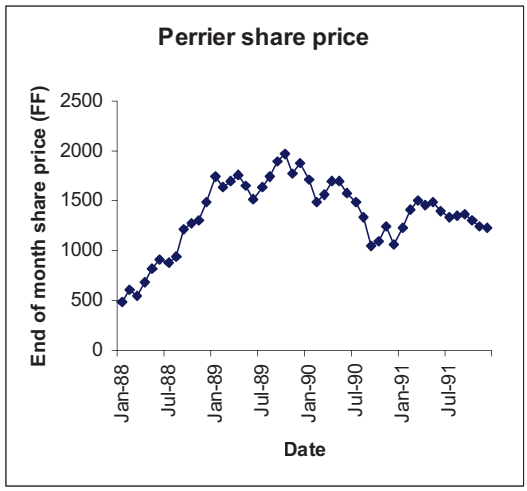


Figure 52.3. How an incident can affect share price

Another example relates to a rail incident. On 10 May, 2002 a train traveling from London Kings Cross derailed at Potters Bar when passing over points 2182A. Three of the four carriages derailed and one ploughed along the platform and struck a bridge. There were 7 deaths and over 70 people were injured. The formal inquiry report by the Rail Safety and Standards Board [9] and the Health and Safety Executive [10] concluded *inter alia* that

- Failure of points 2182A caused the derailment.
- Components in the points were in a poor condition.
- Nuts on the points were missing.
- The points had been poorly maintained and were not adjusted correctly.
- Other sets of points in the Potters Bar area were found to have similar, though less serious, maintenance deficiencies.
- Other sets of points showed evidence that attempts had been made to improve the retention of nuts, suggesting there had been difficulties in the area with such nuts loosening.
- There appears to have been no guidance or instructions for setting up, inspection or maintenance of points of the 2182A type.
- There appears to have been a failure to recognize, record or report safety-related defects in the set up and condition of points 2182A.
- There were deficiencies in response to a report of a rough ride near the points south of Potters Bar station the night before the derailment.
- Wider inspections of a sample of similar points across the rail network found conditions that were not consistent with good engineering practice. The deficiencies were less serious than those at Potters Bar.

These are clear performability failures. The Potters Bar incident had an impact on the share prices of companies involved in rail track maintenance (Figures 52.4a and b below), while companies operating in the same market sector but without rail involvement showed no comparable decline (Figures 52.4.c and d).

Studies have found that this fall often amounts to almost 8% of shareholder value and while recovery tends to occur in fifty trading days or so, the ability to recover varies considerably [11]. Some argue that if the price falls below a threshold, recovery is impossible. The impact of such incidents on companies' share prices come from the direct financial cost of the incident in terms of cash flow, with the market adjusting the stock price accordingly. Then the market adjusts the share price in accordance with its assessment of the way management handled the incident.
Important lessons come from these incidents.

First, that reputation can be harmed at an instant, but can be protected by planning for an emergency and dealing with communication issues well. Timeliness is a major factor in any emergency situation. The Johnson and Johnson incident in 1982 provided a model that a company was expected deal with the actual problem well and create a positive image of how the problem is handled. In contrast, Exxon was unsuccessful in both. While claiming that addressing the pollution was its first priority, company officials took what was regarded as too long to deploy booms to contain the spill.

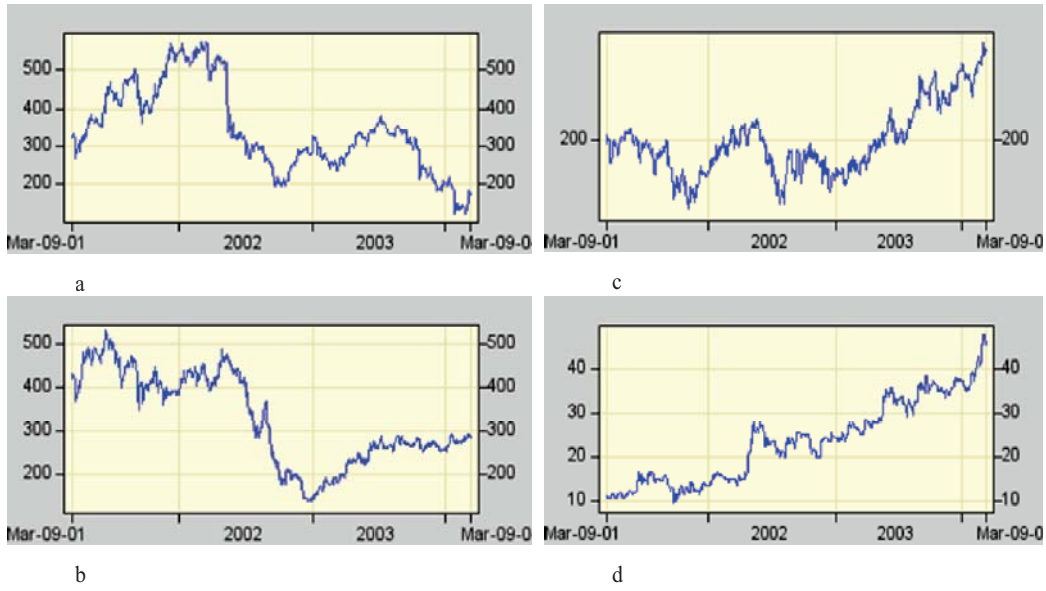


Figure 52.4. Share prices of selected companies following the Potters Bar rail crash

In addition, Exxon was criticized for refusing to acknowledge the extent of the problem, in part, due to the advice of legal counsel – a not uncommon factor in view of potential future liability claims. Company representatives also refused to comment on the incident for almost a week, while the chief executive took six days to make a statement to the media and did not visit the scene until nearly three weeks after the spill. When added together, these actions gave the public the impression that the Exxon Corporation did not take this accident seriously.

52.6 Meeting Some Educational Challenges

In the context of cleaner production referred to earlier in this chapter, a recent study [12] found that, on average, the production and provision of distance-learning courses consumed nearly 90% less energy, and produced 85% fewer climate changing carbon-dioxide emissions than conventional full-time campus based university courses. The much lower environmental impacts of distance learning compared to campus-based courses is mainly due to a major reduction in the amount of student travel, economies of scale in utilization of the campus site, and the elimination of much of the energy consumption of student housing.

The study also compared e-learning courses to print-based distance learning courses.

It showed that e-learning courses offer only a relatively small reduction in energy consumption (on average 20%) and CO_2 emissions (12%) over print based distance learning courses. This was attributed to high student use of networked computing, consumption of paper for printing of web-based material, and additional home heating for night time internet access. This study challenged claims about the "de-materialization" effects and environmental benefits of using ICT to provide services such as higher education.

Table 52.4. Student analyses of corporate environmental reports for variables

Specific variables	BNFL	Envir. agency	Waste & recycling	Agro chem	Aero space	Car industry	Proctor & Gamble
Environment policy and systems	62	15	16	16	15	212	37
Environmental audit	4	37	29	6	14	38	12
Pollution control in the conduct of business operations	64	8	9	20	15	73	23
Prevention or repair of damage to the environment from processing of natural resources	6	10	2	7	7	22	10
Conservation of natural resources	8	33	14	10	18	95	35
Promoting sustainable development	10	25	6	14	4	5	13
Design for environment	6	16	14	0	1	48	24
Other disclosures relating to the environment	14	2	14	12	12	89	4
Conservation of energy in the conduct of business	4	11	3	6	7	54	15
Energy efficiency of products	0	1	2	0	1	31	3
Alternative energy sources	0	13	4	0	0	4	18
Other energy-related disclosures	8	1	3	0	2	1	8
Safety	0	2	0	18	7	11	12
Reducing pollution arising from use of product	2	1	0	6	2	38	3
Product development	0	0	3	23	1	102	5
Other product-related disclosures	0	2	0	3	2	24	3
Other disclosures	0	0	3	0	0	11	0
Number of environmental sentences	188	178	122	143	111	858	225

Table 52.5. Student analyses of corporate environmental reports by sector

Company	Sector	No of employees	Total No of Env sentences	Expressed as a percentage of the number of sentences in the report						
				Environmental sentences	Monetary sentences	Quantitative	Qualitative	Neutral news	Good news	Bad news
Balfour Beatty	Construction, facilities Mgmt	27 000	241	33	1	58	33	34	53	12
McAlpine	Construction, Facilities mgmt	11 000	184	87	1	21	12	14	70	3
Coca Cola	Soft drinks manufacture	50 000	505	63	1	21	40	48	51	1
Unilever	Food, home and personal product manufacture	227 000	210	49	0	30	58	24	67	9
Sainsbury	Food retail	172 000	468	77	3	16	5	75	23	2
Tesco	Food retail	360 000	141	84	5	35	29	25	72	3
Co-op	Banking	4147	140	36	4	51	20	48	42	10
LloydsTSB	Banking	66 000	127	57	0	35	10	53	42	5
Vodaphone	Mobile telecoms product/services	57 378	82	61	1	2	10	19	76	5
Coryton (BP)	Oil refinery	600	125	60	1	29	8	28	25	8
Severn Trent	Water, waste Environmental services	17 000	212	60	1	23	56	50	40	10
First Group	Travel and transport	67 000	135	80	3.7	34	47	45	46	9
Glaxo SmithKline	Pharmaceutical research	110 000	523	80	1.2	20	33	74	17	9

The environmental impacts of a service depend mainly on its requirements for travel and a dedicated infrastructure of buildings and equipment.

The use of ICT or other methods will only benefit the environment if they reduce the service's requirements for energy-intensive transport, dedicated equipment and heating and lighting of buildings. Distance education can do this and is, therefore, an approach that offers many opportunities and efficiencies [13]. It can help avoid some of the seemingly "wasteful" aspects associated with conventional approaches to education and training.

However, distance learning is not without its challenges and one of these is in relation to group activities. Nevertheless, ICT can help here through the use of course conferencing facilities. Another postgraduate course "Enterprise and the environment" seeks to develop such group activity through

the analysis of corporate reports to which students can readily gain access. Students select an organization for study, analyse corporate reports by content analysis and then compare their findings with those of their peers using the course electronic conference. This provides opportunities for different interpretations from content analysis of the same report as well as allowing comparisons in and between industry sectors.

Table 52.4 shows some findings of a student cohort examining reports for mention of specific variables linked to performability, while Table 52.5 compares various sectors. Students commented that the amount of good news reported far outweighs the bad in all sectors. In addition, food manufacturers and banks appear to write more quantitative than qualitative sentences. Perhaps companies make more environmental disclosure where they recognize the sensitivity of the business to reputation damage through the amplification of risk, and certainly this applies to food industries where there have been numerous incidents.

This assignment provides an appropriate and challenging alternative to the conventional business-based project, which in the course is available as an optional audit activity.

52.7 Conclusion

Performability is the holistic view of designing, producing and using a product, system or a service to satisfy the requirements of a customer to the best possible extent. Failures in any respect may put the organization at risk and the significance of that risk depends on the perceptions of stakeholders. Organizations are therefore under increasing pressures to identify, assess and manage their risks.

Inevitably problems occur, but by identifying potential risks, organizations can be ready to deal with the consequences to themselves and their stakeholders. If an incident does occur, appropriate dialog with stakeholders can help minimize the loss to the organization. The social amplification of risk framework relates to both potential impact and the challenges in changing behaviour.

Making engineering students aware of these issues is an important feature of modern engineering education and reflects the holistic approach inherent in the performability concept.

References

[1] Selwyn J, Leverett B. Emerging markets in the environmental industries sector. Department of Trade and Industry, Environmental Industries Unit, Report BPR 394, 2006.

[2] Cleaner production and eco-efficiency. Complementary approaches to sustainable development. World Business Council for Sustainable Development and United Nations Environment Programme, 1998; 3.

[3] International Journal of Performability Engineering, http://www.ijpe-online.com.

[4] Internal Control. Guidance for directors on the combined code. The Institute of Chartered Accountants in England and Wales, London, 1999; ISBN 1 84152 010 1

[5] BSI Management Systems. http://www.bsi-emea.com/index.xalter.

[6] Kasperson RE, Ortwin R, Slovic P, Brown H, Emel J, Goble RL, *et al.*, The social amplification of risk: A conceptual framework. Risk Analysis 1988; 8(2): 177–187.

[7] Breakwell GM, Barnett J. The impact of social amplification of risk on risk communication, HSE Contract Research Report, 2001; 332, HMSO London, ISBN 0 7176 1999 0.

[8] Holgaard JE. Environmental communication in business relations. Working Paper 12, Department of Development and Planning, Aalborg University, Denmark, 2006.

[9] Rail Safety and Standards Board, http://www.rssb.co.uk/formal_2005r.asp

[10] http://www.rail-reg.gov.uk/upload/pdf/incident-pottersbar-interim.pdf

[11] Knight RF, Pretty DJ. The Impact of catastrophes on shareholder value. Oxford Executive Research Briefings, Templeton College, University of Oxford, 1997, http://www.nrf.com/Attachments.asp?id=12546

[12] Roy R, Potter S, Yarrow K, Smith M. Towards sustainable higher education: Environmental impacts of campus-based and distance higher education systems. Open University Design Innovation Group, Faculty of Technology, the Open University, UK, 2005.

[13] Barratt RS. Performability: pedagogical perspectives. International Journal of Performability Engineering 2006; 2:61–74.

53

Towards Sustainable Operations Management
Integrating Sustainability Management into Operations Management Strategies and Practices

Alison Bettley and Stephen Burnley

Faculty of Technology, The Open University, Walton Hall, Milton Keynes, MK7 6AA, UK

Abstract: Sustainability is an increasingly relevant issue for a wide range of organizations, and therefore sustainability management strategies and practices are of growing significance. Because many sustainability impacts are strongly influenced by operations management decisions it is critical that the operations management function embraces the requirements of sustainability management. This has implications for decisions and processes associated with all aspects of operations management including strategy, design, planning and control, and improvement. For example, appropriate environmental and social performance objectives, targets and indicators need to be integrated with quality, cost and other more conventional performance measures. The closed loop supply chain perspective must be adopted and the requirements of other stakeholders in addition to the customer must drive operations decisions. The scope of any given "operation" is thereby expanded considerably and the nature of the operations management role altered, with implications both for the professional development of managers and the research needed to support the manager in this changed role.

53.1 Introduction

Over the last two decades there have been growing pressures for organizations to reduce their environmental impact and move towards "sustainability". The main driving forces for this shift [1–9] can be summarized as:

- competitive pressures, arising from:
  - recognition of the cost advantages of reducing materials and energy consumption and waste production,
  - cost benefits of taking advantage of the economic incentives of green behavior such as subsidies and reduced taxation,
  - the increasing pressures from customers (end consumers and supply chain partners) to demonstrate good environmental stewardship,
- the perceived marketing advantages from demonstration of compliance with standards and so on;
- legal obligations, in a climate of increasing regulation as scientific evidence for human influences on climate change, ozone depletion and so on hardens;

- the demands of investors for security from future liabilities consumer demands and expectations of ethical behavior and good corporate citizenship in the wake of scandals such as Enron;
- internal ethical values, reflecting changed values in society as a whole.

These pressures can and do translate into tangible benefits for the organizations that choose to respond to them – reduced costs, increased market penetration and market share, increased levels of investment, improved brand reputation, new products and markets, and enhanced customer satisfaction.

As more and more organizations recognize these opportunities, adoption of environmental management (ISO 14001 and similar) standards alongside quality management standards (ISO 9001) has become relatively commonplace. The next generation of management systems and standards will embrace sustainability more fully, by integrating social, environmental and economic objectives.

The operations function of the organization is concerned with the arrangement of resources devoted to the production and delivery of the organization's products (goods and/or services) [10]. As such, it is the "engine room" of the organization, and therefore directly responsible for a large proportion of the decisions and the activities that give rise to environmental problems. The design and management of operations strongly influence how much energy and materials resources are consumed in order to manufacture goods or deliver a service. Operations decisions are also partly responsible for how easily an item can be recycled, and the nature and extent of emissions and wastes produced during both a product's manufacture and its use. The solutions to many environmental problems, as well as the causes, therefore lie fairly and squarely in the operations management domain. Similarly operations decisions and activities have a profound impact on many of the wider concerns of sustainability such as those associated with working conditions and practices both internally and in the supply chain. Therefore, if "sustainability" is to become any type of reality, it is critically important that operations management embraces the necessary strategies and practices. This chapter explores the ways in which traditional operations management must develop in order to do just this and to play a full and effective role in progress towards sustainability, for all types of organizations.

The chapter is organized as follows. First, the nature of sustainability itself is explored. Then the scope of "operations" as it needs to be defined for the purposes of sustainability management is discussed. This then forms the basis for a discussion of the ways in which the traditional subdivisions of operations management need to be expanded to incorporate sustainability. Finally the implications for organizations, their operations and operations managers and for the research agenda are identified.

53.2 Sustainability

The conventional definition of sustainable development is "development that meets the needs of the present without compromising the ability of future generations to meet their own needs" [11], although this tends to be interpreted differently in different contexts. Typically at present in industry it is environmental sustainability that is the focus of attention, but sustainability is actually a rather wider concept comprising a broad set of "quality of life" or "corporate social responsibility" measures embracing financial, social and environmental concerns [9, 12–14]. Corporate social responsibility (CSR) has been defined as "the continuing commitment of business to behave ethically and contribute to economic development while improving the quality of life of the workforce and their families as well as of the local community and society at large" (World Business Council for Sustainable Development, 1999, quoted in [15]). This is sometimes referred to as the "three pillars" of economic, social and environmental responsibility, the three Ps of "profit, people and planet" or as the "triple bottom line" (TBL) [16] by organizations adopting sustainability goals and seeking to report their progress to internal and external stakeholders. The very broad scope of sustainability management is illustrated by the BT case study in the box below.

The British Standard on sustainability management defines sustainable development as "an enduring, balanced approach to economic activity, environmental responsibility and social progress" [21]. An important practical implication of this is that simplistic judgments relating to one element alone cannot be made. Decisions must be taken in a way that integrates all these concerns [22], and this means taking into account the concerns of stakeholders from outside the organization as well as within it. This requires proactive steps to engage the relevant stakeholder groups to determine their interests and expectations. This is discussed in more detail in Section 53.3.

Guidance for managers wanting to adopt sustainability management exists or is emerging in the form of various voluntary management standards:

- BS 8900 Guidance for management of sustainable development [21].
- Social Accountability standard SA 8000 [23].
- ISO 26000, a forthcoming standard on sustainability management [24].
- GRI Sustainability Reporting Guidelines [25].

The British and ISO standards explicitly recognize that organizations are likely to want to integrate sustainability management with pre-existing quality and environmental management standards, and the content reflects this.

The extent to which "sustainability" can actually ever be "achieved" is a moot point, especially at the level of an individual enterprise or industry [26]. The many qualitative aspects it embraces militate against any absolute measurement, so that it is meaningless for any business, city or nation to declare itself a sustainable operation. Perhaps it is best considered as analogous to such notions as the well-known quality management "zero defects" concept, an aim around which processes are managed in order to achieve as close to a state of perfection as possible. For example, while the burning of coal to generate power is clearly unsustainable because of the depletion of finite resources and release of carbon dioxide, it is reasonable to consider a combined heat and power plant as being "more sustainable" than the less efficient power-only process.

However, there is at least one significant difference between quality and sustainability management, and that is the complexity associated with the assessment of sustainability, the number of different "measures" it embraces, the impossibility of quantification of a significant proportion of these, and the subjectivity of the judgments. Many attempts to provide the definitive set of sustainability indicators have been made [25, 27, and 28]. The GRI guidelines [25] are becoming established as a significant benchmark, see Table 53.1.

Case Study: BT's Corporate Social Responsibility Strategy

British Telecommunications Plc (BT) (a UK based telecommunications company) has a strong track record in corporate social responsibility management and reporting,it rates consistently highly in the Dow Jones Global Sustainability Index [17] and summarizes its current strategy as follows [18]:

"…to maintain our current momentum in CSR and to focus our efforts on the three biggest challenges:

The need for sustainable economic growth

The need for wider inclusion of all sections of society

The need to tackle climate change."

BT measures its performance and sets annual performance targets in all the following categories [19, 20]:

Customers

Customer satisfaction

Employees

Employee engagement

Diversity of the workforce

Health and safety: lost time injury rate; sickness absence rate

Suppliers

Supplier relationships

Ethical trading

Community

Community contribution

Environment

Global warming CO_2 emissions

Waste to landfill and recycling

Digital Inclusion

Geographical reach of broadband

Integrity

Ethical performance measure

Its annual report follows Global Reporting Initiative guidelines and provides a detailed account of its targets and progress towards them, all set out in relation to its strategic "business principles". The importance of "stakeholder dialog" and "engagement" is stressed throughout, with respect to the following six stakeholder groups: customers, employees, suppliers, shareholders, partners, community.

Whether or not any notion of absolute „sustainability" is practically attainable, it is always feasible to move nearer to it by designing and managing operations appropriately, for example, to reduce the environmental impact of an operation, or to have policies towards supply chain partners that promote good employment conditions.

This requires in the first instance appropriate definition of the scope of the operation so that all the impacts that flow from the operation are taken into account. The principles of life cycle thinking based on the technique of life cycle assessment (LCA) require that the environmental impacts of each and every stage in a product's life from materials extraction to product use and disposal are appraised (see Figure 53.1). The LCA process consists of three stages [29]:

- compiling an inventory of relevant inputs and outputs of a product or system,
- evaluating the potential environmental impacts associated with those inputs and outputs,
- interpreting the results of the inventory analysis and impact assessment phases in relation to the objectives of the study.

Table 53.1. Aspects of sustainability [25]

Economic
Economic performance
Market presence
Indirect economic impacts
Environmental
Materials
Energy
Water
Biodiversity
Emissions, effluents and waste
Products and services
Compliance
Transport
Overall
Social
Labor Practices and Decent Work
Employment
Labor/management relations
Occupational health and safety
Training and education
Human Rights
Investment and procurement practices
Non-discrimination
Freedom of association and collective bargaining
Abolition of child labor
Prevention of forced and compulsory labor
Complaints and grievance practices
Security practices
Indigenous rights
Society
Community
Corruption
Public policy
Anti-competitive behavior
Compliance
Product responsibility
Customer health and safety
Product and service labeling
Marketing communications
Customer privacy

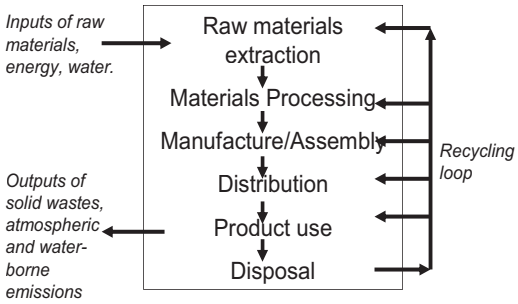


Figure 53.1. Product life cycle

The practical use by organizations of LCA's scientific principles is known as life cycle management (LCM); this is emerging as an important area of research and practice [30] in its own right [31, 32]. It demands as a first step a definition of the system under scrutiny: what should be included within its boundary and what can safely be left out? The scope of the operations system is discussed next.

53.3 Operations as a System to Deliver Stakeholder Value

An operation can be defined as a set of business processes that are directly responsible for converting a variety of resources (such as materials, money and the effort of people) into outputs (such as manufactured goods and/or delivered services) made available to customers. This classic transformation model of operations is shown in Figure 53.2.

Recent thinking in operations management has placed emphasis on taking the "supply chain perspective" so that internal processes are seen as links with external suppliers upstream and customers downstream. In this way issues such as outsourcing can be managed as part of the bigger picture to provide value for customers. Operations can then be represented as in Figure 53.3.

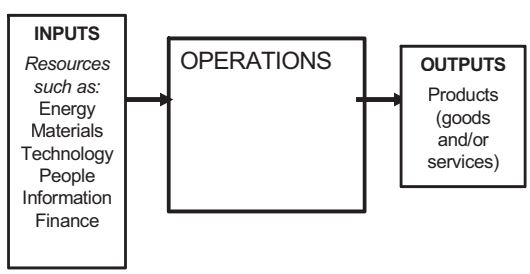


Figure 53.2. The transformation model of operations

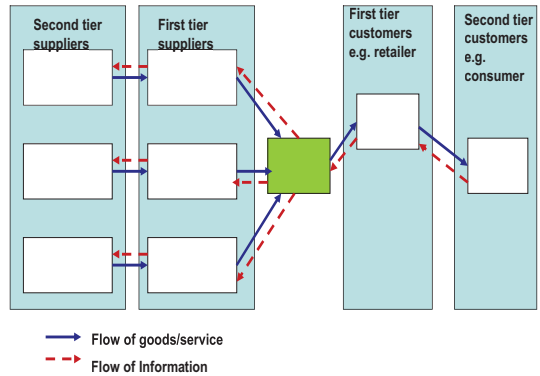


Figure 53.3. Supply network perspective of operations (adapted from [10])

Table 53.2. Stakeholders and their expectations

Stakeholder group	**Examples of expectations/interest – the value they seek from the operation**
Customers (internal or external)	Benefits from use of products/services Value for money.
Suppliers	Contracts Fair dealing
Managers/directors	Profit Fulfilment of organizational mission.
Other employees	Employment security Job satisfaction Good working conditions. Fair remuneration
Owners and other investors	Growth in value. Dividends.
Regulators	Compliance with regulation Performance improvement
Government	Taxes
Local community	Environmental stewardship Employment opportunities Community involvement
Society at large	Contribution to general economic well being Ethical behavior

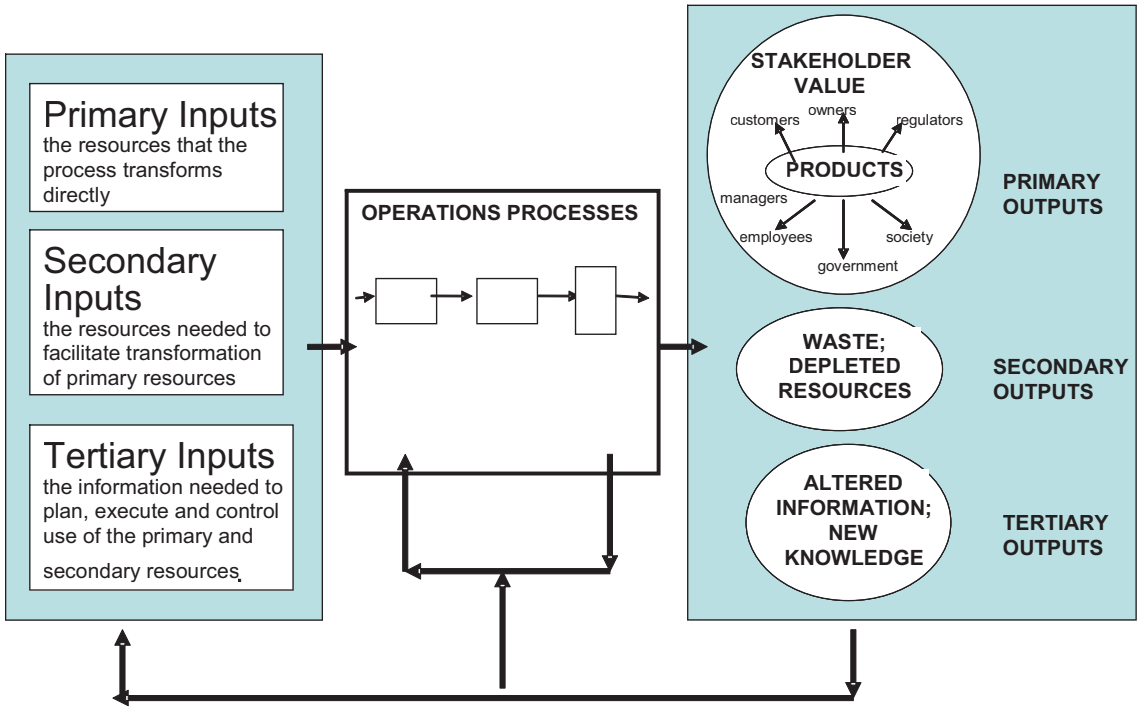


Figure 53.4. Expanded transformation model of operations

To integrate sustainability management with operations management this supply chain perspective must be extended in two linked ways.

First it is insufficient to consider the output of the operation only in terms of the value derived by the customer from the goods and services delivered by the operation. A wider set of stakeholders must be taken into account [33]. Stakeholders are individuals or groups with some sort of interest in the activity, in this case the operation. Typical stakeholders are listed in Table 53.2 along with their likely expectations of the value they seek from the operation. It is delivery of "stakeholder value", the total of the various elements of value sought by all stakeholder groups, including customers [34, 35], that might better define the overarching objective of operations management, as shown in the expanded transformation model of Figure 53.4.

To meet the needs of these various and diverse stakeholder groups, it is self-evidently necessary to understand them first, and this requires processes within the operation to engage stakeholders in an appropriate dialogue, as is specifically recommended in the British Standard on managing sustainable development [21].

Most organizations will have such processes for becoming "close to the customer" (for example, quality management tools such as QFD, or customer relationship management systems). Many may have employee consultation bodies and processes, and most will meet with and report to their shareholders. Other stakeholder groups, however, may be relatively neglected.

The "stakeholder capitalism" concept [36] builds on the stakeholder theory of the firm first developed in the 1980s and stresses the need for collaboration among supply chain partners and other interested parties. Emphasis is placed on the importance of devising and maintaining a suitable value system "architecture" to facilitate and nurture *cooperative* value creation. The entire process might be framed as stakeholder relationship management [33, 34, 37]. An important

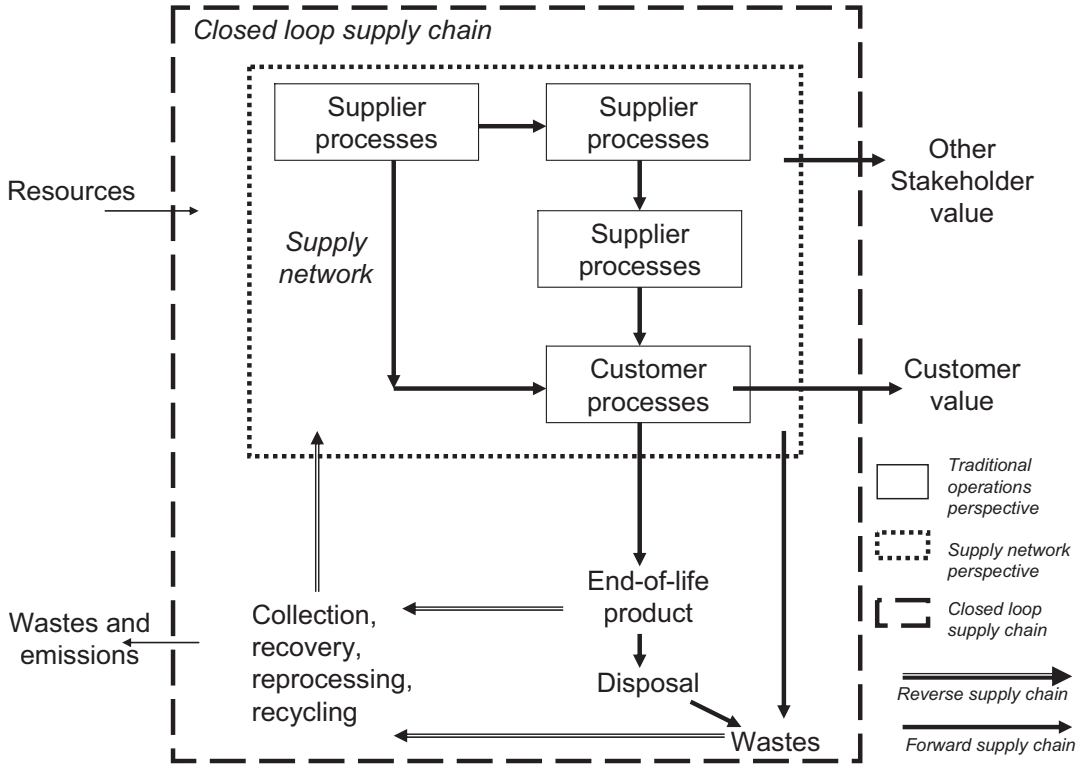


Figure 53.5. Closed loop supply chain in relation to other operations perspectives

implication of this stakeholder-focused thinking is that there is need for substantial change to traditional patterns of working across intra-organizational and inter-organizational boundaries.

The second point follows from this integrated and collaborative supply chain model, that it is necessary to consider a more complete "product system" than even the typical operations supply chain perspective embraces in order to deliver all these aspects of stakeholder value. Traditional supply chains are "forward" supply chains, ending at the point of delivery to the customer.

But if other stakeholders such as society at large are considered then this view is too restricted. The impacts arising from each and every stage in the product life cycle must be considered (see Figure 1). The "reverse supply chain" including product take-back for recycling, final disposal, waste treatment, and so on must be included in what is becoming known as the "closed-loop supply chain", for obvious reasons [38–42]. This is depicted in Figure 53.5.

An application of closed-loop supply chain thinking in the construction industry is given in the box below.

Moreover sustainability embraces more than environmental concerns so the impacts on employment, economic well-being of communities, ethical behavior and so on (as listed in Table 53.1) must also be integrated into the model. The "total product system" perspective advocated by Rhodes adopts this type of extended view, embracing after-markets, the end-of-life phase of the product life cycle and social and labor conditions associated with the various supply chain stages [43].

The "life cycle management" problem facing managers can therefore be framed as how to design and implement sustainable production systems

based on a consideration of all the various sustainability impacts of each stage in the closed loop supply chain [31, 32, 44]. The practical difficulties are manifold: vast quantities of data, different data from different sources, gaps in data, different methods of data aggregation, lack of established methods of measurement, the need for value judgments to decide which issues are priorities, the need for collaboration among all partners in the supply network, and so on. This field incorporates aspects of supply chain management and industrial ecology [31].

Industrial ecology applies the principles of natural ecology to eliminate wastes, cycle elements from end-of-life products to new products, minimize the storage of materials and intermediate products (particularly hazardous materials) and circulate energy within and between processes to minimize external energy inputs. These aims are often achieved by the co-location of processes (operated by one or more organizations) to the mutual benefit of all concerned. See [45], for examples of industrial ecology or symbiosis in practice.

The overall aim is to optimize the sustainability performance of the product system overall, but the feasibility of the business model must also be considered [42], as in the steel section case study as follows:

Case Study: Recycling and Reuse of Structural Steel Sections [38]

Steel is the most recycled material in the world – the technology to handle and return to the primary production processes many different grades of scrap (there are 29 in all) is well-developed. It is estimated that structural sections are recovered from demolition waste with 99% efficiency in the UK. 86% is "recycled" (demolition steel scrap forms the raw material for foundries and electric arc furnaces) and 13% is "reused" (reclaimed and end-of-life sections from building deconstruction which are then refabricated without the need for resmelting).

The opportunities to improve the sustainability of the construction sector through increased steel section reuse are being recognized, there are significant environmental and economic benefits of reuse. The results of a life cycle inventory (LCI) of the processes involved in each of the three main production routes can be summarized as follows [38].

Production route	Life cycle cost £/ton	Total energy requirement GJ/ton
Primary	1040	37
Recycling	950	18
Reuse	680	7

Energy consumption is used as the environmental indicator because analysis of the LCI data shows it is a good proxy for overall environmental performance. It is clear that reuse offers much higher economic and environmental benefits than recycling. However it cannot be assumed that this scale of benefits can be achieved with increased rates of reuse. Constraints on the supply loop are likely to exist, such as the following considerations.

How feasible is deconstruction rather than demolition for most end-of-life buildings?

The demolition industry is geared up for low cost rapid removal of end-of-life buildings, and buildings are not generally designed for deconstruction. Moreover deconstruction is more labor intensive with associated health and safety concerns. It seems likely that as reuse rate increases the costs will also increase, because those buildings most suitable for deconstruction will be chosen first.

How feasible is refabrication?

The work associated with preparation of reclaimed sections for refabrication will vary widely depending on the condition of the sections. The amount of preparation work will increase with reuse rate as the availability of the best quality reclaimed sections reduces.

Is there a big enough market demand for re-fabricated sections to warrant expansion in reuse?

Many of the customers for reclaimed sections expect the cost to be less than that of new parts. If they are similarly priced, customers tend to buy new to reduce perceived risk. However there is a small group of environmentally aware customers who perceive added value in the increased sustainability of reclaimed sections provided they are cost neutral.

It can be concluded that although the environmental benefits remain as indicated by the data given above, the cost savings associated with reuse are likely to fall as the reuse rate increases, making the business case for more reuse less certain.

53.4 Integration of Operations and Sustainability Management

There are several reasons why it is essential to integrate sustainability management decisions with operations management:

- Many of the decisions that affect sustainability are strategic long term ones rather than day-to-day planning and control. It is well-established, for example, that maximum environmental benefits are gained from treating the problem at source (use of an alternative less polluting material, for example) rather than at "end-of-pipe". Therefore sustainability objectives must be considered alongside other performance objectives when devising operations strategy and designing a process or product.
- In the same way that "quality" concerns must become embedded in normal working practice and organizational culture to be effective, so too must sustainability objectives and practices. All employees must be involved and have a thorough understanding of how their activities and responsibilities impact on sustainability performance.
- Operations management at all levels involves a variety of trade-off decisions requiring integration of several factors. Sustainability concerns need to sit alongside others when the relevant decisions are made.
- All aspects of operational performance should preferably be integrated into a single management system (*e.g.*, quality, sustainability, health and safety) so as to reduce the administrative overhead and potential confusion arising from multiple systems.

Many authors have considered issues of interaction and integration between especially environmental sustainability and other aspects of operations management [2, 46–50]. The wider issues raised by consideration of sustainability in the more complete and broader sense have received much less attention to date. However, this can be expected to change. Adoption of sustainable business strategies by organizations will automatically give rise to operations issues to be addressed, see, for example, The discussion by Schmidt *et al.,* of a method to measure the social aspects of sustainability to complement eco-efficiency assessments of BASF products [51].

Kleindorfer *et al*. [50] have documented the various contributions on the subject of "sustainability" to a leading OM journal and identify three groups of interventions:

- Green product and process development *i.e.* the design and development of products and processes that achieve high standards of environmental performance such as reduced energy consumption, ease of recycling and so on.
- Lean and green operations management *i.e.* the planning and control of processes to minimize materials and energy consumption, to address legal constraints and so on.
- Remanufacturing and closed loop supply chains *i.e.* the design of the complete forward and reverse supply chain to address environmental and other sustainability objectives through appropriate recycling and remanufacture.

They define sustainable operations management as "the set of skills and concepts that allow a

company to structure and manage its business processes to obtain competitive return on its capital assets without sacrificing the legitimate needs of internal and external stakeholders and with due regard for the impact of its operations on people and the environment" p. 489 of [50]. The authors note that to date the "people" part of this definition is largely absent from research and recommend that classical models of operations systems are revisited in order to integrate this element.

Sroufe *et al*., identify three sets of "environmental management practices" [52]:

- operational: day to day decisions and practices typically involving shop floor personnel,
- tactical: involving medium term deployment of resources and middle management, such as product design,
- strategic: long-term issues, involving top management decisions about how the firm creates value.

All of these are needed for successful environmental management in the firm as a whole, and many decisions, the authors note, span more than one level.

None of these frameworks sets out the full sustainability agenda for operations management, however. It is timely to identify just how current operations management theory and practice needs to change in order to embrace the full spectrum of sustainability concerns and thereby to enhance organizational performance in this respect. To this end, the requirements of "sustainable operations management" are now discussed in terms of the traditional categories of operations management activities and decision areas as shown in Figure 53.6.

Each of the four elements in Figure 53.6 is significantly implicated by the expanded scope of operations management that the "total product system" or "closed-loop supply chain" perspective demands.

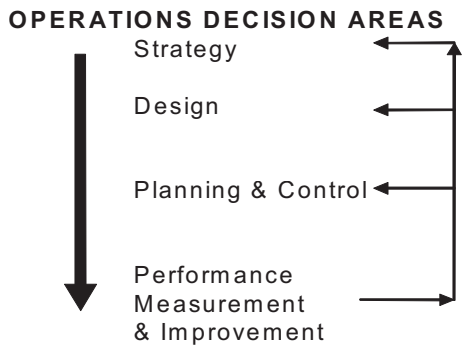


Figure 53.6. Operations management decision areas

53.4.1 Operations Strategy

Operations strategy has been defined as the "major decisions about, and strategic management of: core competencies, capabilities and processes; technologies; resources; and key tactical activities necessary in any supply network, in order to create and deliver products or services and the value demanded by a customer".

The strategic role involves blending these various "building blocks" into one or more unique, organization-specific, strategic architectures [53]. As an example, in order to deliver its overall business strategy of providing low cost stylish furniture to young people and families, furniture retailer IKEA designs and operates a "strategic architecture" consisting of, *inter alia*, the use of innovative designers, and manufacturing and retail systems that expect the customer to do a lot of the work (in-store self-service and home assembly).

Clearly an organization's uniquely designed "strategic architecture" can include provision to meet sustainability objectives. If the organization's overall business strategy includes sustainability then operations strategy, as the means by which business strategy is delivered, must reflect this. Effective sustainable operations management could become a core competence of the organization, and as such a driver of business strategy rather than merely the vehicle for its implementation [50, 54, 55].

Development of a "sustainable operations strategy" requires attention to the following:

- new business models,
- the expanded scope of the operation as a "total product system",
- the legal and regulatory regime,
- new performance objectives and indicators,
- the sustainability issues arising from each of the strategic decision areas.

Each of these is now discussed in turn.

New Business Models and Strategies

Re-appraisal of the entire value system, based on consideration of stakeholder value to be delivered, may identify new business opportunities requiring new business and operations strategies. These might include:

- The need to develop new markets for recycled material or products. This is often a very substantial practical barrier to recycling in practice [56].
- "Disintermediation": the elimination of entire processes so as to supply more directly to the end customer. This is the basis of so-called direct business models typified by the low cost airlines such as EasyJet, and insurance companies such as DirectLine.
- "Servicization": the provision of a service-based product to replace a goods-based product to fulfil a customer need, sometimes referred to as a "product-service system" [57–60]. A simple example is the leasing of fleet cars instead of their purchase. In the chemical industry a service based approach allows suppliers and customers to enter into a mutually beneficial partnership to reduce chemicals consumption [61]. In business markets there is an increasing trend towards leasing and "installed base" management [50, 62].

These models may not all have environmental protection as a key aim but potentially deliver environmental benefits, reduced costs and improved customer service simultaneously.

Geyer and Jackson [38] offer a model to aid identification and selection of new "supply loop strategies". They suggest that the priorities should be those strategies that simultaneously create both environmental and product value when compared to the primary supply chain. It is important to recognize that the results of any such analysis will change over time as a consequence of changing legislative and economic incentives and even changing perceptions of environmental hazard. What seems unattractive today may look very different tomorrow. Recognition of the dynamic nature of opportunities and strategies to address them is therefore important for managers.

The Expanded Scope of the Operation

The scope of the "operation" itself must be expanded to embrace the entire closed loop supply chain [63]. This means at the very least including additional processes, in particular:

- Processes associated with the reverse supply chain, *i.e.*, product take-back processes (including collection from the customer and distribution to waste disposal or recycling stages via appropriate "warehousing" and sorting facilities); remanufacturing and/or recycling processes; waste handling, treatment and disposal processes.
- Stakeholder engagement processes.

These are discussed in more detail under "operations design" later. Not all of these processes need necessarily be internal to the organization, but they must be considered as part of the extended supply chain. It is important that the operation is considered as an entire system so that its overall sustainability performance is optimized.

Meeting Legal Obligations

An important driving force of business and operations strategy is the political and legal environment in which the organization operates. This part of the business environment has become highly dynamic with respect to environmental and social responsibility, with ever tightening legislation to limit emissions and burgeoning initiatives to provide economic incentives for organizations (and individuals) to protect the

environment. Recent examples from the European Union include making producers responsible for the recycling of packaging, end of life vehicles and waste electronic and electrical equipment. A close watching brief is therefore required so as to be able to anticipate, and respond swiftly and appropriately to, the changing regulatory regime [3]. National regulatory regimes and infrastructures are important external drivers of operations strategy. For example, a comparison of the US and Germany found that the German provision of product take-back infrastructure reduced uncertainty and allowed firms to invest in related technology and processes, whereas in the US with no equivalent infrastructure, firms invested differently, with the objective of achieving greater manufacturing flexibility [64].

New Performance Objectives and Indicators

Conventional operations performance objectives [10] comprise cost, quality, speed, flexibility, reliability. "Sustainability" might form a sixth group, to be defined in detail to suit the needs of the individual organization but embracing environmental, and social objectives, addressing issues such as those listed earlier. Alternatively, it might be argued that at least some aspects of sustainability could be integrated into the "quality" objective, although it is harder to see how social responsibility objectives could be fitted into the existing framework. Other frameworks, such as the "balanced scorecard" approach [65] could similarly be modified to incorporate sustainability [66]. Neely's "performance prism" is unique in explicitly identifying stakeholder interests as a precursor to design of a performance measurement system [67].

Guidance on the choice of environmental performance indicators has been given in ISO 14031 [68]. Three types of indicator are likely to be needed

1) Environmental condition indicators: to reflect the state of the physical environment affected by the organization's activities.
2) Operational performance indicators: to reflect the performance of internal operations with respect to emissions and waste production, waste and energy consumed, and so on.
3) Management performance indicators: to cover aspects of environmental management such as the number of staff trained.

Hervani *et al*. [66] have interpreted this guidance for the performance measurement of "green supply chains". The GRI guidelines [25] also contain guidance on indicators to cover the various aspects of sustainability.

Sustainability Issues in the Strategic Decision Areas

The decision areas comprising "operations strategy" can be divided into two categories, structural (long-term "fixed" features) and infrastructural (more tactical in nature), each with a variety of possible sustainability implications [69] as listed in Table 53.3.

Table 53.3. Structural and infrastructural decision areas and related sustainability issues

Structural operating issues	**Examples of sustainability management issues**
Facilities	Location of facilities close to recycling plant and/or close to markets reduces the requirement for packaging and transportation [70]. Location of facilities in developing countries gives rise to ethical issues such as fairness of wage rates, child labor, and choices as to whether to comply only with local environmental regulation or the higher standards of the home country.
Process technology	Technology investment decisions can favour "sustainable" clean technologies to provide future competitive advantage [50]. Process innovation will be driven by increasingly demanding regulations requiring, for example, reduced emissions and/or more recycling.

Table 53.3 Continued

Structural operating issues	Examples of sustainability management issues
	Energy efficient technologies and those that cut down material waste have the twin benefits of saving direct operating costs as well as enhanced environmental performance.
Capacity	Environmental protection regulations may limit capacity (to limit emissions) unless additional controls are installed or process modifications made. Tradable permits may have a similar effect. Capacity to recycle is likely to become increasingly important as regulations become increasingly stringent regarding the percentage of materials to be recycled.
Vertical integration	The closed loop supply chain demands re-consideration of outsourcing or vertical integration options for supply chain configuration. Outsourcing gives rise to ethical issues in relation to treatment of supply chain partners and their employee relations. Direct business models (such as online insurance or travel booking services) cut out many of the intermediary stages between supplier and end consumer thereby saving a variety of energy and materials resources.
Infrastructural operating issues	
Suppliers	Environmental standards require "green purchasing" policies involving additional criteria to be applied in the selection of suppliers. For example car manufacturers such as Ford and Vauxhall require all their suppliers to carry ISO14001 registration and are proactive in helping suppliers achieve this. Companies are increasingly pooling resources on suppliers in order to protect themselves form poor practices further up the supply chain [71]. "Fairtrade" criteria are also relevant.

Table 53.3 Continued

Structural operating issues	Examples of sustainability management issues
New products	Life cycle thinking must be applied to product design. There may be scope for innovative "product-service systems" to reduce overall impact.
Workforce	Direct involvement of the workforce is essential for effective sustainability management. Organizational culture, and appropriate performance measurement systems play important roles.
Quality and improvement management	Environmental management systems use the same basic continuous improvement "plan, do, check, act" framework as quality management systems and many organizations seek to integrate them to reduce management system overheads. Sustainability objectives should be integrated with others in an overall performance management framework. Risk assessment techniques can play a role in deciding the priority issues for improvement. Deployment of "lean" operations strategies should lead to more resource efficiency and thereby support environmental sustainability, although research indicates that the linkage between "lean" and "green" is rather complex and a lean production strategy does not address all elements of, emissions reduction, for example [72].
Planning and control systems	Conventional planning and control techniques and systems do not embrace sustainability objectives, but in principle MRP, ERP, capacity planning tools and so on could be modified so to do.

Voluntary Standards and Integrated Performance Management Systems

Many organizations see benefits in the integration of management systems, that is incorporating the

requirements of standards such as quality management, ISO 9001 [73], health and safety management, BS8800 [74] and environmental management, ISO 14001 [75] or EMAS [76] in one overall performance management system covering all relevant performance objectives [77]. There are many common features and principles underlying these standards (such as employee involvement and continuous improvement) and the ISO standards explicitly identify particular linkages. Integration of management systems could deliver more effective implementation of individual aspects and reduce the management overhead of administering separate systems [78]. Inclusion of the requirements of sustainability management will extend such integrated systems even further, see the list of standards in Section 53.2. The case study of BMW Designworks in the following box illustrates one organization's approach.

Case Study: A New Sustainability Management System in the BMW Group [81]

BMW has a long-established tradition of environmental management. All its manufacturing facilities are certified to ISO 14001 and it has also sought to improve the environmental performance of its business partners and its non-production facilities. The company turned its attention to sustainability management in 1999 and chose Designworks/USA as a pilot site. The challenge was both to develop and to implement a sustainability management system (SMS) based on the ISO 14001 framework.

Designworks/USA, a provider of design and engineering services to the rest of the BMW group as well as to external clients in a variety of industries, was selected for the pilot because of the influence that design has over many sustainability issues and because it was perceived that designers would bring creative flair to bear on the task of developing and implementing the SMS. At the start of the initiative Dreamworks/USA had no comprehensive approach to managing its environmental and social aspects. External consultants and a member of the BMW staff familiar with their environmental management system took the lead in producing an internal standard "A Sustainability Management System Guidance" which required Dreamworks/USA to develop procedures to:

- Identify and prioritize sustainability aspects and impacts.
- Identify legal requirements related to sustainability concepts and to evaluate compliance.
- Identify legal requirements related to sustainability concepts and to evaluate compliance.
- Develop sustainability objectives and targets within each organizational function.
- Identify and deploy education and training to ensure awareness and competence.
- Regularly interact with stakeholders including regulators and the public.
- Routinely audit the organization's management system against the requirements stipulated in the SMS standard.
- Ensure that top management periodically reviews the SMS.

A form of risk assessment was used to prioritize the various sustainability aspects. This was based on seven dimensions of: probability of occurrence, intensity, duration, legal and regulatory requirements, stakeholder concerns, leadership potential, and level of control.

Benefits of the SMS have so far (only two years into the implementation process) included procedures for supplier selection and partnerships, shared commitment with some clients to sustainability, and improved internal human resource management policies and practices. A particularly notable outcome is a focus on the long term vision of the company. To date little attention has been given to results metrics, making it difficult to assess costs and benefits.

Particular challenges of implementation have included:

- Involving suppliers in the vision.
- Influencing clients to incorporate sustainability attributes into product design specifications.
- Developing the knowledge of design staff with respect to sustainability in a harsh commercial climate where all employees must account for every minute of the working day.
- The perceived conflict between the creative design culture of the organization on the one hand and the management system demands of rigorous systematic evaluation, documentation and control on the other.
- The perceived conflict between the creative design culture of the organization on the one hand and the management system demands of rigorous systematic evaluation, documentation and control on the other.
- The systematic integration of social issues into the design process.

The strategic significance of performance management systems is twofold: first, a strategic approach is needed to implement them successfully [79, 80]; and second they are the means of delivery of the competitive advantage that sustainability strategies (or indeed any other) can provide in terms of both what they achieve and what they represent in the eyes of customers and other stakeholders. The reporting requirements of standards are an important element: the transparency and credibility of good sustainability reporting is a significant public relations tool with respect to customers and regulators.

53.4.2 Operations Design

Operations design is concerned with both product and process design and their interactions. Sustainable operations design takes account of the entire product life cycle.

The sequence of design decisions needs to be as follows:

1) Analysis of the value system and determination of the *stakeholder value elements* that need to be delivered – an extension of the "product concept" idea that normally forms the basis of operations design decisions [10].
2) Design of the package of component goods and services that provides these benefits.
3) Determination and design of the *processes* needed to deliver the package, including the reverse as well as the forward supply chain.

Sustainable operations design requires particular attention to the following:

- Taking a "product-service system" perspective.
- Product and process design to optimize life cycle performance.
- Integration of the reverse supply chain.
- Development of relevant stakeholder engagement processes.
- Integration of financial and environmental costs.
- Application of risk assessment techniques.

A "Product-Service System" Perspective

The product designer must design an integrated bundle of goods and services, not just the goods element (the Volvo case study in the following box illustrates this). It is the total package that delivers the required value, the performance, to customers and all other stakeholders.

Case Study: Volvo's Alternative Fueled Vehicles [111]
As part of the Volvo Car Corporation's comprehensive approach to sustainability management, it has worked as a partner in a Swedish initiative to develop the market for alternative fueled vehicles. Such an approach recognizes that designing and producing the more sustainable product is far from enough to ensure significant market penetration, a viable business proposition and indeed significant contribution to "sustainable transport" overall. Other processes must also be put in place, such as

provision of financial incentives for consumers, fueling and service infrastructure and appropriate training for sales staff. The following extract from Volvo's Sustainability Report illustrates the wide scope of activities that are involved in ensuring that a more sustainable product is commercially successful.

1. The Offer	
Develop alternative fuel cars	*Volvo Cars has a broad offer of alternative vehicles in Sweden. in fact, of the eight car models currently in production, four of the models can be ordered with a Bi-Fuel (biomethane/natural gas engine) or FlexiFuel (powered on ethanol) engine.*
2 Government Actions and Incentives	
Swedish National Government	*No tax on renewable fuels like biogas*
	Vehicle taxation based on CO_2
	Reduction on the taxable value of alternative fuel company cars
	From 2006, major fuelling stations above a certain size must provide renewable fuel
	Governmental procurement Swedish municipal authorities
	Free parking in many towns
	No road tolls/congestion charges in Stockholm
	Preferential taxi zones
	Rebates on additional costs
	Free electricity for electric vehicles
3. Infrastructure	
Fuelling options	*Gas consists of a combination of biogas (biomethane) produced locally from organic waste and non-renewable natural gas formed in the earth's crust. E85 is produced from sugar cane or other crops. Currently, there are 62 biogas fuelling stations and approximately 350 E85 fuelling stations throughout the country*
Dealerships as fuelleling stations	*Increased availability and appeal of alternative fuel vehicles prompted some Volvo dealerships to establish CNG/biomethane fuelling stations.*
Encouraging infrastructure through partnerships	*Biogas Cities is a partnership to encourage investment in the biomethane fuel and vehicle market.*
4. Sales and Marketing	
Educating about alternative fuel cars	*Training for sales people emphasised how to sell alternative fuel cars by focusing on the customer benefits.*
Developing sales tools	*Sales tools like the web-based price comparison were developed to counteract increased competition on the environmental market. The environmental impact of different Volvo models can also be compared on our website.*

At the strategic level this might lead to entirely new business models, as discussed earlier. At the design level, the features included in the tangible part of the product offering will determine to some extent the nature of the services required. For example, maintenance intervals will be determined by technical specifications of goods and components; or the customer's need for training and service support will be determined by how user-friendly the product is perceived to be.

Marketers have long understood the need for an integrated approach, models such as the "augmented product model" [82–84] and the "augmented service offering" [85] provide guidance on the identification of all the relevant service processes that might need to be incorporated into a "product-service system".

Product and Process Design to Optimize Life Cycle Performance

Design of products to optimize the overall product performance with respect to environmental impact based on life cycle analysis and life cycle thinking

is known as "eco-design" [86–89]. The early stages of product development, where the product concept itself is devised, is recognized as particularly important for sustainability – incremental changes to existing products can only offer limited benefits. The concept of eco-design is being extended to embrace the social aspects of sustainability and the term "sustainable product design" is sometimes used to make the distinction [90].

Product and process design interact; in the case of services, of course, the process *is* the product, but in other cases too, the product specification determines the processes that must be operated. Eco-design principles might be considered to embrace process design to some extent, but the focus is almost exclusively on tangible products rather than on the manufacturing processes that produce them or on associated service processes. Eco-design of services is a relatively neglected field in the research literature.

The main elements that process designers can manipulate and some of the principal impacts on sustainability are as follows.

- *Physical layout and flow* impacts on resource efficiency; perhaps some process stages can be eliminated entirely reducing energy and materials consumption. The impact on working conditions and employee satisfaction must also be considered.
- *Supply network design:* industrial ecology principles might be applied. Socially responsible supply chain design takes account of risks that might arise from operating where human rights issues are a concern, for example [91, 92]. Design also needs to address partnership management issues because cooperation among supply chain partners is such a critical element of sustainability management [93].
- *Process technology* can impact on resource efficiency either by offering intrinsically cleaner production routes or by providing the means of better process control.
- *People:* both customers and employees may be integral elements of operations. Both need to have the motivation, knowledge and skills to make the necessary input. Education, training and communication processes are therefore of vital importance, as well as the more obvious job and service design concerns. The environmental and social impacts of different modes of working also need to be considered.

Sustainable operations design must be an integrative process, seeking to manipulate many variables and to resolve many apparent conflicts among the large number of performance criteria to be met. Proposals to simplify the approach are legion – see, for example, [94] and [95] – and in the absence of any established universal methodology many organizations devise their own, focusing on the priority issues for their particular situation. Sustainability adds in an entirely new set of difficult trade-off dilemmas (whereby achievement of one performance objective is only possible at the expense of another) that seem particularly intractable because of the impossibility in some cases of deciding which the most sustainable approach is. Subjective appraisal of the context of the decision and its consequences must be integrated with analysis of the detail of the design options. Whatever the approaches chosen, sustainable product/process design needs to manage trade-offs in a systematic way; first, to identify the trade-offs that exist and second, to support the decision in the trade-off situation [96]. Evaluation techniques based on risk assessment (discussed later) are a probable way forward.

Integration of the Reverse Supply Chain

The reverse supply chain involves the following key business processes [41]:

- Product acquisition: retrieval of the product from the market including any commercial transaction involved as well as physical collection.
- Reverse logistics: transportation to the recovery location.

- Testing and inspection: to determine the sorting and recovery options.
- Sorting and disposition: sorting is on the basis of quality and composition to determine the route of the rest of the reverse supply chain.
- Recovery: reconditioning and regaining products, components and materials.
- Re-distribution and sales of the regained products may coincide with the forward supply chain or may require new channels and markets to be developed.

The actual operating processes needed depend on the nature of the returned material, of which there are four main types [41]:

- End-of-life returns: taken back from the market to avoid environmental damage arising from waste items and materials, *e.g.*, collective recycling systems operated for batteries and tyres.
- End-of-use returns: after a period of operation; can be remanufactured or traded in second hand markets.
- Commercial returns: returned little-used or unused, *e.g.*, surplus stock; product recalls
- Re-usable items: such as pallets, refillable cartridges, bottles.

Recovery options for manufactured goods are listed in Table 53.4.

Consideration of recovery option needs to be included at the product design stage so as to maximize the opportunities for ready recovery of high value parts [98]. The economic/business aspects of the supply loop and its constituent processes must be considered as well as the technical issues, as was illustrated by the earlier steel section case study. Several different product recovery strategies have been identified in the computer industry [99]. For example, Dell uses a vertically integrated approach with its own recycling facility, while Hewlett Packard has established a joint venture to set up a recycling operation.

Table 53.4. Recovery options (adapted from [97])

Options	Operations	Output
Direct reuse	Inspection and testing to determine any damage Cleaning	As original product
Repair	Testing/inspection Restore product to working order; component replacement or repair	As original product
Refurbishing	Testing/inspection Upgrading, replacement or repair of critical modules	As original product
Remanufacturing	Manufacture new products partly from old components	New product
Cannibalization	Selective retrieval of components	Some reusable components/ parts; others to be scrapped
Scrap	Shred, sort, recycle and dispose of	Materials and residual waste

Stakeholder Engagement Processes

Sustainability management requires "engagement" or dialog with all relevant stakeholder groups. From the operations perspective, how can "stakeholder value" be delivered by an operation if there is not a clear understanding of just what aspects of value those stakeholders expect? From the stakeholders' perspective, how can they assess the operation's performance and capability to meet their needs without relevant and timely information? Not all the organization's stakeholders may be appropriate targets for dialogue with the operations function, but many will be. For example, discussion with employees about working practices, with supply chain partners about their local human rights issues, with regulators about interpretation of legal obligations,

with local communities about the local impacts of operational activities such as transportation, should or could all involve operations managers. Identification of relevant stakeholder groups is therefore an essential first step; stakeholder mapping is a useful technique to this end [36, 100].

Reporting to stakeholders is one half of the necessary dialogue. The GRI guidelines [25] identify the following characteristics of good reporting in this context:

- Materiality: covering topics that reflect the organization's significant economic, social and environmental impacts
- Inclusiveness: identifying the stakeholder groups whose interests are addressed by the report
- Completeness: presents an appropriate set of results that collectively address all the significant impacts so as to paint a complete picture of the organization's position
- Balance: includes both positive and negative aspects of performance
- Comparability: consistent reporting allowing comparisons over time and with any other appropriate reference points
- Accuracy: reporting should be accurate and detailed enough for stakeholders to assess performance
- Timeliness: reporting should be regular and at appropriate intervals for stakeholders to make informed decisions
- Clarity: information should be presented in a way that is accessible to the relevant stakeholder groups
- Reliability: information should be presented in such a way that it could be subject to examination.

The other half of the dialog, eliciting information from stakeholders, might involve surveys, panels, user groups and focus groups, for example, [101]. There has been criticism of the extent of true organizational commitment to engagement, with many of these activities viewed as little more than public relations exercises, resulting in little genuine organizational learning. The Accountability standard AA1000SES [102] seeks to counter this by providing a systematic framework for managing the engagement process so as to meet well-defined organizational objectives. This comprises a ten-stage process:

1. Identify stakeholders.
2. Initial identification of material issues.
3. Determine and define engagement objective and scope.
4. Establish engagement plan and period schedule.
5. Determine and define ways of engaging that work.
6. Build and strengthen capacity.
7. Understand material aspects, identify opportunities and risk.
8. Operationalize and internalize learning.
9. Measure, monitor and assess performance.
10. Assess, redefine and re-map.

Integration of Financial and Environmental Costs

Operations design must always take cost into account. Indeed seeking the least-cost process solution is often an objective in itself, although the interactions of cost with other factors, price and demand in particular, must be considered. "Value engineering" techniques [103] seek to link the cost of a component or feature to function so as to ensure that products are not "over-engineered" to meet specifications they do not need to fulfil. The linkage between resource use and cost means that many measures taken to reduce costs (such as eliminating a component or activity, or reducing the amount of material in the product) will also have a positive effect on sustainability. However traditional approaches to value engineering do not consider the entire product life cycle, and would require extension and adaptation to integrate sustainability concerns.

Environmental accounting forms a large field in its own right. It is in principle straightforward although effort and time consuming for an organization to assess its environmental costs. Four categories of environmental costs have been identified [104, 105]: waste and emission treatment; prevention and environmental management; material purchase value of wastes and emissions; processing costs of wastes and emissions. Few organizations use accounting systems that allow them to quantify these costs although a

comprehensive implementation of "lean thinking" should at least identify the material wastes generated. However, even if organizations did employ this type of information to identify ways to simultaneously reduce costs and improve resource efficiency, this would not necessarily lead them to address the most significant aspects from the sustainability perspective. First not all environmental costs are "internalized", they are "external costs" borne by national economies or by society at large. Examples include costs arising from the adverse health consequences of pollution, or governmental expenditure on flood prevention measures demanded by climate change. In principle there is no reason why an organization should not choose to assess the external costs arising from its activities and to use these in its internal decision making [106] in a form of "full cost accounting" [107]. In practice, determining the true costs of emissions, waste and so on is fraught with difficulty. Still more problematic would be any attempt to quantify the sustainability costs arising from adverse social consequences. For the foreseeable future, therefore, product and process designers must seek to integrate a variety of quantitative and qualitative factors to determine an overall optimum "sustainable" solution.

Application of Risk Assessment Techniques

Risk assessment techniques offer a way of prioritizing the various demands being made on the organization and its operations [108]. Risk assessment is an important generic tool that can be applied to all aspects of business management including sustainability management to determine those aspects of particular significance to the organization, and thereby requiring particular management attention. Indeed the Turnbull report of 1999 [109] specifically requires all companies quoted on the London Stock Exchange to ensure they have internal systems to control and manage *all* the business risks they face, arising from both internal and external factors.

The magnitude of a risk is the probability of occurrence of an event that could have harmful consequences multiplied by the severity of those consequences. Simple qualitative or quantitative scoring approaches can be used to rank options according to the risks they represent. More complex and detailed risk assessment systems are used routinely in operations management where there is a specific need such as when there is significant large scale hazard involved, as in the case of emergency planning. Environmental management uses risk assessment to identify *significant* environmental "aspects and impacts" [110].

An aspect or impact that could cause catastrophic damage to ecosystems or that could give rise to non-compliance with legal obligations would be deemed high risk to the organization and thereby deserving of priority attention.

Assessing risk almost inevitably involves some subjectivity, but it is nonetheless of paramount importance to use a consistent and systematic approach to provide transparent decision-making and to facilitate the revisiting of risk assessments and the decisions which follow from them as the factors involved change over time.

Risk assessment can take place at all levels of operations management, to inform decisions about business strategy, about product and process design as well as to determine the priorities for incremental improvements. For example, BT's annual CSR report contains a comparative assessment of all the various CSR risks it considers that it faces, including climate change, supply chain working conditions, diversity and outsourcing [19].

53.4.3 Planning and Control

Operations planning and control is concerned with matching supply and demand on a day to day basis. Decisions concern the loading of individual people, machines or work stations, the sequencing and scheduling of work, and monitoring and control, to check that what was planned was actually carried out, and to take remedial action as necessary. Conventionally it is quality, volume and timing that is planned and controlled, to ensure that what is produced matches what is demanded by customers, but for sustainable operations management additional objectives come into play. Decisions on loading, sequencing and scheduling should be taken with sustainability objectives in mind as well as product quality, cost and so on. Very often environmental and cost objectives will

coincide – energy efficiency leads to reduced energy costs – but this will not always be the case. Scheduling work to minimize noise pollution overnight, for example, may reduce process efficiency. The important thing is that the sustainability objectives are taken into account in making the day to day trade-off decisions. Often such trade-offs can be avoided completely by appropriate operations design, such as in this example the sound-proofing of machines, workstations or buildings.

Operations planning and control uses a variety of techniques [10], such as:

- MRP (materials requirements planning), MRPII (manufacturing resource planning), and ERP (enterprise resource planning).
- Capacity planning.
- Inventory management tools such as economic order quantity analysis and Pareto analysis.
- JIT (just in time) and lean management tools such as kanban control.

These tools have been developed to serve the traditional operations planning and control perspective and therefore do not currently explicitly provide for the management of environmental or other sustainability aspects. However, in some cases the underlying philosophy is already strongly linked to resource efficiency; the elimination of waste is a key principle of lean management techniques. In other cases environmental objectives can in principle be incorporated into the management frameworks relatively straightforwardly, although modified tool design and implementation is far from a trivial exercise [112]. The collection of a large amount of additional data is needed, requiring considerable change to established working practices and therefore posing a significant barrier to change.

The J Sainsbury case study in the following box illustrates the relevance of planning and control to sustainability objectives, and the trade-off decisions that are made in practice.

Case Study: J Sainsbury plc (UK Supermarket Chain)

J Sainsbury plc identifies transport as a significant source of environmental impact of its operations and recognizes the value of transporting its products more efficiently, both to reduce emissions and for the cost savings that result [113]. It therefore seeks not only to employ more efficient and alternative fueled vehicles but also to plan and control its logistics activities accordingly. For example, "*Our suppliers will ….take deliveries to our stores if they have empty vehicles on their way back to their sites",* p. 34 of [113]. However, some of the conflicts in objectives that businesses must manage are evident in the comment from the most recent environmental report, "*… we failed to meet our fuel consumption target due to nationwide reorganization of our transport network to increase product availability…".*

Buildings energy efficiency is also important and as well as making use of technology such as combined heat and power and solar panels, energy management is part of every store manager's annual targets and is an integral part of the formal "retail procedures" followed by all store staff. This is backed up by consumption information available in stores so that performance can be checked daily. However once again, the difficulty of combining sustainability with business objectives is highlighted: "*…in 2005/06 we experienced a large energy increase and a decrease in efficiency [measured by carbon dioxide emissions per square metre of floor space], primarily due to extended opening hours, night restocking to increase availability and the introduction of pharmacies in most of our stores",* p. 28 of [113].

With respect to wider sustainability objectives J Sainsbury plans and controls various of its store activities to provide high quality and responsive customer service such as managing performance against targets for checkout queuing times and time to answer telephone queries. It also has an active "colleague engagement" program aimed at ensuring staff are well-trained and motivated and monitors progress through a "colleague engagement index".

53.4.4 Improvement

Operations improvement is the systematic identification and evaluation of performance gaps (between the current and some desired future state) and the design and implementation of the means to close these gaps. It is typically proactively managed in the form of "continuous improvement", a concept that underpins both quality and environmental management methods as set out in the relevant standards and in performance management frameworks such as six sigma or the EFQM excellence model. This is therefore an aspect of operations management into which it ought to be relatively straightforward to integrate sustainability concerns. The common ground shared by these standards and systems can be summarized in terms of the following features:

- Continuous improvement cycle as the basis of the management framework (plan, do, check, act is a typical manifestation).
- Employee involvement and empowerment.
- Customer focus.
- Team working.
- Supportive organizational culture.
- Audit and analysis principles and techniques.

A strategic approach is needed, including top management commitment, the inclusion of sustainability at the level of corporate mission and vision level and the embedding of the principles and practices throughout all levels of the organization [52, 114].

An important part of managing improvement is determining the priorities. Typical conventional operations management approaches include importance–performance analysis [115] and the identification of core processes, critical success factors and key performance indicators [116]. The latter framework, being an all-embracing one, could incorporate sustainability performance objectives alongside others in a fully integrated model of the enterprise. In environmental management "significant" environmental aspects and impacts are usually determined via some form of risk assessment, as discussed earlier. Sustainability priorities can be determined in the same way.

A suitable set of performance indicators covering all aspects of operational performance, including sustainability, must be devised for effective audit, improvement, progress monitoring and reporting. [117–119]. Different organizations are likely to need different indicator sets and different targets, depending on the nature of their business and the context in which they operate. Environmental operational performance indicators should cover the following areas according to ISO 14031 [68]:

- Materials, *e.g.*, quantities (total or per unit output) used, recycled, disposed of.
- Energy, *e.g.*, energy use per unit of production output.
- Services supporting the organization's operations, *e.g.*, amount of cleaning agents used by contracted service providers.
- Physical facilities and equipment, *e.g.*, hours per year that a piece of equipment is in use; the amount of land used for a quantity of production.
- Supply and delivery, *e.g.*, fuel consumption of vehicle fleet.
- Products, *e.g.*, amount of energy consumed by use of a product.
- Services provided by the organization, *e.g.*, quantity of materials used during after-sales service of products.
- Wastes, *e.g.*, quantity of waste produced per year and/or per unit of production.
- Emissions, *e.g.*, quantity of air emissions with global warming potential; quantity of radiation released; noise measured at a particular location.

Guidance on indicators for the social aspects of sustainability (see Table 53.1) is provided in [14, 25, 51] and [120]. For example, employment practices might be assessed in terms of:

- Number of days lost due to job-related illnesses.
- Level of employee satisfaction.

- Participation in employee consultation mechanisms.
- Comparative wage levels.

Community relations might be assessed in terms of:

- Number of local jobs created.
- Number of employees participating in community programs.
- Participation in community liaison activities.

The implementation of sustainability management is itself an "improvement" for most organizations and progress with it will require review from time to time; the "sustainable development maturity matrix" given in BS 8900 is an appropriate tool [21].

The Marks and Spencer case study in the box below illustrates improvement in sustainability practices.

Case Study: Marks and Spencer (UK Food, Fashion and Home Retail Chain)

Marks and Spencer's Corporate Social Responsibility Report [121] stresses improvement throughout. Against each of the 17 sub-categories of product, people and places that its report considers it clearly states: what it set out to do in the previous year, how it actually performed in that year and the targets for the following year. An example covering just a single sub-category is given below. Note that the report includes comments on social as well as environmental benefits.

Reducing Waste from Packaging and Products

Since 1997, legislation has made retailers and other businesses responsible for the costs of recycling packaging.

We pay a levy (worked out on the basis of how much packaging we use), to help fund efforts to meet a UK recovery target which includes both recycling and other ways of reusing waste. For 2005, this target has increased from 63% to 65%. Over the next few years, this type of legislation will be extended to other products, starting with electrical goods in 2006.

What We Set Out to Do in 2004/05

Legislation

Monitor the planned implementation of European Union "takeback"/recycling legislation on batteries and electrical equipment.

Carrier Bags

Work with potential suppliers of sustainable plastic carrier bags to improve the version trialled.

Food Packaging

Develop an action plan to improve the environmental performance of food packaging.

Food Labelling

Phase-in new labelling policies on food products supported by training for suppliers and independent checking. Monitor customer feedback and changes to legislation.

How We Did in 2004/05

Legislation

We monitored the development of the British Retail Consortium's proposals for funding the collection and recycling of used electrical equipment for introduction in 2006. We appointed external specialists to manage our UK and Republic of Ireland packaging waste compliance.

Food Packaging

We developed a "Responsible Food Packaging" initiative which includes requirements to: reduce packaging; move towards more natural materials; use more recycled materials; and promote easy to open designs and tamper proofing. As a direct result of this we conducted trials on repackaging sandwiches in cardboard instead of plastic and using light-weight foamed

plastic trays for pre-prepared meals. We developed an easy-to-open salad bowl in consultation with "Help the Aged". We also extended the use of tamper-evident packaging wherever practical. In January 2005 we launched a sixmonth trial to use recycled plastic in the manufacture of a range of bottles and trays in partnership with the following organisations: Waste Resources Action Programme (WRAP), Closed Loop London and London Remade. In March 2005 we held a packaging workshop with our largest food supplier sponsored by WRAP which resulted in several possible projects to reduce packaging being identified.

Carrier Bags

We did not progress with the sustainable plastic carrier bag due to difficulties in making the naturally based polythene strong enough

In Addition We Have…

We continued to operate a programme that reuses or recycles around 50 million clothing hangers a year. We started a project to reduce the number of clothing hanger designs we use to reduce the costs of the hangers and improve recycling rates.

What We Aim to Do in 2005/06

Legislation

Monitor and ensure compliance with the UK implementation of legislation (Waste Electrical and Electronic Equipment Directive) covering the recycling of used electrical products in 2006.

Food Packaging

Continue to implement "Responsible Food Packaging" initiative including measures to:

- *Introduce biodegradable plastic packaging made from starch for fruit, vegetables and salads from April 2005.*
- *Replace plastic sandwich packaging with cardboard alternatives.*
- *Extend the use of light-weight foamed plastic trays to half of our pre-prepared meals saving about 50 tonnes of packaging a year.*
- *Review and improve environmental labelling of food packaging (e.g., advice on recycling).*
- *Work with Waste Resources Action Programme (WRAP) on packaging reduction initiatives.*

Clothing Packaging

Introduce a new streamlined range of clothing hangers from September 2005, supported by improved levels of reuse and recycling.

The report states "We regard CSR as a process of continuous improvement and alongside our successes we made some mistakes which we are addressing". It goes on to describe an improvement to sourcing of wood for garden furniture from sustainable sources after failing to be able to address challenges made by Greenpeace on its original claims, and improvements to waste food handling after a prosecution arising from a milk spillage incident.

53.5 Implications for Operations Management

The foregoing discussion demonstrates unequivocally that

- sustainability management needs operations management, in order for the many new and modified organizational practices essential to deliver progress towards sustainability to be appropriately designed and implemented;
- operations management needs sustainability management, in order for operations to meet the increasing demands being made by increasingly wide-ranging, vocal and influential groups of stakeholders.

There are three groups of implications arising from this.

1) The nature of the operations management discipline and function must *expand* to address the various sustainability issue adequately. This has been referred to as the "expanding horizon of operations management" [63]. While this is consistent with the importance in general of inter-functional and inter-disciplinary interfaces to the practice and theory of operations management [122], it adds considerably to the complexity of the operation.
2) The nature of the operations management function and role in organizations must not just expand to encompass the additional concerns, it must *change* in order to cope with the complexity of the expanded function. Emphasis should be placed how to design, implement and demonstrate integrative solutions that address multiple performance criteria effectively. This is likely to need confidence with the design and introduction of innovative solutions as well as competence with incremental continuous improvement approaches. Substantive development of new knowledge, skills and capabilities is required. For example, Gloet has identified the following four sets of management capabilities that must be built to support sustainability management [123].
   i. The following roles must be fulfilled: capacity to work across myriad interfaces; leadership – to articulate the vision of sustainability and social responsibility and the positive impact on the organization; change management
   ii. Effective relationship management is critical, for effective collaboration and communication across various boundaries.
   iii. Adoption of a strategic focus is necessary, for the development of sustainable business models, alignment of business and sustainability goals, and the ability to implement strategy throughout all levels of the organization.
   iv. A learning focus and systems thinking are essential to cope with the dynamic and complex nature of sustainability management.

   Professional development programs should be developed and offered accordingly.
3) There is a need for practical tools to assist the operations manager with this expanded and more complex role. Sustainability management is inherently problematic because of its large scope, the diverse nature of performance indicators, the need for value judgments and its relative newness in the business and operations management arena. Sustainable development is rooted in relatively abstract concepts requiring subjective assessment, an approach at odds with the more "scientific" analytical approach with which most operations managers are comfortable. It is therefore essential for researchers and practitioners to work in concert to develop appropriate tools to help organizations make concrete progress towards sustainability.

53.6 Conclusions

The relevance of sustainability issues to operations management is clear, yet to date, few operations managers would identify sustainability management as a key part of their remit. However, as sustainability objectives become more crucial for organizations for a whole raft of reasons, it is the operations function that must respond. Operations is, after all, the vehicle by which business strategy is implemented, and perhaps even more importantly, it is the main agent responsible for so many sustainability impacts. If the operations response is to be positive and effective then considerable change is needed on the following fronts. First, an appropriately wide systems view of the operation must be taken to allow all environmental and social impacts to be properly "managed" within the overall system. Second, it is imperative that there is integration of sustainability objectives at all levels of operations management so that the issues can be addressed at the appropriate level (strategy, design, *etc.*). Third, there is a need for appropriate professional development of operations managers to support these changes, and for additional research to

provide managers with practicable tools and techniques.

While environmental management systems are relatively well-developed and ripe for integration with operations management systems, the broader concept of sustainability management is as yet by contrast in its infancy, and its integration poses significant organizational challenges. Nevertheless it is essential that this nettle is grasped if industries and nations are to make real progress towards sustainability goals.

References

[1] Schultz K, Williamson P. Gaining competitive advantage in a carbon-constrained world: strategies for European business. European Management Journal 2005; 23(4):383–391.

[2] Inman RA. Implications of environmental management for operations management. Production Planning and Control 2002; 13(1):47–55.

[3] Porter ME, van der Linde C. Green and competitive: ending the stalemate. Harvard Business Review, 1995;Sep–Oct 1995:120–134.

[4] Soyka PA, Feldman SJ. Capturing the business value of EH&S excellence. Corporate Environmental Strategy 1998; 5(2): 61.

[5] Jenkins H. Small business champions for corporate social responsibility. Journal of Business Ethics 2006; 67:241–256.

[6] Orsato RJ. Competitive environmental strategies: when does it pay to be green? California Management Review 2006; 48(2): 127.

[7] Carroll AB. Managing ethically with global stakeholders: a present and future challenge. Academy of Management Executive 2004; 18(2):114–120.

[8] Johnson HH. Does it pay to be good? Social responsibility and financial performance. Business Horizons 2003; Nov–Dec 2003:34–40.

[9] Payne DM, Raiborn CA. Sustainable development: the ethics support the economics. Journal of Business Ethics 2001; 32:157–168.

[10] Slack N, Chambers S, Johnston R. Operations management. 4th ed. FT Prentice Hall, New York, 2003.

[11] World Commission on Environment and Development, Our common future, 1987.

[12] Wilkinson A, Hill MR, Gollan P. The sustainability debate. International Journal of Operations and Production Management 2001; 21(12):1492–1502.

[13] Carroll AB. The pyramid of corporate social responsibility: toward the moral management of organizational stakeholders. Business Horizons, 1991; July-August: 39–48.

[14] Kok P, *et al.,* A corporate social responsibility audit within a quality management framework. Journal of Business Ethics 2001; 31:285–291.

[15] Castka P, *et al.,* Integrating corporate social responsibility (CSR) into ISO management systems – In search of a feasible CSR management system framework. The TQM Magazine 2004; 16(3):216–224.

[16] Elkington J. The "triple bottom line" for 21st century business. In: Starkey R, Welford R, editors. The Earthscan reader in business and sustainable development. Earthscan, 2001.

[17] Dow Jones Indexes. Dow Jones Sustainability Indexes, 2006.

[18] British Telecommunications Plc (BT), Changing world: sustained values. BT, 2006.

[19] British Telecommunications Plc (BT), Social and environmental report – Let's make a better world. BT, 2006.

[20] British Telecommunications Plc (BT), BT: Society and environment. 2006.

[21] BSI, BS 8900: 2006 Guidance for management of sustainable development, 2006.

[22] Gibson RB. Beyond the pillars: Sustainability assessment as a framework for effective integration of social, economic and ecological considerations in significant decision-making. Journal of Environmental Assessment Policy and Management. 2006;8(3):259–280.

[23] SA 8000, Social Accountability International: New York, 2001.

[24] Webb K. The ISO 26000 social responsibility guidance standard - progress so far. ESG UQAM 2005.

[25] Global reporting initiative, sustainability reporting guidelines, version 3.0. Global Reporting Initiative. 2006.

[26] James P. Towards sustainable business? In: Charter M, Tischner U, editors. Sustainable solutions – Developing products and services for the future. Greanleaf: Sheffield, 2001.

[27] Veleva V, Ellenbecker M. A proposal for measuring business sustainability. Greener Management International 2000; Autumn:101–120.

[28] Lamberton G. Sustainability accounting – A brief history and conceptual framework. Accounting Forum 2005; 29:7–26.

[29] BSI, BS EN ISO 14040:2006 Environmental management – life cycle assessment – Principles and framework, 2006.
[30] Byung-Chul C, *et al.,* Life cycle assessment of a personal computer and its effective recycling rate. International Journal of Life Cycle Assessment 2006; 11(2):122–128.
[31] Seuring S. Emerging issues in life-cycle management. Greener Management International 2004; 45: Spring: 3–8.
[32] Westkamper E, Alting L, Arndt G. Life cycle management and assessment: approaches and visions towards sustainable manufacturing. Proceedings of Institution of Mechanical Engineers Pt B: Journal of Engineering Manufacture 2001; 215:599–626.
[33] Post JE, Preston LE, Sachs S. Managing the extended enterprise: the new stakeholder view. California Management Review 2002; 45(1):6–28.
[34] Payne A, Ballantyne D, Christopher M. A stakeholder approach to relationship marketing strategy. European Journal of Marketing 2006; 39(7/8):855–871.
[35] Laszlo C, Sherman D, Whalen J. Expanding the value horizon: how stakeholder value contributes to competitive advantage. Journal of Corporate Citizenship 2005; winter: 65–76.
[36] Freeman E, Liedtka JM. Stakeholder capitalism and the value chain. European Management Journal 1997; 15(3):286–296.
[37] de Man R, Burns TR. Sustainability: supply chains, partner linkages, and new forms of self-regulation. Human Systems Management 2006;5:1–12.
[38] Geyer R, Jackson T. Supply loops and their constraints: the industrial ecology of recycling and reuse. California Management Review 2004; 46(2):55–73.
[39] Guide VDR, Harrison TP, Van Wassenhove LN. The challenge of closed-loop supply chains. Interfaces 2003; 33(6):3–6.
[40] van Hoek RI. Case studies of greening the automotive supply chain through technology and operations. International journal of environmental technology and management 2001; 1(1/2):140–163.
[41] Krikke H, Blanc Ile, van de Velde S. Product Modularity and the design of closed-loop supply chains. California Management Review 2004; 46(2): 23–39.
[42] Guide VDR, Van Wassenhove L. Business aspects of closed-loop supply chains – Exploring the issues. Pittsburgh: Carnegie Bosch Institute, 2003.
[43] Rhodes E. From supply chains to total product systems. In: Rhodes E, Warren JP, Carter R, editors. Supply chains and total product systems: A reader. The Open University and Blackwell Publishing: Oxford, 2006.
[44] Garcia Sanchez I, Wenzel H, Jorgenson MS. Models for defining LCM, monitoring LCM practice and assessing its feasibility. Greener Management International 2004; 45: Spring: 9–25.
[45] Desrochers P. Regional development and inter-industry recycling linkages: Some historical perspectives. Entrepreneurship and Regional Development 2002; 14:49–65.
[46] Gupta M, Sharma K. Environmental operations management: an opportunity for improvement. Production and Inventory Management Journal 1996; Third Quarter: 40–46.
[47] Tsoulfas GT, Pappis CP. Environmental principles applicable to supply chain design and operation. Journal of Cleaner Production 2006; 14:1593–1602.
[48] Gupta MC. Environmental management and its impact on the operations function. International Journal of Operations and Production Management 1995; 15(8):34–51.
[49] Elliott B. Operations management: A key player in achieving a sustainable future. Management services 2001; July 2001:14–19.
[50] Kleindorfer PR, Singhal K, Van Wassenhove LN. Sustainable Operations Management. Production and Operations Management 2005; 14(4): 482–492.
[51] Schmidt I, *et al.,* SEEbalance: Managing sustainability of products and processes with the socio-eco efficency analysis by BASF. Greener Management International 2004; 45:Spring: 79–94.
[52] Sroufe RP, *et al.,* Environmental management practices – A framework. Greener Management International 2002; 40: Winter: 23–44.
[53] Lowson RH. Operations Strategy: Genealogy, classification and anatomy. International Journal of Operations and Production Management 2002; 22(10):1112–1129.
[54] Hayes RH, Upton DM. Operations-based strategy. California Management Review 1998; 40(4):8–25.
[55] Gagnon S. Resource-based competition and the new operations strategy. International Journal of Operations and Production Management 1999; 19(2):125–138.
[56] Guide VDR, Teunter RH, Van Wassenhove LN. Matching demand and supply to maximize profits from remanufacturing. Manufacturing and Service Operations Management 2003; 5(4):303–316.

[57] Mont O. Reducing life-cycle environmental impacts through systems of joint use. Greener Management International 2004; 45: Spring: 63–77.
[58] Halme M, Jasch C, Scharp M. Sustainable homeservices? Towards household services that enhance ecological, social and economic sustainability. Ecological Economics 2004; 51:125–138.
[59] Stahel WR. Sustainability and services. In: Charter M, Tischner U, editors. Sustainable solutions – Developing products and services for the future. Greanleaf: Sheffield 2001.
[60] Roy R. Sustainable product-service systems. Futures 2000;32:289–299.
[61] Reiskin ED, White AL. Servicizing the chemical supply chain. Journal of Industrial Ecology 2000; 3(2 and 3):19–31.
[62] Oliva R, Kallenburg R. Managing the transition from products to services. International Journal of Service Industry Management 2003; 14(2):160–172.
[63] Corbett CJ, Klassen RD. Extending the horizons: Environmental excellence as key to improving operations. Manufacturing and Service Operations Management 2006; 8(1): 5–22.
[64] Klassen, RD, Angell LC. An international comparison of environmental management in operations: The impact of manufacturing flexibility in the US and Germany. Journal of Operations Management 1998; 16: 177–194.
[65] Kaplan S, Norton DP. The balanced scorecard – Measures that drive performance. Harvard Business Review 1992; Jan.–Feb: 71–79.
[66] Hervani AA, Helms MM, Sarkis J. Performance measurement for green supply chain management. Benchmarking: An International Journal 2005;12(4): 330–353.
[67] Neely A, Adams C, Crowe P. The performance prism in practice. Measuring Business Excellence 2001;5(2): 6–12.
[68] BSI, BS EN ISO 14031:2000 Environmental management – Environmental performance evaluation – Guidelines, 2000.
[69] Angell LC, Klassen RD. Integrating environmental issues into the mainstream: an agenda for research in operations management. Journal of Operations Management 1999; 17:575–598.
[70] Hill MR. Sustainability, greenhouse gas emissions and international operations management. International Journal of Operations and Production Management 2001; 21(12):1503–1520.
[71] ENDS, Firms link up to monitor suppliers' CSR risks. ENDS Report, 2006; 379: 23.
[72] Rothenberg S, Pil FK, Maxwell D. Lean, green, and the quest for superior environmental performance. Production and operations management 2001; 10(3): 228–243.
[73] BSI, BS EN ISO 9001:2000 Quality management systems – Requirements, 2000.
[74] BSI, BS 8800:2004 Occupational health and safety management systems – Guide, 2004.
[75] BSI, BS EN ISO 14001:2004 Environmental Management Systems – Requirements with guidance for use, 2004.
[76] DEFRA, The pinnacle of environmental management - an introductory guide to EMAS. Department for Environment, Food and Rural Affairs 2003.
[77] Karapetrovic S, Willborn W. Integration of quality and environmental management systems. The TQM Magazine 1998; 10(3): 204–213.
[78] Wilkinson G, Dale BG. Integration of quality, environmental and health and safety management systems: an examination of the key issues. Proceedings of Institution of Mechanical Engineers Pt B: Journal of Engineering Manufacture 1999; 213:275–283.
[79] Beer M. Why total quality management programs do not persist: The role of management quality and implications for leading a TQM transformation. Decision Sciences 2003; 34(4):623–641.
[80] Hill S, Wilkinson A. In search of TQM. Employee Relations 1995; 17(3):8–25.
[81] McElhaney KA, Toffel MW, Hill N. Designing a sustainability management system at BMW Group – The Designworks/USA case study. Greener Management International 2004; 46 (summer):103–116.
[82] Levitt T. Marketing success through differentiation - of anything. Harvard Business Review, 1980(Jan/Feb): 83–91.
[83] Payne A, Holt S, Frow P. Relationship value management: exploring the integration of employee, customer and shareholder value and enterprise performance models. Journal of Marketing Management 2001; 17:785–817.
[84] Payne A, Holt S. Diagnosing customer value: integrating the value process and relationship marketing. British Journal of Management 2001; 12:159–182.
[85] Gronroos C. Service management and marketing – A customer relationship management approach. Wiley, New York, 2000.

[86] Maxwell D, Sheate W, van der Vorst R. Functional and systems aspects of the sustainable product and service development approach for industry. Journal of Cleaner Production 2006; 14:1466–1479.

[87] Karlsson R, Luttropp C. Ecodesign: What's happening? An overview of the subject area of ecodesign and of the papers in this special issue. Journal of Cleaner Production 2006;14:1291–1298.

[88] Bhamra TA. Ecodesign: the search for new strategies in product development. Proceedings of Institution of Mechanical Engineers Pt B: Journal of Engineering Manufacture 2004; 218: 557–569.

[89] Charter M, Tischner U. Sustainable solutions – Ddeveloping products and services for the future. Greanleaf, Sheffield, 2001.

[90] Tischner U, Charter M. Sustainable product design. In: Charter M, Tischner U, editors. Sustainable solutions –Ddeveloping products and services for the future. Greanleaf: Sheffield. 2001.

[91] Leiper QJ, Riley P, Uren S. The environmental challenge for supply chain management. In: Rhodes E, Warren JP, Carter R, editors. Supply chains and total product systems: A reader. The Open University and Blackwell Publishing: Oxford, 2006.

[92] Winstanley D, Clark J, Leeson H. Approaches to child labour in the supply chain. In: Rhodes E, Warren JP, Carter R, editors. Supply chains and total product systems: A reader. The Open University and Blackwell Publishing: Oxford, 2006,

[93] Seuring S. Integrated chain management and supply chain management comparative analysis and illustrative cases. Journal of Cleaner Production 2004; 12: 1059–1071.

[94] Khan FI, Sadiq R, Veitch B. Life cycle iNdeX (LInX): a new indexing procedure for process and product design and decision-making. Journal of Cleaner Production 2004; 12:58–76.

[95] Tischner U. Tools for ecodesign and sustainable product design. In: Charter M, Tischner U, editors. Sustainable solutions – Developing products and services for the future. Greanleaf: Sheffield, 2001.

[96] Byggeth SH, Handling E. Trade-offs in ecodesign tools for sustainable product development and procurement. Journal of Cleaner Production 2006; 14:1420–1430.

[97] Thierry M, *et al.,* Strategic issues in product recovery management. California Management Review 1995; 37(2):114–135.

[98] King AM, Burgess SC. The development of a remanufacturing platform design: A strategic response to the Directive on Waste Electrical and Electronic Equipment. Proceedings of Institution of Mechanical Engineers Pt B: Journal of Engineering Manufacture 2005; 219:623–631.

[99] Toffel MW. The growing strategic importance of end-of-life product management. California Management Review 2003; 45(3): 102–129.

[100] Johnson G, Scholes K. Exploring corporate strategy. 3rd ed. Prentice Hall, Englewood Cliffs, NJ, 1993.

[101] Cumming JF. Engaging stakeholders in corporate accountability programmes: A cross-sectoral analysis of UK and transnational experience. Business Ethics: A European Review 200110(1):45–52.

[102] Accountability, AA1000SES Stakeholder engagement standard – Exposure draft.: London, 2005.

[103] Thiry M. A framework for value management practice. Project Management Institute 1997:

[104] Gale R. Environmental management accounting as a reflexive modernization strategy in cleaner production. Journal of Cleaner Production 2006; 14: 1228–1236.

[105] Gale R. Environmental costs at a Canadian paper mill: A case study of environmental management accounting. Journal of Cleaner Production 2006;14: 1237–1251.

[106] Jasch C. How to perform an environmental management cost assessment in one day. Journal of Cleaner Production 2006; 14: 1194–1213.

[107] Atkinson G. Measuring corporate sustainability. Journal of Environmental Planning and Management 2000; 43(2):235–252.

[108] Reinert KH, Jaycock MA, Weiler ED. Using risk assessment to facilitate and enhance the movement to sustainability. Environmental Quality Management 2006; Spring:1–8.

[109] Turnbull N. Internal Control, guidance for directors on the combined code. Institute of Chartered Accountants in England and Wales, 1999.

[110] Gilbert M, Gould R. Achieving environmental standards. 2nd ed. FT Pitman, London, 1998.

[111] Volvo Car Corporation, Sustainability Report, 2005.

[112] Melnyk SA, *et al.,* Green MRP: identifying the material and environmental impacts of production schedules. International Journal of Production Research 2001; 39(8):1559–1573.

[113] J Sainsbury plc, Corporate Responsibility Report, 2006.

[114] Zwetsloot GIJM. From management systems to corporate responsibility. Journal of Business Ethics 2003; 44:201–207.
[115] Slack N. The importance-performance matrix as a determinant of improvement priority. International Journal of Operations and Production Management 1994; 14(5):59–75.
[116] Oakland J. Chapter 13 Implementation of TQM and the management of change, in TQM Text with cases. Butterworth Heinemann, London, 2000.
[117] Ammenberg J, Hjelm O. The connection between environmental management systems and continual performance improvement. Corporate Environmental Strategy 2002; 9(2):183–192.
[118] Azzone G, Noci G., Identifying effective PMSs for the deployment of "green" manufacturing strategies. International Journal of Operations and Production Management 1998; 18(4):308–335.
[119] de Burgos Jimenez J, Lorente JJC. Environmental performance as an operations objective. International Journal of Operations and Production Management 2001; 21(12):1553–1572.
[120] Epstein MJ, Roy M-J. Improving sustainability performance: specifying, implementing and measuring key principles. Journal of General Management 2003; 29(1):15–31.
[121] Marks and Spencer, Corporate Social Responsibility Report, 2005.
[122] Voss CA. Operations Management – From Taylor to Toyota – and beyond? British Journal of Management 1995; 6 (Special Issue): S17–S29.
[123] Gloet M. Knowledge management and the links to HRM: developing leadership and management capabilities to support sustainability. Management Research News 2006; 29(7): 402–413.

54

Indicators for Assessing Sustainability Performance

P. Zhou and B.W. Ang

Department of Industrial and Systems Engineering, National University of Singapore, Singapore

Abstract: Sustainability is a universally advocated and quoted concept. To assess the sustainability performance of an entity, *e.g,.* a company, an industry or a country, appropriate indicators are often developed for the use of analysts and decision makers. Numerous sustainability indicators can be found in the literature, which vary from a non-composite indicators to composite indicators. We first deal with non-composite indicators for sustainability. We then introduce the concept of composite indicators and discuss why they are more suitable for assessing sustainability. From the viewpoint of operations research, we describe the methods for constructing composite sustainability indicators and highlight the usefulness of multiple criteria decision analysis and data envelopment analysis. An illustrative example is presented for assessing alternative methods in constructing composite sustainability indicators.

54.1 Introduction

Sustainable development has increasingly been incorporated into different levels of society, *e.g.*, companies, industries, and countries. According to the definition given by the Brundtland Commission [57], sustainable development implies that development should "meet the needs of the present without compromising the ability of future generations to meet their own needs". The concept is easy to understand but there are many practical issues among which the assessment of sustainability is a difficult but indispensable one. Different tools have been developed for assessing sustainability. The study by Ness *et al*. [36] provides an excellent categorization of various sustainability assessment tools. According to the study, the tools can be broadly divided into three main categories, namely *indicators*, *product-related assessment*, and *integrated assessment tools*. In this chapter, we shall limit our discussion to the indicator approach to assessing sustainability.

Indicators are quantitative measures that represent the state of an individual object such as a product or a complex system. The indicator approach has been widely studied for decision and policy-making in sustainability assessment [22]. Among the numerous sustainability indicators, some are micro-level based, *e.g.*, [3, 8, 23, 29, 47, 51], while others are at the macro level, *e.g.*, [19, 21, 22, 27, 28, 39, 44, 54, 60]. In addition, the indicators for sustainability can also be classified by the theme involved, such as economic, environmental/ecological, and socio-political [21].

From the methodological viewpoint, we may also classify sustainability indicators into two groups. One could be termed *non-composite*

indicators since it involves the use of an individual or a set of individual indicators. Examples include the 58 indicators for sustainability developed by the United Nations Commission on Sustainable Development [52] and the 30 energy indicators for sustainable development proposed by the International Atomic Energy Agency [24]. The other group consists of *composite indicators,* whose development has recently gained considerable attention. Examples of composite indicators are the Human Development Index of the United Nations Development Program [45] and the Environmental Sustainability Index developed by Yale, Columbia, World Economic Forum and the Joint Research Center of European Commission [13]. We shall study these two approaches to assessing sustainability and present a survey on some methods for constructing composite sustainability indicators. This is by no means a comprehensive survey of sustainability indicators but rather an assessment on some recent methodological developments in the area.

The remainder of this chapter is organized as follows. In Section 54.2 we provide an introduction to non-composite indicators. Section 54.3 presents the concept of composite indicators and highlights their uses in assessing sustainability. In Section 54.4, we present the most popular methods for constructing composite sustainability indicators from the viewpoint of operations research. In Section 54.5, we give an example to assess the methods described in Section 54.4 in constructing composite sustainability indicators. Section 54.6 concludes the chapter.

Acronyms and Notation

CO_2	Carbon Dioxide
CSIs	Composite Sustainability Indicators
DEA	Data Envelopment Analysis
EF	Ecological Footprint
EPI	Environmental Performance Index
ESI	Environmental Sustainability Index
GDP	Gross Domestic Product
GS	Genuine Savings
HDI	Human Development Index
LPI	Living Planet Index
MCDA	Multiple Criteria Decision Analysis
OECD	Organization for Economic Co-operation and Development
SAW	Simple Additive Weighting
WDI	Weighted Displaced Ideal
WP	Weighted Product
WWF	World Wildlife Foundation
I_i	The CSI of entity i
I_{ij}	The value of entity i with respect to sub-indicator j
w_j	The standardized weight for sub-indicator j
$w_j(P_{kl})$	The weight for sub-indicator j if entity k performs better than entity l in terms of the sub-indicator; otherwise it is equal to zero
$w_j(I_{kl})$	The weight for sub-indicator j if entity k is indifferent from entity l in terms of the sub-indicator; otherwise it is equal to zero
T	Production technology
$\mathbf{x}_i = (x_{i1}, \cdots, x_{iK})$	The vector of inputs for entity i, which consists of the inputs consumed in a production process, *e.g.*, material and labor
$\mathbf{y}_i = (y_{i1}, \cdots, y_{iL})$	The vector of desirable outputs for entity i, which consists of the desirable outputs generated from a production process, *e.g.*, electricity
$\mathbf{u}_i = (u_{i1}, \cdots, u_{iS})$	The vector of undesirable outputs for entity i, which consists of the undesirable outputs generated from a production process, *e.g.*, pollutants
REI	Radial environmental performance index, *i.e.*, the optimum objective value of model (54.6)
$SBEI$	Slacks-based environmental index derived from model (54.8)
gI_i	The aggregated performance score of entity i from model (54.9)
bI_i	The aggregated performance score of entity i from model (54.10)

α A control parameter not less than 0 and not larger than 1

$I_i(\alpha)$ The CSI given by the MCDA-DEA approach with parameter α

54.2 Non-composite Indicators for Sustainability

Non-composite indicators for sustainability refer to an individual or a set of individual indicators for assessing sustainability. They can be broadly classified into two types. The first consists of a set of indicators, which are usually built upon certain important aspects of sustainable development. For example, the International Atomic Energy Agency [24] provides an excellent paradigm by carefully selecting a total of 30 energy indicators for sustainable development. These indicators are classified into social, economic and environment dimensions which are further classified into seven themes and 19 sub-themes. Among these 30 indicators, each can be used to assess a particular issue relevant to sustainable development. Since the IAEA study, the use of energy indicators for assessing sustainable development has gained much attention, *e.g.*, [27]. A set of individual indicators has the ability of covering different aspects of sustainability, and therefore provides detailed insights towards sustainable development. Nevertheless, a set of indicators is usually complex and difficult to interpret due to their large size [27]. As a result, the approach is not able to provide a concise overview of sustainability for the use of decision and policy making.

The second type of non-composite indicators consists of those which use a single measure to represent multiple aspects of sustainability. Since this type of indicators often integrates multiple aspects of sustainability by a common unit such as dollar, they may be termed an integrated index. Ang [2] recently proposed such an integrated index for monitoring energy efficiency trends. Two other well-known integrated indexes for sustainability are the genuine savings (GS) developed by World Bank [56] and the ecological footprint (EF) proposed by Wackernagel and Rees [55].

GS measures the true rate of savings in an economy after taking into account investments in human capital, depletion of natural resources and damage caused by pollution. Since GS is derived from standard national accounting measures of gross national savings by incorporating several environmental indicators, it could be treated as an effective proxy for tracking sustainable development [38]. EF is defined as "the amount of land and water area a human population would hypothetically need to provide the resources that the population consumes and to absorb the wastes that the population produces". It has been widely used as an indicator for modeling environmental sustainability, which can be used to explore the sustainability of individual lifestyles, organizations, industry sectors, regions and nations. An integrated index such as GS and EF provides an aggregated picture of the state of a system. A major feature is that it takes into account many aspects of sustainability using a common measurable unit. However, in practice it may not be easy to represent all the aspects of sustainability using the same unit. This problem, however, can be overcome by using the approach of composite indicators.

54.3 Composite Indicators for Sustainability

According to the OECD Glossary of Statistical Terms (http://stats.oecd.org/glossary), a composite indicator is formed when individual indicators are compiled into a single index on the basis of an underlying model of the multi-dimensional concept that is being measured. Technically, it is a mathematical aggregation of a set of individual indicators that measure multi-dimensional concepts but usually have no common units of measurement [35]. The approach of composite indicators has its pros and cons. Table 54.1 shows some major ones as discussed in [35] and [46].

Table 54.1. Pros and cons of composite indicators

Pros	Cons
– Can summarize complex or multi-dimensional issues for supporting decision/policy makers – Can provide a big picture which is easier to interpret than trying to find a trend in many separate indicators – Can offer a rounded assessment of countries' or regions performance – Can reduce the size of a set of indicators or include more information within the existing size limit – Can facilitate communication with general public, *e.g.* citizens and media	– May send misleading, non-robust policy messages if a composite indicator is poorly constructed – May invite politicians or stakeholders to draw simplistic policy conclusions – May involve stages where judgmental decisions have to be made – May disguise serious failings in some dimensions and increase the difficulty of identifying proper remedial action – May lead to inappropriate policies if dimensions of performance that are difficult to measure are ignored

Composite indicators have been increasingly applied for performance monitoring, benchmarking, policy analysis and public communication in wide range of sectors including economy, environment and society by many national and international organizations. Their popularity has been pointed out by Saisana *et al*. [46] as the temptation of stakeholders and practitioners to summarize complex and sometime elusive process (*e.g.*, sustainability) into a single figure to benchmark country performance for policy consumption. Three well-known composite indicators relevant to sustainable development are described below, namely the

(a) living planet index,
(b) environmental performance/sustainability indexes, and
(c) the human development index.

The living planet index (LPI) was first released in 1998 and has been updated periodically by the World Wildlife Foundation (WWF) [58] for measuring the overall state of the Earth's natural ecosystems, which includes national and global data on human pressures on natural ecosystems arising from the consumption of natural resources and the effects of pollution. It is derived from three sub-indicators that track trends in approximately 3,000 populations of more than 1,000 vertebrate species living in terrestrial, freshwater and maritime ecosystems around the world. The LPI together with EF published by the WWF provide vital information for gauging the world's progress towards sustainable development.

The environmental performance/sustainability indexes (EPI/ESI) were initiated by the World Economic Forum (WEF) in 2002 for measuring environmental protection results at the national scale. Two versions of EPI have been published so far and the latest, the 2006 EPI [14], is based on 16 sub-indicators falling into six well-established policy categories including environmental health, air quality, water resources, productive natural resources, biodiversity and habitat, and sustainable energy. The 2002 EPI includes 23 OECD countries but the 2006 EPI covers 133 countries and provides a solid foundation for assessing the progress of these countries towards sustainability. Compared to the EPI, the ESI combines more sub-indicators in a broader range and therefore provides a bigger picture for measuring long-term environmental prospects [13]. The 2005 ESI covers 146 countries and involves 76 underlying sub-indicators.

The human development index (HDI) was introduced by the United Nations Development Program in 1990, which was later published annually in the Human Development Report [45]. The HDI was constructed based on three sub-indicators that reflected three major dimensions of human development: *longevity*, *knowledge*, and *standard of living*. It offers an alternative to national income as a summary measure of human well-being. The latest version of HDI can be found in the Human Development Report 2005 [53], which covers 175 UN member countries.

Besides the above three composite indicators, there are several others which are listed in the information sever: http://farmweb.jrc.cec.eu.int/ci/ maintained by the Joint Research Center of European Commission. Considering the popularity of composite indicators and the complexity of sustainability, it is expected that composite indicators will increasingly be used to measure and evaluate sustainability. Hereafter, we call the composite indicators for sustainability as *composite sustainability indicators* (CSIs).

54.4 Recent Methodological Developments in Constructing CSIs

Many techniques have been used to construct CSIs, *e.g.*, *life cycle assessment*, *environmental accounting approach*, *production efficiency theory* as discussed in [35, 37]. From the viewpoint of operations research, the existing aggregation techniques for constructing CSIs can be divided into two categories: the *indirect approach*, which often involves the normalization of the original sub-indicators and the weighting and aggregation of the normalized data where *multiple criteria decision analysis* (MCDA) plays an important role, and the *direct approach*, in which a CSI is directly obtained from the original sub-indicators by using data envelopment analysis (DEA) type models from the point of view of productive efficiency.

54.4.1 MCDA Methods for Constructing CSIs

Consider the case where there are *m* entities whose sustainability performance is to be evaluated based on *n* sub-indicators and these sub-indicators have no common measurable units. Let I_{ij} denote the value of entity *i* with respect to sub-indicator *j* and w_j denote the standardized weight assigned to sub-indicator *j*. The weights are often interpreted as the coefficients of importance that reflect the preference information of decision makers. Without loss of generality, we further assume that all the sub-indicators are of the benefit type which satisfy the property of *the larger the better*. The problem is to aggregate $I_{ij}\,(j=1,\cdots,n)$ into a CSI I_i that can be used to assess the sustainability performance of entity *i*:

$$\begin{bmatrix} I_{11} & I_{12} & \cdots & I_{1n} \\ I_{21} & I_{22} & \cdots & I_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ I_{m1} & I_{m2} & \cdots & I_{mn} \end{bmatrix} \rightarrow \begin{bmatrix} I_1 \\ I_2 \\ \vdots \\ I_m \end{bmatrix}.$$

Since different sub-indicators have different measurable units, normalization procedure is often needed to give dimensionless sub-indicators. Various normalization procedures are available, *e.g.*, the *Z*-Score transformation [13] and the linear normalization [64]. Saisana *et al*. [46] have shown that the choice of normalization methods has no severe effects on the values of composite indicators derived while the choice of aggregation methods has. Hence, we shall limit our discussions to the aggregation methods for constructing CSIs in the context of MCDA. We assume that $I_{ij}\,(j=1,\cdots,n)$ are the values after normalization.

The *simple additive weighting* (SAW) method, also known as the *weighted sum* method, is a popular aggregation method for constructing CSIs. See, for examples, [13, 14, 26]. The SAW method can be formulated as

$$I_i = \sum_{j=1}^{n} w_j I_{ij} \qquad i=1,\cdots,m\,, \tag{54.1}$$

where I_i is the CSI of entity *i*. An assumption implied is that the sub-indicators are preferentially independent which may be difficult to satisfy. However, even if the assumption does not hold, the SAW method would yield extremely close approximation to the ideal value function [59]. Another problem is that the weights carry the meaning of trade-off ratios as demonstrated by Munda and Nardo [32], which is inconsistent with its meaning of importance coefficients. Despite these limitations, the SAW method has been widely applied due to its transparency and ease of understanding.

The *weighted product* (WP) method, *i.e.*, (54.2), is a MCDA method in which the system with poor performance in some attributes is penalized more

heavily [48]. It represents an in-between concept compared with the SAW method with full compensability and the non-compensatory MCDA approach [35]. Ebert and Welsch [12] have shown that the WP method would lead to a more meaningful composite indicator compared with the SAW method.

$$I_i = \prod_{j=1}^{n} (I_{ij})^{w_j} \qquad i = 1, \cdots, m \,. \tag{54.2}$$

The *weighted displaced ideal* (WDI) method is based on the concept that the best system should have the least distance from the ideal system [63]. It has been further investigated by Diaz-Balteiro and Romero [11] for constructing an appropriate sustainability index. The WDI method can be formulated as

$$I_i(p) = \left[\sum_{j=1}^{n} w_j^p I_{ij}^p \right]^{1/p} \qquad i = 1, \cdots, m \,. \tag{54.3}$$

A main advantage of the WDI method is that it allows for the nonlinearity of the aggregating function with different degree by setting $p \geq 2$. Evidently, the WDI method consists of a class of aggregating methods. If $p = 1$, the WDI method is the same as the SAW method.

In addition to the above aggregation methods, the non-compensatory MCDA approach has also been used to construct composite indicators, especially when ranking among different entities is the only consideration [32–34]. In general, two main steps are involved. In the fist step, an outranking matrix $(e_{kl})_{m \times m}$ is built based on a pair-wise comparison of different entities according to the whole set of sub-indicators using the following model:

$$e_{kl} = \sum_{j=1}^{n} (w_j(P_{kl}) + \tfrac{1}{2} w_j(I_{kl})) \quad k, l = 1, \cdots, n \,, \tag{54.4}$$

where $w_j(P_{kl})$ and $w_j(I_{kl})$ are respectively the weights of the sub-indicators presenting a preference and an indifference relation between entity *k* and entity *l*. In the second step, for each of $m!$ possible complete rankings of different entities an individual score is computed as the summation of e_{kl} over all the $\frac{m(m-1)}{2}$ pairs of entities. The ranking order with the maximum individual score is the final ranking of these entities in terms of their sustainability.

A main feature of non-compensatory MCDA approach is that it does not allow for the compensability among different sub-indicators. Therefore, it is consistent with the concept of strong sustainability [20]. The non-compensatory MCDA approach provides an explicit axiomatic system for constructing CSIs, by which the sources of technical uncertainty and imprecise assessment are reduced to the degree as small as possible [32–34]. A limitation of this approach is that it can only offer the ordinal information about the sustainability of different entities. Another limitation is that it is difficult to compute the scores for all the possible rankings when the number of entities becomes large.

As there are many MCDA aggregation methods, a problem in constructing CSIs is the choice of an appropriate method. With more emphasis given to the cardinality of composite indicators, Zhou *et al*. [64] recently developed an objective measure called the Shannon-Spearman measure for comparing alternative MCDA methods in constructing composite indicators. They found that the WP method may be the most appropriate since it could lead to the minimum information loss.

In using MCDA methods to construct CSIs, it is assumed that the weights for sub-indicators are given. In practice, it is challenging to determine such weights. A popular method for deriving the weights is the *analytical hierarchy process* (AHP), and Singh *et al*. [47] gave an illustration on how to use the AHP method to construct a CSI for the steel industry. In addition, such statistical techniques as factor analysis and principal component analysis can also offer a set of objective weights for sub-indicators for the aggregation purpose. More discussions on the comparisons of different weighting methods can be found in [35].

54.4.2 Data Envelopment Analysis Models for Constructing CSIs

Data envelopment analysis (DEA), developed by Charnes *et al*. [4], is a well established nonparametric approach used to evaluate the relative efficiency of a set of comparable entities with multiple inputs and outputs. Numerous DEA studies have so far been reported, *e.g.* [7, 15–18, 30, 40–42, 65, 67, 69]. In recent years, it has been increasingly used to construct composite indicators owing to its ability in combining multi-dimensional data into an overall index.

The use of DEA in constructing CSIs begin with the development of *environmental performance index* (EPI), which could be treated as a useful tool for assessing the environmental aspect of sustainable development. To do so, we first reconsider the relationships among various sub-indicators in a production framework. From the viewpoint of production theory, all the sub-indicators may be divided into three categories, namely *inputs, desirable outputs* and *undesirable outputs*. Their relationships can be modeled by a production technology. If we use $\mathbf{x}_i = (x_{i1}, \cdots, x_{iK})$, $\mathbf{y}_i = (y_{i1}, \cdots, y_{iL})$ and $\mathbf{u}_i = (u_{i1}, \cdots, u_{iS})$ to, respectively, denote the vectors of inputs, desirable outputs and undesirable outputs of entity i, the piecewise linear production technology given by the observed data can be modeled as:

$$\begin{aligned} T = \{(\mathbf{x},\mathbf{y},\mathbf{u}) : & \sum_{i=1}^{m} z_i x_{ik} \le x_k, k = 1, \cdots, K \\ & \sum_{i=1}^{m} z_i y_{il} \ge y_l, l = 1, \cdots, L \\ & \sum_{i=1}^{m} z_i u_{is} = u_s, s = 1, \cdots, S \\ & z_i \ge 0, i = 1, \cdots, m\} \end{aligned} \quad , \qquad (54.5)$$

In the literature, model (54.5) was coined as the environmental DEA technology which exhibits constant returns to scale [14]. More discussions on the properties and characterizations of various environmental DEA technologies can be found in [67].

Once the environmental DEA technology is specified, its incorporation with different types of efficiency measures would lead to a number of EPIs. For instance, Zaim and Taskin [62] applied the hyperbolic graph measure to construct an environmental efficiency index for comparing CO_2 emissions in OECD countries. Färe *et al*. [16] provided a formal approach to constructing an EPI by using the theory of Malmquist quantity index number. Using the idea in Färe *et al*. [16], Zaim [61] developed an aggregate pollution intensity index for measuring environmental performance of state manufacturing. More recently, Zhou *et al*. [69] proposed a non-radial DEA approach to measuring environmental performance.

Among the previous studies, the undesirable outputs orientation DEA type model (54.6) highlighted by Tyteca [49, 50], where the subscript "0" represents the entity to be evaluated, is particularly attractive. It provides an aggregated and standardized efficiency measure *REI*, *i.e.,* the optimum objective value of model (54.6), for measuring environmental performance. In addition, *REI* is the reciprocal of the Shephard input distance function used in Färe *et al*. [16] and Zaim [61]:

$$\begin{aligned} REI = \lambda^* = \min\ & \lambda \\ s.t.\ & \sum_{i=1}^{m} z_i x_{ik} \le x_{0k}, \quad k = 1, \cdots, K \\ & \sum_{i=1}^{m} z_i y_{il} \ge y_{0l}, \quad l = 1, \cdots, L \\ & \sum_{i=1}^{m} z_i u_{is} = \lambda u_{0s}, \quad s = 1, \cdots, S \\ & z_i \ge 0, \quad i = 1, \cdots, m \end{aligned} \quad , \qquad (54.6)$$

Despite its usefulness, model (54.6) has weak discriminating power in environmental performance comparisons since it use radial efficiency measure. As Zhou *et al*. [69] argued, the use of non-radial efficiency measures could improve its discriminating power by much. Nevertheless, model (54.6) as well as its extensions to non-radial cases can only model the environmental aspect of sustainability performance. This is due to the fact that these models are undesirable outputs oriented and consider only the environmental inefficiency. It is

reasonable to identify the economic inefficiencies and integrate them into *REI* to construct a CSI. Along this line, Zhou *et al*. [65] proposed the following slacks-based model for measuring economic inefficiencies after the environmental inefficiencies are eliminated:

$$\begin{aligned}\rho^* = \min\ & \frac{1-\frac{1}{K}\sum_{k=1}^{K} s_k^- / x_{0k}}{1+\frac{1}{L}\sum_{l=1}^{L} s_l^+ / x_{0l}} \\ s.t.\ & \sum_{i=1}^{m} z_i x_{ik} + s_k^- = x_{0k},\quad k=1,\cdots,K \\ & \sum_{i=1}^{m} z_i y_{il} - s_l^+ = y_{0l},\quad l=1,\cdots,L \\ & \sum_{i=1}^{m} z_i u_{is} = \lambda^* u_{0s},\quad s=1,\cdots,S \\ & z_i \geq 0,\quad i=1,\cdots,m; s_k^-, s_l^+ \geq 0\end{aligned} \tag{54.7}$$

The set of constraints on undesirable outputs in model (54.7) can guarantee that the entity evaluated has now been an efficient practitioner in the environmental aspect of sustainability. Therefore, model (54.7) can be used to evaluate the economic inefficiency of the entity evaluated by a slacks-based efficiency measure ρ^* after its pollutants are adjusted to their minimum levels. By integrating the pure environmental inefficiency and the economic inefficiency, Zhou *et al*. [65] proposed the following slacks-based environmental index:

$$SBEI = \lambda^* \times \rho^* . \tag{54.8}$$

Since *SBEI* combines environmental and economic inefficiencies, it could be treated as a composite indicator for modeling sustainability performance. A major feature of this index is that it puts environmental protection in the first position and economic development second. In addition, *SBEI* is also a standardized index because it lies in the interval (0,1] and satisfies the property "the larger the better".

Previous studies have shown that DEA models could offer an appealing framework to construct a CSI without the predetermination of weights for sub-indicators. However, since the approach is built on the production theory in economics, it requires the categorization of sub-indicators into inputs, desirable outputs and undesirable outputs. Considering the diversity of sub-indicators related to sustainable development, in some cases it may not be appropriate to treat them as inputs, desirable outputs and undesirable outputs in a unifying production framework.

54.4.3 An MCDA-DEA Approach to Constructing CSIs

As mentioned earlier, a critical issue in using MCDA aggregation methods to construct CSIs is the subjectivity in assigning weights for sub-indicators. Different weight combinations may lead to different ranking results and it is unlikely that all the entities would easily reach a consensus in determining an appropriate set of weights. In addition, it may not be easy to obtain the expert information for deriving the weights. Although previous DEA models could offer a framework for constructing a CSI without assigning the weights for sub-indicators, it still requires us to categorize sub-indicators into inputs, desirable outputs and undesirable outputs. To avoid these issues, the following model [43, 68], which combines the idea of DEA and the SAW method, can be used:

$$\begin{aligned}gI_i = \max\ & \sum_{j=1}^{n} w_{ij}^g I_{ij} \\ s.t.\ & \sum_{j=1}^{n} w_{ij}^g I_{kj} \leq 1,\quad k=1,\cdots,m . \\ & w_{ij}^g \geq 0,\ j=1,\cdots,n\end{aligned} \tag{54.9}$$

Model (54.9) provides an aggregated performance score for entity i in terms of its sustainability performance. By solving model (54.9) repeatedly for each entity, we will obtain a set of indexes $gI_1, gI_2, \cdots, gI_m$ for these entities. Note that the objective function in model (54.9) is externally similar to the SAW method. The main difference is that in model (54.9) the weights for sub-indicators are endogenous and changeable while in the SAW method they are exogenous and fixed. In essence, model (54.9) is an output maximizing multiplier DEA model with multiple outputs and constant

inputs. It should be pointed out that the approach proposed by Despotis [9, 10] to reassessing the *human development index* can be considered as an extension to model (54.9). More recently, Ramanathan [43] applied the same model to study a multi-criteria inventory classification problem.

In virtue of its DEA feature, model (54.9) can help each entity select the "best" set of weights for use. It avoids the subjectivity in determining weights and therefore provides each entity a relatively objective index for measuring sustainability. Nevertheless, if an entity has a value dominating other entities in terms of a certain sub-indicator, this entity would always obtain a score of 1 even if it has severely bad values in other more important sub-indicators. Furthermore, only model (54.9) may lead to the situation that a large number of entities have a performance score of 1 and further ranking among them becomes difficult. To address these issues, Zhou *et al*. [66] recently developed a model as follows:

$$\begin{aligned} bI_i = \min & \sum_{j=1}^{n} w_{ij}^b I_{ij} \\ s.t. & \sum_{j=1}^{n} w_{ij}^b I_{kj} \geq 1, \quad k = 1, \cdots, m . \\ & w_{ij}^b \geq 0, j = 1, \cdots, n \end{aligned} \tag{54.10}$$

Model (54.10) seeks the "worst" set of weights for each entity which are used to aggregate the sub-indicators into a performance score. Externally, model (54.10) is very similar to an input minimizing multiplier DEA model with multiple inputs and constant outputs. However, in model (54.10) all the sub-indicators are of the benefit-type and it is not appropriate to consider them as "inputs". It provides a way for further performance comparison among those incomparable entities only based on model (54.9).

The two indexes provided by models (54.9) and (54.10) are based on the weights that are most favourable and least favourable for each entity, which could only reflect partial aspects of an entity in terms of its sustainability performance. It is therefore logical and reasonable to combine them into an overall index by the following way:

$$I_i(\alpha) = \alpha \cdot \frac{gI_i - gI^-}{gI^* - gI^-} + (1-\alpha) \cdot \frac{bI_i - bI^-}{bI^* - bI^-}, \tag{54.11}$$

where $gI^* = \max\{gI_i, i = 1, \cdots, m\}$, $gI^- = \min\{gI_i, i = 1, \cdots, m\}$, $bI^* = \max\{bI_i, i = 1, \cdots, m\}$, $bI^- = \min\{bI_i, i = 1, \cdots, m\}$, and $0 \leq \alpha \leq 1$ is a control parameter. If $\alpha = 1$, $I_i(\alpha)$ is a normalized version of gI_i. If $\alpha = 0$, $I_i(\alpha)$ is a normalized version of bI_i. For other cases, $I_i(\alpha)$ is a compromise between the two indexes. If decision makers have no strong preference, $\alpha = 0.5$ would be a fairly neutral and reasonable choice.

Compared with models (54.9) and (54.10), model (54.11) provides a more encompassing CSI since it takes into account two extreme cases. It has been used to address a multi-criteria inventory classification problem in a recent study [68]. According to Zhou *et al*. [66], $I_i(\alpha)$ satisfies a number of desirable properties including the units invariant property. The units invariant property implies that it is not necessary to normalize the sub-indicators into dimensionless before aggregation.

Another desirable feature of the above procedure, *i.e.* models (54.9) –(54.11), is that they can easily incorporate some additional information about the weights for sub-indicators when they become available. In principle, this can be done by a number of methods as reviewed in [1]. Cherchye *et al*. [5, 6] and Mahlberg and Obersteiner [31] have given a few demonstrations on how to restrict the flexibility of weights. Zhou *et al*. [66] pointed out that the use of "proportion constraints" is more suitable for the current scenario because it is not difficult to have a consensus among decision makers or domain experts as to the relative importance of each sub-indicator. In addition, the "proportion constraints" type of weight restrictions has the desirable units invariant property [6].

From the above discussions we can find that models (54.9)–(54.11) offer a flexible and systematic procedure to constructing CSIs. Since the computation of $I_i(\alpha)$ integrates the ideas of MCDA and DEA, we may call the procedure

MCDA-DEA approach. The approach uses some DEA concepts while retaining the simplicity and ease of understanding of the SAW method. It simultaneously considers data weighting and aggregation in the process of constructing CSIs and avoids the procedure of data normalization.

54.5 An Illustrative Example

Consider then example where the sustainability performance of 30 OECD countries in 2002 are to be assessed based on the four sub-indicators namely, total primary energy supply, population, GDP and CO_2 emissions. Since the four sub-indicators could only reflect partial aspects of sustainability, the example is mainly used for illustration purposes rather than to provide any policy implications. The data were collected from the International Energy Agency [25] and their summary statistics can be found in [65].

We apply the group of MCDA methods (exclusive of the non-compensatory MCDA approach), the DEA models and the MCDA-DEA approach as described in Section 54.4 to compute the CSIs of the countries, respectively. The non-compensatory MCDA approach is not included because it can only give the rank indexes of the countries but will involve the computation and comparisons of scores for 30! rankings. For MCDA methods, the linear normalization procedure highlighted in [64] and equal weights ($w_1 = w_2 = w_3 = w_4 = 0.25$) setting are adopted. In the DEA models, total primary energy supply and population are taken as input, GDP as desirable output and CO2 as undesirable output. In terms of the MCDA-DAE approach, $\alpha = 0.5$ is used as the control parameter.

Table 54.2 shows the CSIs as well as the ranks of the 30 countries in the sequence of their CSI averages. It can be seen that the CSIs derived from MCDA methods are closely related, and so do those derived from DEA models. On the other hand, the CSIs based on the MCDA methods have no strong correlation with the CSIs based on the DEA models. These could be explained by the diverse intrinsic natures of MCDA and DEA. Interestingly, the CSIs from the MCDA-DEA approach have the relatively consistent correlation with the CSIs from other methods. It is likely due to the fact that the MCDA-DEA approach integrates the ideas of MCDA and DEA.

Not surprisingly, various aggregation methods could lead to different CSIs and even different rankings, which demonstrate the importance of selecting an appropriate aggregation method. In general, if it is appropriate to model sub-indicators in a production framework, DEA type models (54.6) to (54.8) are recommended since they have good theoretical foundation and can provide a CSI with higher discriminating power, *i.e.*, *SBEI*. In addition, their uses will not involve the determination of the weights for sub-indicators. Otherwise, the MCDA-DEA approach seems to be more suitable since the weights need not be predetermined. Besides, the MCDA-DEA approach can provide a flexible and encompassing index by the use of control parameter α. However, if the emphasis is on simplicity and ease of understanding, the WP method is recommended since it is simple and has some good theoretical properties compared with other MCDA methods [12, 64].

Table 54.2. CSIs of 30 OECD countries by alternative aggregation methods

Country	MCDA			DEA		MCDA-DEA
	SAW	WP	WDI (p=2)	REI	SBEI	
Luxembourg	0.459 (2)	0.133 (2)	0.016 (29)	1.000 (1)	1.000 (1)	0.417 (5)
Iceland	0.750 (1)	0.170 (1)	0.031 (17)	0.749 (8)	0.105 (14)	0.500 (2)
Ireland	0.091 (4)	0.058 (3)	0.019 (26)	1.000 (1)	0.522 (2)	0.399 (6)
Switzerland	0.060 (10)	0.049 (7)	0.023 (20)	1.000 (1)	0.253 (4)	0.537 (1)
Italy	0.044 (19)	0.017 (22)	0.023 (22)	1.000 (1)	0.409 (3)	0.227 (9)
Norway	0.069 (9)	0.053 (4)	0.029 (19)	0.914 (6)	0.210 (5)	0.195 (11)
United States	0.251 (3)	0.005 (30)	0.047 (9)	0.501 (15)	0.157 (9)	0.500 (3)
Austria	0.051 (14)	0.042 (9)	0.040 (11)	0.686 (9)	0.165 (8)	0.444 (4)
New Zealand	0.084 (6)	0.053 (5)	0.433 (1)	0.487 (18)	0.078 (19)	0.213 (10)
Denmark	0.072 (8)	0.050 (6)	0.053 (7)	0.581 (10)	0.140 (10)	0.398 (7)
Sweden	0.042 (20)	0.040 (11)	0.031 (18)	0.969 (5)	0.180 (6)	0.026 (21)
France	0.045 (17)	0.016 (23)	0.036 (15)	0.825 (7)	0.165 (7)	0.067 (18)
Netherlands	0.030 (25)	0.026 (17)	0.289 (2)	0.491 (17)	0.099 (17)	0.140 (12)
Spain	0.031 (23)	0.019 (19)	0.060 (5)	0.553 (13)	0.107 (13)	0.250 (8)
Portugal	0.053 (13)	0.039 (12)	0.083 (4)	0.555 (12)	0.103 (15)	0.119 (15)
Japan	0.085 (5)	0.010 (29)	0.037 (13)	0.540 (14)	0.113 (12)	0.140 (13)
United Kingdom	0.044 (18)	0.015 (25)	0.020 (25)	0.565 (11)	0.121 (11)	0.128 (14)
Germany	0.057 (11)	0.012 (28)	0.023 (21)	0.496 (16)	0.100 (16)	0.077 (17)
Greece	0.047 (16)	0.035 (14)	0.054 (6)	0.418 (24)	0.077 (20)	0.083 (16)
Hungary	0.054 (12)	0.038 (13)	0.017 (27)	0.470 (21)	0.067 (22)	0.037 (20)
Belgium	0.034 (22)	0.031 (15)	0.040 (10)	0.484 (19)	0.089 (18)	0.005 (28)
Mexico	0.030 (24)	0.014 (27)	0.035 (16)	0.481 (20)	0.066 (23)	0.017 (22)
Finland	0.051 (15)	0.040 (10)	0.014 (30)	0.427 (23)	0.070 (21)	0.017 (23)
Poland	0.024 (30)	0.018 (21)	0.250 (3)	0.282 (29)	0.034 (28)	0.000 (30)
Turkey	0.026 (28)	0.018 (20)	0.022 (24)	0.453 (22)	0.061 (24)	0.006 (27)
Slovak Republic	0.076 (7)	0.044 (8)	0.050 (8)	0.319 (27)	0.032 (29)	0.061 (19)
Canada	0.030 (26)	0.015 (24)	0.023 (23)	0.339 (26)	0.057 (25)	0.014 (24)
Korea	0.027 (27)	0.014 (26)	0.036 (14)	0.340 (25)	0.044 (27)	0.009 (26)
Australia	0.026 (29)	0.020 (18)	0.016 (28)	0.307 (28)	0.056 (26)	0.003 (29)
Czech Republic	0.036 (21)	0.029 (16)	0.038 (12)	0.258 (30)	0.031 (30)	0.010 (25)
Mean	0.093	0.037	0.063	0.583	0.157	0.168
Standard Dev.	0.150	0.035	0.093	0.238	0.192	0.178

54.6 Conclusion

Indicators have been widely used to assess sustainability performance. Many indicators for sustainability have been developed, among which some are non-composite while others are composite indicators. We give an overview on indicators for sustainability. From the viewpoint of operations research, we describe the methods for constructing composite sustainability indicators (CSIs) and highlight the usefulness of MCDA and DEA. We introduce the so-called MCDA-DEA approach as a suitable method for constructing CSIs since it incorporates the good features of the DEA approach and the SAW method. We then present an illustrative example for assessing alternative aggregation methods in constructing CSIs. Some general guidelines on the selection of an appropriate aggregation method are also presented.

References

[1] Allen R. Athanassopoulos A, Dyson RG, Thanassoulis E, Weights restrictions and value judgements: evolution, development and future directions. Annals of Operations Research 1997; 73:13–34.

[2] Ang BW. Monitoring changes in economy-wide energy efficiency: from energy-GDP ratio to composite efficiency index. Energy Policy 2006; 34:574–582.

[3] Callens I, Tyteca D. Towards indicators of sustainable development for firms: a productive efficiency perspective. Ecological Economics1999; 28:41–53.

[4] Charnes A. Cooper WW, Rhodes E. Measuring the efficiency of decision making units. European Journal of Operational Research 1978; 2:429–444.

[5] Cherchye L, Lovell CAK, Moesen W, van Puyenbroeck T. One market, one number? A composite indicator assessment of EU internal market dynamics. European Economic Review. 2007; 51:749–779.

[6] Cherchye L, Moesen W, Rogge N, van Puyenbroeck T. An introduction to "benefit of the doubt" composite indicators. Social Indicators Research, 2007; 82:111–145.

[7] Cooper WW, Seiford LM, Tone T. Introduction to data envelopment analysis and its uses: with DEA-Solver software and references. Springer, New York 2006

[8] Choi HC, Sirakaya E. Sustainability indicators for managing community tourism. Tourism Management 2006; 27:1274–1289.

[9] Despotis DK. Measuring human development *via* data envelopment analysis: the case of Asia and the Pacific. Omega 2005; 33:385–390.

[10] Despotis DK. A reassessment of the human development index *via* data envelopment analysis. Journal of the Operational Research Society 2005; 56:969–980.

[11] Diaz-Balteiro L, Romero C. In search of a natural systems sustainability index. Ecological Economics 2004; 49:401–405.

[12] Ebert U, Welsch H. Meaningful environmental indices: A social choice approach. Journal of Environmental Economics and Management 2004; 47:270–283.

[13] Esty DC, Levy MA, Srebotnjak T, de Sherbinin A. 2005 Environmental sustainability index: Benchmarking national environmental stewardship. Yale Center for Environmental Law and Policy, New Haven, CT, 2005.

[14] Esty DC, Levy MA, Srebotnjak T, de Sherbinin A, Kim CH, Anderson B. Pilot Environmental Performance Index. Yale Center for Environmental Law and Policy, New Haven, CT, 2006.

[15] Färe R, Grosskopf S. Modeling undesirable factors in efficiency evaluation: comment. European Journal of Operational Research 2004; 157:242–245.

[16] Färe R, Grosskopf S, Hernández-Sancho F. Environmental performance: An index number approach. Resource and Energy Economics 2004;26:343–352

[17] Färe R, Grosskopf S, Lovell CAK. Production Frontiers. Cambridge University Press, New York, 1994.

[18] Färe R, Grosskopf S, Tyteca D. An activity analysis model of the environmental performance of firms – Application to fossil-fuel-fired electric utilities. Ecological Economics 1996; 18:161–175.

[19] Gagliardi F, Roscia M, Lazaroiu G. Evaluation of sustainability of a city through fuzzy logic. Energy. 2007; 32: 795–802.

[20] Gutes MC. The concept of weak sustainability. Ecological Economics 1996; 17:147–156.

[21] Hanley N, Moffatt I, Faichney R, Wilson M. Measuring sustainability: A time series of

alternative indicators for Scotland. Ecological Economics1999; 28:55–73.
[22] Hezri A, Dovers SR. Sustainability indicators, policy and governance: Issues for ecological economics. Ecological Economics 2006; 60:86–99.
[23] Hunter C, Shaw J. The ecological footprint as a key indicator of sustainable tourism. Tourism Management 2007; 28:46–57
[24] Energy indicators for sustainable development: Guidelines and methodologies. International Atomic Energy Agency (IAEA). Vienna, 2005.
[25] CO_2 emissions from fuel combustion: 1971-2002. International Energy Agency, OECD, Paris, 2004.
[26] Kang SM. A sensitivity analysis of the Korean composite environmental index. Ecological Economics 2002; 43:159–174.
[27] Kemmler A, Spreng D. Energy indicators for tracking sustainability in developing countries. Energy Policy 2007; 35:2466–2480.
[28] Kratena K. Ecological value added' in an integrated ecosystem-economy model – An indicator for sustainability. Ecological Economics 2004; 48:189–200.
[29] Labuschagne C, Brent AC, van Erck RPG. Assessing the sustainability performances of industries. Journal of Cleaner Production 2005; 13:373–385.
[30] Lovell CAK, Pastor JT, Turner JA. Measuring macroeconomic performance in the OECD: A comparison of European and non-European countries. European Journal of Operational Research 1995; 87:507–518.
[31] Mahlberg B, Obersteiner M. Remeasuring the HDI by data envelopment analysis. International Institute for Applied Systems Analysis (IIASA), Interim Report IR-01-069, Laxemburg, Austria, 2001.
[32] Munda G, Nardo M. On the methodological foundations of composite indicators used for ranking countries. Proceedings of the First OECD/JRC Workshop on Composite Indicators of Country Performance, Ispra, JRC, 2003.
[33] Munda G. "Measuring sustainability": a multi-criterion framework. Environment. Development and Sustainability 2005; 7:117–134.
[34] Munda G. Multiple criteria decision analysis and sustainable development. In: Figueira J, Greco S, Ehrgott M, editors. Multiple criteria decision analysis: State of the art surveys. Springer, Boston, 2005; 953–988.
[35] Nardo M, Saisana M, Saltelli A, Tarantola S, Hoffman A, Giovannini E. Handbook on constructing composite indicators: Methodology and user guide. OECD Statistics Working Paper OECD 2005; 3.
[36] Ness B, Urbel-Piirsalu E, Anderberg S, Olsson, L. Categorising tools for sustainability assessment. Ecological Economics 2007 60:498–508.
[37] Olsthoorn X, Tyteca D, Wehrmeyer W, Wagner M. Environmental indicators for business: a review of the literature and standardization methods. Journal of Cleaner Production 2001; 9:453–463.
[38] Pillarisetti JR. The World Bank's "genuine savings" measure and sustainability. Ecological Economics 2005; 55:599–609.
[39] Pearce DW, Atkinson GD. Capital theory and the measurement of sustainable development: an indicator of 'weak' sustainability. Ecological Economics 1993; 8:103–108.
[40] Ramanathan R. Combining indicators of energy consumption and CO_2 emissions: A cross-country comparison. International Journal of Global Energy Issues 2002; 17:214–227.
[41] Ramanathan R. An introduction to data envelopment analysis: A tool for performance measurement. Sage Publications, New Delhi, 2003
[42] Ramanathan R. An analysis of energy consumption and carbon dioxide emissions in countries of the Middle East and North Africa. Energy 2005;30:2831–2842
[43] Ramanathan R. ABC inventory classification with multiple-criteria using weighted linear optimization. Computers and Operations Research 2006; 33:695–700.
[44] Rennings K, Wiggering H. Step towards indicators of sustainable development: Linking economic and ecological concepts. Ecological Economics 1997; 20:25–36.
[45] Sagar AD, Najam A. The human development index: a critical review. Ecological Economics 1998; 25:249–264.
[46] Saisana M, Saltelli A, Tarantola S. Uncertainty and sensitivity analysis techniques as tools for the quality assessment of composite indicators. Journal of the Royal Statistical Society A 2005; 168:307–323.
[47] Singh RK, Murty HR, Gupta SK, Dikshit AK. Development of composite sustainability performance index for steel industry. Ecological Indicators, 2007; 7(3):565–588.

[48] Triantaphyllou E. Multi-criteria decision making methods: a comparative study., Boston, 2000.
[49] Tyteca D. On the measurement of the environmental performance of firms – A literature review and a productive efficiency perspective. Journal of Environmental Management 1996; 46:281–308.
[50] Tyteca D. Linear programming models for the measurement of environmental performance of firms - concepts and empirical results. Journal of Productivity Analysis 1997; 8:183–197.
[51] Ugwu OO, Haupt TC. Key performance indicators and assessment methods for infrastructure sustainability – A South African construction industry perspective. Building and Environment 2007; 42:665–680.
[52] United Nations Commission on Sustainable Development (UNCSD), Indicators of Sustainable Development: Guidelines and Methodologies. United Nations, New York, 2001.
[53] United Nations Development Program (UNDP), Human Development Report 2005. Oxford University Press, New York, 2005.
[54] Van den Bergh. JCJM, Ecological economics and sustainable development. Edward Elgar, Cheltenham, 1996.
[55] Wackernagel M, Rees WE. Our ecological footprint: Reducing human impact on the earth. New Society Publishers, Gabriola Island, 1996.
[56] World Bank, World Development Indicators 1999. World Bank, Washington, DC, 1999.
[57] World Commission on Environment and Development (WCED), Our Common Future. Oxford University Press, Oxford, 1987.
[58] World Wildlife Foundation (WWF), Living Planet Report 2004. Gland, Switzerland, 2004.
[59] Yoon KP, Hwang CL, Multiple attribute decision making: An introduction. SAGE Publications, Thousand Oaks, CA, 1995.
[60] Yuan W, James P, Hodgson K, Hutchinson SM, Shi C. Development of sustainability indicators by communities in China: A case study of Chongming County, Shanghai. Journal of Environmental Management 2003; 68:253–261.
[61] Zaim O. Measuring environmental performance of state manufacturing through changes in pollution intensities: a DEA framework. Ecological Economics 2004; 48:37–47.
[62] Zaim O. Taskin F. Environmental efficiency in carbon dioxide emissions in the OECD: a non-parametric approach. Journal of Environmental Management 2000; 58:95–107.
[63] Zeleny M. Multiple criteria decision making. McGraw-Hill, New York, 1982.
[64] Zhou P, Ang BW, Poh KL. Comparing aggregating methods for constructing the composite environmental index: an objective measure. Ecological Economics 2006; 59(3):305–311.
[65] Zhou P, Ang BW, Poh KL. Slacks-based efficiency measures for modeling environmental performance. Ecological Economics 2006; 60(1):111–118.
[66] Zhou P, Ang BW, Poh KL. A mathematical programming approach to constructing composite indicators. Ecological Economics, 2007; 62(2):291–297.
[67] Zhou P, Ang BW, Poh KL. Measuring environmental performance under different environmental DEA technologies. Energy Economics, 2008; 30: 1–14.
[68] Zhou P, Fan L. A note on multi-criteria ABC inventory classification using weighted linear optimization. European Journal of Operational Research; Nov.2007; 182(3):1488–1491.
[69] Zhou P, Poh KL, Ang BW. A non-radial DEA approach to measuring environmental performance. European Journal of Operational Research 2007; 178(1):1–9.

55

Sustainable Technology

Ronald Wennersten

Royal Institute of Technology, School of Energy and Environmental Technology
Department of Industrial Ecology, Sweden

Abstract: Technology has increased the capabilities of mankind during the last 100 years in a revolutionary way. We are now, however, facing a totally new situation where we can see obvious signs of dysfunctions in planetary processes like climate change, globally spread synthetic chemicals, *etc.* At the same time, as we have realized that "the sky is the limit", there is an even more vigorous reliance on technology. Many researchers, politicians and company leaders have strong faith in that new technologies will solve the problems. Sustainable technology cannot exist as such. Technological change as well as societal change is needed in order to steer technology towards sustainability. These changes can only be achieved through a combination of top-down and bottom-up processes. Top-down processes will have to engage co operation between governments, business NGOs as well as other powerful institutions. Bottom-up movements will be built on small-scale socio-technical experiments by local authorities and citizens groups, innovative professionals and entrepreneurs, artists and other out-of-the-box thinkers. Technological change is a path-dependent process which can cause severe lock-in effects. The choices made in the past will restrict our possibilities today. In a similar way, our choices today have consequences for the range of options left open to future generations. It is important for society to try to foresee the impact of technological change, so that the merits of such change can be discussed in a democratic process. Against this background tomorrow's technicians need to have a comprehensive view based on studies of economy, sociology and ecology where the consequences of the technology and driving forces for sustainable development are central. In such a process, visions based on scenario techniques, will be important tools for creating visible pathways to a more sustainable future.

55.1 Introduction

Technology has increased the capabilities of mankind during the last 100 years in a revolutionary way. At the same time this development has lead to large negative effects on the global environment as well as major changes in social behaviour of people. More than 50% of the population on earth is now living in cities with new consumption behaviours. We are facing a serious situation where we can see obvious signs of dysfunctions in planetary processes like climate change, globally spread synthetic chemicals *etc.*

At the same time, as we have realized that "the sky is the limit", there is an even more vigorous reliance on technology. Many researchers,

politicians and company leaders have strong faith in that new technologies will solve the problems. It is like an ever ongoing process that new technology should solve the problems that technology has created. This reversed way of handling the situation has turned out to be increasingly costly, but we just do not seem have the knowledge and tools to control the development.

This paper will address the role of technology in directing our societies towards more sustainable pathways. One of the key questions to discuss is if there are such thing as sustainable technologies and how we can distinguish these technologies from non sustainable technologies.

The success of technology is partly based on the success of natural science with its ability to quantify natural phenomena and in using mathematical models for creating possibilities to make predictions. At the top of this hierarchy are the basic sciences like physics and chemistry where a very limited system can be modeled with great "exactness". The natural sciences have formed a penetrating norm for "good science" also influencing social sciences. It is important to realize that the success story of science and technology is precisely based on specialization and strict limitation of the system borders. The tackling of problems concerning sustainable development, however, imply the opposite, generality and wide system boundaries. Another important conception is that science is objective and free of value judgments. Scientists and engineers are expected to deliver an objective expert judgment allowing politicians to make the most rational decisions. This conception has to be questioned at many levels.

55.2 What Is Technology for?

It should be clear that the intention here is not to appraise what is good or bad in these perceptions, but rather to conduct an unbiased discussion of the role of technology and the engineer in the development of a sustainable society. A rather broad definition of the concept technology will be adopted namely:

- Science of industrial arts and manufactures
- Applied science
- All means employed by a social group to provide material comforts

Technology defined in this way includes:

- New materials as nano materials, polymers
- Products as mobile phones, cars, medicines
- Processes as environmental technologies
- Production technologies as biotechnology

There is an on going discussion about the hen and the egg whether technology is pushed into the society or dragged by consumer demand. Most people, however, agree upon the statement that technology is one of the most important factors for economic development and also the main factor for the progress in many sectors like in construction, agriculture, transport, and energy.

There are, however, a lot of signs that technology in itself is not the sole solution for many of the real underlying problems of human beings and below are a few examples of this:

- In spite of the fact that the market is full of technology intended to save time, many people feel that they have less and less time for themselves.
- The IT-industry provides us with technology to improve the communication between people and still, more and more people experience isolation and lack of close human contact.
- Increasingly efficient technologies in the fishery industry have resulted in rapid fish depletion in the seas.
- The car industry provides proof of impressive development of car performance. Cars are, however, still one of the major threats to sustainability in cities and for the emission of green house gases.
- Combating poverty – a central subject for discussion in the Johannesburg conference – has not demonstrated success through the development of science and technology.

Many more examples could be listed, but these demonstrate anyway how the development of technology takes place as a partly aimless stroll in

a maze due to the knowledge fragmentation, that is precisely the basis for its success. It is obvious that many people have experienced a better life through technology development, but the question is more how we proceed further on. There might be so that the level where more products are not raising the quality of life for people has been reached in many developed countries. New lifestyles and values have to be found.

The development of technology is more and more controlled by relatively short-term micro-economical goals. This results in an appearance of technical and economical rationality on the micro level. However it appears technically and economically irrational on the macro level when it comes to damages to and depletion of ecological systems and natural resources, and difficulties in satisfying the basic human needs on a global scale. This situation is very much conserved through a one-sided focus on the micro-economical level in education and research at the technical universities, stressing the possibilities for patenting and commercial exploitation of results.

What should be counted at the end, *i.e.*, the real effects on people, needs and values, cannot be understood and described on the micro level with its strict system boundaries. Individual human behavior is too complex and we have to adapt constantly to new knowledge and experience, making the use of historical data uncertain. Human values also have a cultural basis depending on the social environment, which is also an important part of sustainable development. The main question to discuss here is if technological change has an important role in sustainable development or if sustainable development belongs to a class of human problems which has been classified as "no technical solution problems" [1].

55.3 The Linear Production System

The industrialized society is built upon a more or less linear transformation of natural resources into different goods and at the end waste, as shown in Figure 55.1, utilizing more and more sophisticated technologies. This transformation has been possible only through the use of cheap "unlimited" resources of fossil fuels. It is important to understand that the cornerstones of this system were starting to shake only 50 years ago with the signs of serious global environmental effects and the oil crisis. We now have the technological tools to affect the carrying capacity of the global eco systems. We can no longer move the problems to other areas on earth as we have constantly done in the past. However it seems that we are more and more locked in concerning technological systems depending on fossil fuels. This dependence is both structural and institutional. There is an immense infrastructure that supports the existing technological systems. The ways we develop technologies are hidden in our research, educational and funding institutions. It is also more or less hidden from public control in the democratic process.

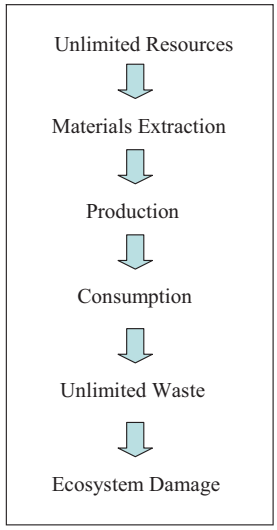


Figure 55.1. The linear production system

55.4 Is Globalization a Solution?

Today we are facing a situation where cheap material and fossil fuel resources are becoming scarcer. Globalization has stimulated the use of energy even more. Oil and gas demand is high and growing, so much that the world today consumes twice as much oil as is found. Countries like China and India, who cannot escape the technological lock-in, have ever growing energy needs. The

world does and will continue to depend primarily on oil coal, and gas for our energy requirements now and into the foreseeable future. The cost for developing new fossil resources also seems to increase exponential in spite of technological development.

Liberal economists argue that the raising demand for resources will create markets for the development of new technologies both for renewable energy sources but also in exploiting new reservoirs for fossil fuels. This development is, however, highly dependent on a stable political situation which can favor a continuous growth of the global market.

The situation is now that the places with the greatest demand for fossil fuels cannot supply their own needs. Over the next few decades, oil and gas production in the North Sea, North America and China are expected to fall, or rise too little to keep pace with demand. Only a few places have surplus reserves—chiefly the Middle East, Africa and Russia. Decision-makers in the energy industry, government, and international agencies thus face difficult decisions. How will the supply-demand problem be resolved? One possibility is a continuation of globalization. According to this vision, free markets will ensure that investment capital and fossil fuels are distributed efficiently [2]. At the other extreme is a future that involves more regulation and confrontation. Rather than free markets, anxious governments will decide how capital and energy supplies are apportioned. Rather than globalization, this would be "deglobalization" with a continuation of the "old ways" of bi-lateral political agreements securing point to point long term supply lines and markets. We can see many signs of such a development today. China is very active in developing bi-lateral cooperation in Africa to secure supplies of energy and mineral resources as well as gaining control of transport routes, *e.g.*, directly pipe crude from the Middle East to Xingjian. United States has a global strategy for securing energy supplies where the Middle East has a central role as well as controlling transport routes, *e.g.*, the Strait of Malacca. Lately they have announced a more active strategy for controlling resources also in Africa.

Russian energy group Gazprom has recently stated in a press release [3] that they will develop the Shtokman field without foreign partners. The Shtokman gas condensate deposit lies in the Barents Sea, in the north of Russia. The Shtokman gas will instead be piped to European markets. The Gazprom change in policy came as a total surprise for large multinational oil companies who had expected to get possibilities to take part in the exploration of the vast gas field. The dependence on fossil fuels of our industrial system is thus more and more becoming a security problem threatening the globalization process.

55.5 Technology Lock-in

Technology-lock in has been discussed from the point of view that mature technologies have developed comparative advantages over a long time with the effect that new technologies have difficulties for break through. One example of this is the gasoline car, which have been developed for more than 100 years, and where we now have an established infrastructure with gas stations, reparation facilities, *etc.* [4]. This situation will effectively hinder the development of alternative technologies for cars.

This lock-in effect is even more serious if we look at higher system levels. Incremental innovations in existing technology chains and even replacement of single technologies with new technologies within the existing framework can usually be favoured by research and development effects, legislation, subsidiaries, *etc.* The industrial system, based on the principles discussed earlier, has, however, created a lock-in effect which is deeply rooted at many levels, structural and institutional. For many reasons the focus on technological development is on a low system level while the problems often arise on a higher system level incorporating many types of technologies. An "environmentally friendly" bulldozer running on hydrogen that it is used to destroy rain forest cannot be classified as sustainable technology.

The development of new technologies is not a straight forward process following the development of science. Many important inventions like

the steam engine was invented before the basic principles of thermodynamics were evolving. However it is obvious in many ways that technology development is becoming more and more controlled by scientific development.

The knowledge of the processes for technological change among developers is limited. Engineers often know as little of technological change as a fish knows about hydrodynamics. The innovation process is also complex and it can be difficult to foresee the end products. As technological tools increase in complexity, so does the type of knowledge needed to support them. Complex modern machines require libraries of written technical manuals of collected information that has continually increased and improved. Their designers, builders, maintainers, and users often require the mastery of decades of sophisticated general and specific training given at our engineering faculties. Moreover, these tools have become so complex that a comprehensive infrastructure of technical knowledge-based tools, processes and practices exist to support them. Complex manufacturing and construction techniques and organizations are needed to construct and maintain them. Entire industries have arisen to support and develop succeeding generations of increasingly more complex tools.

This situation has created an extremely complicated lock-in situation which will hinder radical changes in technological systems to evolve, systems based on more sustainable solutions. The existing ways of technology transfer to developing countries also favors the development of similar lock-in effects in these countries.

It is thus obvious that the evolution of sustainable technology systems will call for major changes in innovation processes, public participation, education, *etc.*

55.6 From Techno-centric Concerns to Socio-centric Concerns

55.6.1 Changing the Focus

In order to achieve a major change in the development of sustainable technologies, it is of great importance to understand the driving forces and institutional infrastructures for technology development. If we are going to develop really sustainable technologies, we have to understand these driving forces and let this knowledge affect areas like innovation processes, education, *etc.*, in a more fundamental way than today.

The development of technologies has had different driving forces and concerns through history. In the early civilizations the driving force for technology development has been necessity in the struggle for survival which has been formulated in the phrase “necessity is the mother of invention”. To support a growing population new technologies in, *e.g.*, agriculture developed. In this phase we can say that the development was both techno-centric and socio-centric, but less eco-centric. The technology had to extend the ability to perform different tasks but it had also an important cultural role. The environmental issues were of less importance simply because the effects were minor and people could move around if negative effects occurred.

Starting from the industrial revolution the development of technologies was very much techno-centric. The focus for technology development was mainly on technical and economical viability. People had to adapt to the mayor changes in culture when they moved from rural areas into the growing cities. This situation is obvious today in many developing countries. The large improvements of the abilities of technologies, which was made possibly through machineries and cheap fossil fuels created a new situation. When serious environmental effect reached a level that it threatened economic growth, end of pipe technology solutions were gradually developed. From the beginning there was a resistance from industry towards increasing costs connected to environmental concern, but today this is accepted in the developed economies and there is even a large and viable market for products in this area. The change in concerns has evolved gradually through the process shown in Figure 55.2.

Today it is hard to see that the development of technology is really that of necessity. Flat screen TVs have hardly been produced as a result of necessity. The development today is more a result

of temporary resource abundance. In this situation the globalization with new growing markets is of central importance for the world economy.

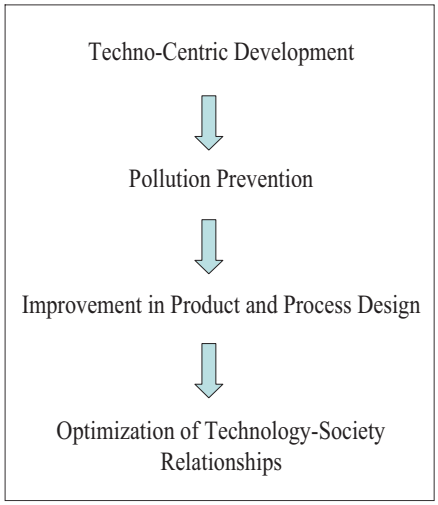


Figure 55.2. Evolution of technology in relation to environment and society

Following this development concepts like cleaner production and Design for Environment (DSE) have developed towards eco-centric concerns. Environmental concerns have been gradually more integrated in the company activities through different management system like ISO 14001.

However the existing paradigm is still that technology is considered largely in isolation from the environmental, social, political, and economic processes that shape it – processes that are themselves shaped, altered and adapted by technology. Optimization of technology–society relationships is still hardly developed. An approach like DSE aims to minimize the environmental consequences of human activities through modification of technological artefacts. An important tool for this is life cycle analysis. At the company level, this translates into the application of environmental constraints to traditional business beliefs and behaviours. The goal is one of optimization through the development of existing relationships and marginal modifications of industrial systems. This is one important effect of lock-in on the existing system level. Radical changes are very difficult to achieve.

55.6.2 Towards a More Holistic View

A more holistic conceptualization of technology, however, directs attention away from the technological artefacts toward the knowledge, relationships, values and assumptions that underpin technological choices. Greener, cleaner, more environmentally friendly technology is no longer the means to more sustainable paths. Rather the goal should be design for society (DFS). technology from this perspective is the product of a complex set of relationships internal and external to the company, many beyond its direct control.

Designing for and within society extends research and practice of technology management and development beyond the traditional frameworks of engineering and management decision making and asks fundamental questions about the nature and the role of companies and technologies in their social and environmental contexts. DFS would include a more holistic view of techno-centric, eco-centric, and socio-centric concerns as shown in Figure 55.3.

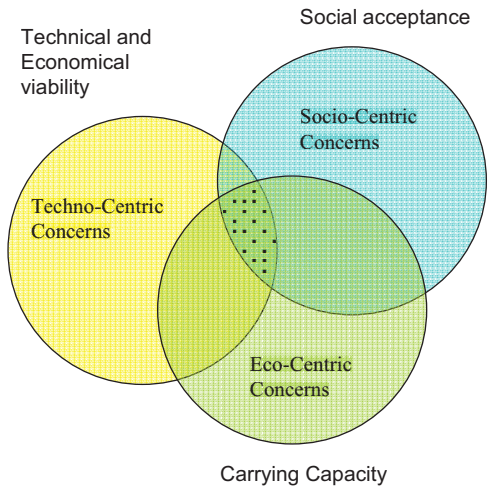


Figure 55.3. The relation between eco-centric, techno-centric, and socio-centric concerns

DFS would include important moral aspects like equity and justice concerning existing and future generations. A conclusion from this is that a radical change in this process cannot be achieved by multi national companies or institutions.

It can only be changed through a democratic process involving broad participation from society. The social question is probably the key issue to solve for stopping rebound effects with the development of technology. It is human behaviour and the resulting social dynamics that lie at the heart of today's social and ecological problems.

Social sustainability is dependent on ecological sustainability for maintaining the carrying capacity of the living systems. On the other hand ecological sustainability has become dependent on social sustainability. With a growing population, constrained in their abilities to meet their needs, it becomes increasingly difficult to protect the environment and even more to save resources for future generations.

If one today should try to sum up the misery of the world, the reason for this misery would in a very limited extension be due to the fact that the industrialized countries have invented too few technical products that can be sold. In this context it is also interesting to look at "Millennium Development Goals" formulated by UN. In the beginning of the new millennium there was an important worldwide, international consensus decision about development goals and actions: The eight goals that were established were:

- Eradicate extreme poverty and hunger,
- Achieve universal primary education,
- Promote gender equality and empower women,
- Reduce child mortality,
- Improve maternal health,
- Combat HIV/AIDS, malaria and other diseases,
- Ensure environmental sustainability,
- Develop a global partnership for development.

This is a clear example of the necessity to include the socio-centric concern in formulating sustainability targets and objectives. A changing view towards design for society will have a profound effect on the way technology is developed. In order for this more holistic approach to evolve, we will need fundamental changes in the society initiated by a broad discussion among all stakeholders. Key issues will be the change in how we educate engineers and the development of a technological culture in society with a broad public participation.

55.7 Technology and Culture

The evolution of science and technology has formed a strong belief in the concept of progress in society. The idea was conceived and developed mainly by science and is based on a new picture of the world and the premise that science views itself as an infinitely developing system of knowledge and a way of remaking the world. Therefore progress became one of the industrial-society ideology's pillars and the idea of progress might be one of the most important corner stones in the western society. It might also be natural that in a world of change, time is perceived as some linear property while in a old nomad culture with very little change, time is a more circular property.

We have now reached a state where we slowly are coming to realize that this line of progress is by no way guaranteed in the evolutionary process. If we do not change our paths to become more sustainable for all life forms, then we will go the same way as every other life form that failed to adapt to the carrying capacities of the eco systems.

Changes in production systems and cultural changes go hand in hand. The gradual process of industrialization imposed one of the most radical shifts in living conditions and culture in human history. Technical innovations not only changed working conditions, but forced profound social change on the whole fabric of society, upon human relations and the individual's perception of time and space. This rapid change at all levels in our society and the dependence on technology has also created a fundamental criticism towards science and technology as the fundaments for the industrial development and globalization.

The author Paul Virilio has focused on speed as one of the most important factors and threats in our society where the fast development of technology is seen as one of the main threats to human beings. In an interview he says [5]:

> *"This means that history is now rushing headlong into the wall of time. As I have*

> *said many times before, the speed of light does not merely transform the world. It becomes the world. Globalization is the speed of light. And it is nothing else! Globalization cannot take shape without the speed of light. In this way, history now inscribes itself in real time, in the 'live', in the realm of interactivity." "But we must engage in resistance first of all by developing the idea of a technological culture." "For example, we have developed an artistic and a literary culture. Nevertheless, the ideals of technological culture remain underdeveloped and therefore outside of popular culture and the practical ideals of democracy. This is also why society as a whole has no control over technological developments. And this is one of the gravest threats to democracy in the near future. It is, then, imperative to develop a democratic technological culture."*

In the Western societies, with an increasingly faster metabolism, people often experience a gap between their human ambitions and real life. They have less time to fulfil their ambitions which are steadily growing. There is also a growing skepticism towards politicians and experts which creates fundamental difficulties when new technologies are introduced. If we want to rely on democratic processes we have to accept that technology development is a part of society and should be discussed more broadly in. Civil society will have a fundamental role in a transition to a more sustainable society. A system where people are involved in democratic processes is the best organization for a fair distribution of goods and power, and for minimizing the perils of life.

55.8 Technology and Risk

An important and complex issue is the relation between technology and risk. What kind of new risks will be introduced with new technologies and how can we assess them from a sustainability point of view? Each wave of technology trend to create a set of waste previously unknown by humans, *e.g.*, toxic waste, radioactive waste, electronic waste.

There are numerous of examples when new technologies have created new risks which were revealed many years after their introduction. One of the more well known is the introduction of the chemical DDT. In 1948 the Swiss chemist Paul Hermann Müller won the Nobel Prize for his discovery of DDT, an insecticide useful in the control of malaria, yellow fever and many other insect-vector diseases. The substance was regarded as a miracle agent to control insects and it was used widely and in large amounts. About 40 ears later signs of serious effects on the environment showed up. DDT accumulated in the food chain and affected reproduction of animals high up in this chain, *e.g.*, seals. The first debate about this was created in the 1960s by Rachel Carson with her book "Silent Spring".

The effects of technology on the environment are both obvious and subtle. The more obvious effects include the depletion of non renewable natural resources (such as petroleum, coal, ores), and the added pollution of air, water, and land. The more subtle effects include long-term effects like global warming, deforestation, natural habitat destruction, and coastal wetland loss.

The history shows us that the delay of revealing risks with new technologies could be as long as 50 years and then the damage to environment could be severe. At the same time there is a constant stream of unsystematic alarms from media around new technologies, alarms which are very difficult to handle for politicians and the public. Are we introducing new "DDTs" today? Chemicals like Perfluorinated chemicals (PFCs) and their precursors is a group of chemicals widely used in a range of consumer, *e.g.*, non-stick coatings on items such as cooking pans, and stain repellent coatings on everything from carpets and furniture to microwave popcorn bags and fast-food packaging. Although more research is needed, existing studies have shown that perfluorinated chemicals are extremely persistent and bio accumulative, as well as probably cancer-causing and hormone disrupting. Recent research has indicated that a major source of PFCs in the environment is the migration of PFC precursors from consumer products; in other words, PFCs are leaking from our products into the environment.

Examples of new technologies being introduced without comprehensive risk assessment are:

- Nano materials,
- Genetically modified crops and food,
- Gene therapy,
- Energy technologies, *e.g.*, fusion.

There are three important questions to rise in accordance to this:

1. How can we assess the long term effects of new technologies and new materials including effects on environment, human health, culture, human behaviour, criminal use, *etc.*?
2. How can the risk perspective be assessed and communicated to other stakeholders in the democratic process?
3. Who should decide what is an acceptable risk is and if new technologies should be accepted?

It is often considered that the development of science and technology have created a more secure environment for mankind. Paradoxically, however, it seems as if technological development has increased rather than decreased people's worries over various risks. People are afraid of BSE, radiation from mobile phones, toxins in food, terrorism *etc.* Furthermore, there is no indication that the confidence people place in experts has increased. On the contrary there are clear tendencies that people increasingly look for answers outside science. One of the precise reasons for this situation is the fragmentation of research and education and the fact that the results produced are difficult to communicate to a broader public. The basic difficulty for communication is perhaps not the knowledge base of the receivers, but rather the perception by the scientific community that research results are always objective and free from value judgments. This is a very serious problem that is undermining confidence in science and technology and in the long term the democratic foundations of society. From the very beginning engineers must anchor their solutions more carefully in terms of society, which requires a change in education. Openness about values in development of technology is a basis for re-creating the confidence in the engineer in the society.

Risk is thus an important parameter in many decision processes in our society. There are several problems with existing methods for risk assessment. One is that there are large uncertainties in the results. Another problem is that there are no well defined methods for describing what often is called "worst case" scenarios. The public has a strong tendency to focus on the worst possible consequences while experts tend to weight in uncertainties and probabilities, which will lower the risk. Worst Case will just not happen! The results from existing methods for risk assessment are also very difficult to communicate to the different stakeholders involved in the decision process.

In a democratic society it is important that the methods for risk assessment are transparent and the results from risk assessment should be possible to communicate in participatory decision processes involving many stakeholders, *e.g.*, politicians, NGOs, public. Concerning risk it is important to discuss how the precautionary principle can be applied. That is if we do not know the risks we should be precautious. We cannot rely on calculated low probabilities for events to happen any more. Accident likes that in Chernobyl and effects like that from DDT shows that skepticism towards these calculations is highly justified. Technological risks have an essential role in a broad public discussion. This will be an important part of a more developed technology culture.

55.9 Innovation and Funding of R&D

In the last few years sustainable development has been recognized as a serious challenge and major strategic issue by managers in many companies. Although pressures for this vary across industrial and national contexts, they are increasingly changing the rules of competition, making extant competencies obsolete, creating winners, losers and opportunities for niche players. Traditional risk management techniques and innovation strategies are insufficient to deal with these added difficulties. Effective sustainable development

innovation involves embedded organizational capabilities and the ability recognizes and responds to often context specific, conflicting and sometimes ambiguous pressures. Yet it is precisely because sustainable development innovation is hard, and important, that such capabilities can be the grounds for competitive advantage. The development of environmental protection technologies opened new markets for business. The same situation will now occur for sustainable development, but it will require totally new and more complex strategies.

Innovations, like in environmental technologies, are often focused on products or product chains. More seldom higher system levels are taken into account. The reason for this is that innovations in systems, like transportation systems, in a city is hard to finance because there will be many actors taking part and delivering products to the system. There is thus a need for new funding mechanisms supporting the development of technology from socio-centric concerns that is on a higher system level. This will need a closer co operation between several stakeholders like companies, public sector, and universities.

Many researcher put hope on new technologies for radical dematerialism as the new innovation strategy. This could be achieved through production of goods using less material and energy. However this race is becoming more and more like that of the hare and the tortoise. Using less material and energy in products will not keep up with the increase in consumption. Dematerialism could also be achieved through substitution of human labor. The hope is than that the sustainability of economies of the future will be based almost entirely on services; leasing will become the norm for products, and firms must learn to sell services, not products [6].

On the other hand, the one-sided concentration on the invention of marketable products which we have today is problematic. Much evidence is there to show that more focus should be on more qualitative research in social science and the humanities and especially on trans-disciplinary research.

55.10 Engineering Education for Sustainable Development

Technology has the potential to play a vital role in the development of sustainable societies and new concepts and tools for a deeper understanding of the evolution of technology are being developed in research. There are, however, large barriers for more holistic and socio-centric concepts to be practically realized in the industrial society. There are two important explanations for this. One is that these new concepts have not on a deep level influenced the education programs at the technical universities [7]. Still the engineering education is very much taught as if technological change was independent of the societal context. The other explanation is that there is still not an effective triple helix working in practice with a close co operation between universities, industry, and the public sector. This cooperation will be essential for a more radical change in the industrial systems and consumer behaviours.

The traditional view with a knowledge split where engineers possess the expert knowledge and politicians make decisions about the direction has proved unsustainable. We must create an educational system where the engineering students themselves develop values and understanding of all parts of a sustainable development, and use this as a part of their engineering knowledge. Perhaps a central part of the new role for engineers is precisely to list scientific criteria for a technological development that supports sustainable development on local and global scale. This change will increasingly be required by the industry through their changing strategies towards sustainable development.

When the environmental education at our technical universities started in the beginning of the 1970s its emphasis was on environmental protection. Central issues were basic ecology, the effects of point discharges and environmental protection techniques with regard to cleaning of water and air in particular. This was a clear reflection of the environmental work that took place in many western countries from the end of the 1950s up to the mid 1980es. During this period there was an intense expansion of water and air

cleaning technology, focusing on point discharges, a type of activity where the role of the engineer was evident. In other parts of the industry the environmental issues were still not relevant.

In connection to regional problems, such as acidification and eutrophication gaining importance, an increasingly larger portion of system analyses were added to the syllabus during the 1980s. Cause and effect, measures and effects, more system based analysis, formulated a number of new problems. The environment issue became more complex.

In the beginning of the 1990s, a change took place in the western world. The focus was shifted from point discharges to products and services**.** The environmental work in a company became more focused on studies of the total life cycle of a product" from cradle to grave", *e.g.*, from raw material withdrawal via production and product to mass disposal at the end. In the environmental syllabus basic environment management was introduced.

At the same time, global environmental issues came into focus. Large scale environmental problems such as the carbon dioxide problem and discharge of different compounds affecting the ozone layer were now discussed. The problems here are concerned with the impact on the most basic of the eco-system's functions, and the consequences of environmental destruction are considerably more serious than the local problems discussed during the early environmental work. We have now begun to realize that we have started closing in on the outer boundaries of the global system.

From this threat, the concept of sustainable development developed during the 1980s where ecological carrying capacity and the relationship between environment and growth became increasingly important, as well as the relationship between South and North. The Rio Conference 1992 formulated this change in a number of documents.

This change of the environmental work that has taken place during the last ten years has also changed the impact and content of the environmental issues for the engineer. During the 1970s environmental work in the society was concentrated to very few technicians within communal and private business with the aim to develop and handle environmental protection technology in large installations with point discharges. Laws and discharge approvals from local and regional authorities controlled their activities. Other engineers rarely reflected on the environmental work.

Focus on products and services during the 1990s have resulted in a demand in the market for the company's environmental work. The need for environmental management was strengthened and a large number of tools were developed, such as environmental labeling, ISO-certification, LCA, *etc.* This created a need for environment management skills for all engineers independent of where in the production line he/she was placed. This change of the need for knowledge for all technicians also shows the importance of having a general and compulsory environmental syllabus as important as other parts of the engineering curriculum.

We can thus see that the active role for the engineer in sustainable development has slowly changed from the 1960s and 1970s, where technology for environmental protection was the focus to the 1980s and 1990s when the environmental work on the company level started to become integrated and environmental aspects of technological development becoming increasingly proactive. Knowledge of environmental management becomes important for the engineer. The technical development is, however, still not conditioned upon what is sustainable from a global perspective. Knowledge of environmental management will hardly suffice for the role of the engineer in sustainable development and therefore it just remains necessary to discuss and formulate the need for knowledge required to carry out a sustainable development.

Technology and the engineer will play a very important role in the development towards sustainable societies. The education for sustainable development, however, has a long way to go before it has any effect on this process. The difficulties to overcome are of different powers.

One task is to clearer formulate the role of the engineer and thus the role of the technical universities in sustainable development. What is

science and what are values in sustainable development? This also includes a discussion about the views on natural science and its relation to economy and social issues in a broader society perspective. The engineer must already in his education be taught to understand and take part in public debates about the role of technology to satisfy human needs.

It took 25 years in many technical universities to get a compulsory and general environmental education for all students. There are many lessons from this development and below are some of these briefly highlighted:

- The management of the technical university must take a stance and clearer position regarding sustainable development and the need for the student to have general knowledge in the form of compulsory courses in addition to the engineering subjects.
- There must be an open debate at the university and in society about the role of the engineer and technology in sustainable development. Is it possible to develop the technology on a scientific ground without values? How and when will these values come in and how shall this be made clear in the public debate? The confidence in the engineer must be re-established.
- The discussion about education and sustainable development must be broadened between teachers and researchers to make it possible for everybody to participate.
- Continuing education of teachers must be given priority for education of students to achieve high quality. For this to happen, the basic forms of education must be changed towards further use of case studies and less lecturing. The Internet will also play an important role in freeing the teachers from administration and tied lectures.
- Research and research methods connecting to issues about the role of technology and sustainable development must be given priority. Education must gather nutrition from research in the form of questions and concrete case studies.

The concept of sustainable development includes the creation of possibilities for welfare today without preventing possibilities for welfare tomorrow. This perspective must be a guiding principle for the engineers of tomorrow. This is easy to say, but it is difficult to apply in practice. In today's globalized world technical innovations and technical progress have such a large impact on habits and behavior, on the economy and thus the flow of energy and material. The use of technology and development is controlled by a number of economical and social factors that must be recognized. Against this background tomorrow's technicians need to have a comprehensive view based on studies of economy, sociology and ecology where the consequences of the technology and driving forces for sustainable development are central.

55.11 Industrial Ecology – The Science of Sustainability

There is an existing industrial paradigm in our society, which is still mainly based on the idea of the linear production system with "minor" changes. The tendency in developing technologies is still mainly to first create the problems and then to mitigate them. There are, however, signs of a developing paradigm on a totally different system level. This can clearly be seen in the evolution of industrial ecology as a research field. Industrial ecology is an emerging field which might turn out to be a suitable platform for a more practical approach to sustainable technologies.

From being very much focused on industrial metabolism, industrial ecology has gone further to incorporate a more comprehensive, integrated view of all the components of the industrial economy and their relations with the bio sphere and the society. Industrial ecology has very much followed the evolutionary process shown in Figure 55.2. In one of the first textbooks [8] in the following description is given:

> *"Industrial ecology is the means by which humanity can deliberately and rationally approach and maintain a desirable carrying capacity, given continued economic, cultural and technological evolution. The concept requires that an industrial system be viewed nor in isolation from its surrounding systems, but in concert with them. It is a systems view in which one seeks to optimize the total materials cycle from virgin material, to finished material, to component, to product, to obsolete product, and to ultimate disposal. Factors to be optimized include resources, energy, and capital."*

The concept of industrial ecology is developing rapidly and important new considerations are how the north–south dimensions and how different concepts like justice and equity should be tackled. This evolution is a natural process in developing industrial ecology towards a more socio-centric perspective.

55.12 Conclusions

Technology can and will have a major role to play in developing more sustainable paths for our societies. Sustainable technology cannot, however, exist as such. Technological change as well as societal changes is needed in order to steer technology towards sustainability. These changes can only be achieved through a combination of top-down and bottom-up processes. Top-down processes will have to engage governments, business NGOs as well as other powerful institutions. Bottom-up movements will be built on small-scale socio-technical experiments by local authorities and citizens groups, innovative professionals and entrepreneurs, artists and other out-of-the-box thinkers.

Technological change is a path-dependent process which can cause severe lock-in effects. The choices made in the past will restrict our possibilities today. In a similar way, our choices today have consequences for the range of options left open to future generations. It is important for society to try to foresee the impact of technological change, so that the merits of such change can be discussed in a democratic process. In such a process visions based on scenario techniques will be important tools for creating visible pathways to the future.

References

[1] Hardin G. The tragedy of the commons. Science 1968; 162; 1243–1248.

[2] Friedman TL. The world is flat -A brief history of the twenty-first century, 2005; ISBN 0-374-29288-4

[3] http://jamestown.org/edm/article.php?article_id=2371531

[4] Cowan R, Hultén S. Escaping lock-in: The case of the electric vehicle. Technological Forecasting and Social Change 1996; 53:61–79.

[5] Virilio P. Interview with Ctheory. 2000, http://www.ctheory.net/articles.aspx?id=132

[6] Ayres R. Technology, progress and economic growth. European Management Journal 1996; I4(6): 562–575.

[7] Vanderburg WH, Khan N. How well is engineering education incorporating social issues. Journal of Engineering Education 1994;83: 357-61

[8] Allenby BR, Graedel TE. Industrial Ecology, Prentice Hall. 1 edition, 1995; ISBN: 0-13-125238-0.

56

Biotechnology: Molecular Design in a Globalizing World

M.C.E. van Dam-Mieras

Open Universiteit Nederland, Heerlen, The Netherlands

Abstract: Presently we are living in a society that could be described to some extent as a global networked society. Differences in welfare between the different parts of that society are enormous. However, in that global networked society the need for a development that is more sustainable than the present one is becoming more and more obvious. The chapter deals with the question "What does the process of co-development of modern biotechnology and society look like in a globalizing world?"

56.1 Introduction

Biotechnology can be described as the use of biological systems for the production of goods and the provision of services at an economically relevant scale. Described in this way it is a technology that has a very long tradition already. Since the development of genetic modification in the second half of the previous century biotechnology has led to violent debates in society. But also modern biotechnology is broader than genetic modification. It may be seen as a result of developments in molecular sciences that enable analysis, modeling, simulation and modification of biological systems at a molecular scale in the context of research and the development of products and services.

The societal debates referred to above are a normal phenomenon in the process of co-development of technology and society. Technology development is a complex process that can not be managed in a "top-down" way, it also asks for "bottom up activities" that cannot really be planned. This process of co-development is complex and rather unpredictable.

56.2 What is Biotechnology?

A description of biotechnology could be "biotechnology is the use of biological systems for the production of goods and the provision of services at an economically relevant scale". Such a broad description would also include agriculture and the food and feed industry of course, which is not what comes to ones mind first in relation to modern biotechnology. A characteristic that jumps to the fore in modern biotechnology is that this technology is based upon developments in molecular sciences applied to biological systems. Modern molecular sciences make it possible to analyze, model, simulate, design and modify biological systems at a molecular level. From that perspective the distinction between, for instance, biotechnology and nanotechnology is rather inspired by the sector in which the knowledge is

applied and in practice the boundaries between the domains are fading. Within biotechnology itself molecular sciences also blur the boundaries between different sub-sectors such as health, agriculture, and industrial production. It may be expected that biotechnology through its (potential) applications in many fields will influence most sectors of the economy. Therefore, reflection on its potential impact on ecological systems and on the sustainability of production systems deserves attention [10].

Modern biotechnology is not only characterized by the application of molecular knowledge to biological systems, but further, a second characteristic is the combination of molecular sciences and ICT. Without ICT instruments it would not be possible to store, process, and manage the huge amounts of data generated in (bio)molecular research and to model, simulate, design, and modify biological systems and processes.

56.3 The Importance of (Bio)Molecular Sciences

Modern biotechnology and genetic modification are often mentioned in one breath and the societal debate mainly focuses on the latter. Changes in DNA, the natural storage medium for genetic information, are not only produced in the biotechnology laboratory, however, they also occur in nature. Exchange of DNA during crossing over is a part of the process of meiosis during the formation of gametes, bacteria can exchange DNA via plasmids, a viral infection can result in small changes in host DNA, and so-called mutagenic chemical compounds and radiation can lead to DNA mutations. These naturally occurring processes have inspired the development of the technique of DNA recombination. What is characteristic for recombinant DNA technology is that the modifications are deliberately brought about in the laboratory and that the exchange of DNA is more targeted, as far as possible, than in natural processes of DNA exchange. Recombinant DNA technology makes possible an exchange of DNA between unrelated species and this cannot be brought about by natural crossings. Furthermore, the modern techniques for analysis and separation make the selection process of modified cells easier. The resulting genetic modifications should be placed in the context of processes relevant to man in domains such as health, agriculture, and industrial production [11].

In addition to recombinant DNA techniques and techniques for analysis and separation of molecules and cells, also the possibility to isolate and culture cells from different origin is crucial. In microbiology there is, of course, a rather long experience with the cultivation of bacteria, yeasts, and viruses, but the culture of isolated cells from different organisms like plants, animals, and humans is more recent. During research on recombinant DNA technology and cell culture work is done on a very small scale in the laboratory, but in the development of production processes and services scaling up to larger volumes has to take place. The latter belongs to the domain of bioprocess technology

56.3.1 The “Omics” Research Domains

The extensive international co-opration in the human genome project [18] has contributed to the emergence of a whole range of “omics” research domains. Examples are genomics, proteomics, metabolomics, pharmacogenomics, and nutri-genomics.

Genomics research deals with the way genetic information is stored in the genome of cells. Genetic information is codified in the sequence of four DNA building blocks. Which of the codified information will be expressed at a certain moment is determined by, among others, the external conditions and the development stage of the cells. The field of research dealing with the expression of genetic information is also called functional genomics.

Proteogenomics deals with the translation of genetic information into protein structures within cells. Before the genetic information stored in DNA can become physiologically effective DNA structures have to be translated into protein structures. Proteins are crucial for all processes taking place in living cells. The old idea of one

gene code for one protein has been abandoned. Apparently, the genetic information on a gene can be read in different ways. The huge amounts of proteins and the complexity of their interactions make proteomics another interesting field of research.

Metabolomics concentrates on the study of metabolic processes within cells. The metabolic household within cells is a highly co-ordinated interaction between very large amounts of bio-molecules. It is effective, efficient and flexible and is continuously adapted to external conditions.

In pharmacogenomics the genetic information on human DNA is taken as a point of departure in the development of new drugs.

Nutrigenomics places genetic information in the context of food and nutrition.

56.3.2 Techniques for Analysis and Separation of (Bio)Molecules

The developments described above also influence developments in other domains, for instance, in the domain of techniques for the analysis, and separation of (bio)molecules and cells. The analysis and separation technologies in the bio-molecular research domain make it possible to identify very small amounts of bio-molecules in highly complex samples. In research this opens the way to a study of biological processes at a cellular and molecular level. The technologies can also be used for optimization of monitoring, control and management of production processes and production chains. An important characteristic of this new generation of techniques for analysis and separation is that, thanks to the combination of (bio)molecular knowledge, information technology, and automation very small amounts of biological compounds in very large amounts of samples can be analyzed at a high speed.

56.3.3 Bio-informatics

Moreover, the contribution of bio-informatics, the integration between bio-molecular sciences and information technology, is of great importance. On the one hand, bio-informatics produces databanks with data on structure of DNA and proteins. On the other, the development of computer software that makes possible processing, storage, and search of these huge amounts of data is part of the field of bio-informatics. Bio-informatics makes it possible to model, simulate, and design at a molecular scale. Of course, the enhancement of communication and co-operation between the highly international community of peers cannot be overestimated either.

56.3.4 Biotechnology and Nanotechnology

In biotechnology and in research in the “omics” domains the emphasis is on the application of molecular knowledge in the context of biological systems. The demarcation from nanotechnology is not very sharp, however. Nanotechnology focuses on the development of functional devices at a molecular scale. One can think of applications in the field of micro-electronics (miniaturization), energy (solar cells), and medical practice (diagnosis and drugs delivery). These developments will most probably result in the design of new classes of micro- and nano-produced devices in which biological and non-biological components can be combined. The integration of expertise from electronics, silicium technology, chemistry, and bio-moleular sciences opens many new perspectives.

56.4 Application of Biotechnology in Different Sectors of the Economy

Modern biotechnology can be seen as a key technology that will not only lead to innovations is many sectors, but will also result in many new interactions between different sectors of the economy. The technology also has great potential for making large scale production processes more sustainable. However, sustainable development is a complex process and the availability of technology per se will not lead to a more sustainable development that the present one. Changes in behavior, organization, institutions, and power relations are needed as well.

56.4.1 Biotechnology and Healthcare

In the healthcare sector development in bio-molecular sciences and technology can result in completely new products or ways of diagnosis, treatment, and prevention, or in new production methods for existing products. The use of recombinant DNA technology in health care will result in new drugs, DNA vaccines, constructs for gene therapy, and therapeutic stem cells.

Biotechnology can also contribute to the development of cleaner production processes in the pharmaceutical industry. In the pharmaceutical sector, just as in the sector of fine chemicals, relatively small amounts of high prize products are developed. The waste streams from the production process may be rather large, however. The replacement of chemical conversion steps by biotechnological conversion steps can make the production process more efficient and can result in a reduction of waste streams, which will lead to a reduction of costs. The investments that have to be made to replace conventional process steps by biotechnological process steps are high, however.

Another point of attention in the pharmaceutical sector is the protection of intellectual property rights (IPR). The production costs in the sector may not be so high, but the initial R and D costs and the costs of assessing effectiveness and safety of products are very high. This makes the protection of property rights an important issue in this sector. These very high developments costs in the pre-market development stage also explain why in the present global economy many of newly developed products will not be available for people in developing countries [3],[23],[21], and [32].

56.4.2 Biotechnology and Agriculture

Within the agricultural sector the objective is often a higher yield by adaptation to unfavouable culture conditions and the incorporation of resistance against diseases, pests, and herbicides. Such applications in the domain of plant breeding do not result in completely new products, but rather in the (man-desired) improvement of existing crops. Recombinant DNA technology enables the introduction of genetic information from unrelated organisms and that can not be realized with conventional breeding techniques. Furthermore, the application of bio-molecular knowledge has also greatly increased possibilities for selection. Therefore, modern biotechnology brings more characteristics within reach and reduces the development time of crops. A relatively new development is the use of genetically modified plants in the production of pharmaceutical products (biopharming).

Also in this sector there are important points of discussion in the context of sustainable development. The protection of intellectual property rights and access to knowledge and technology for people in economies in transition is such a very important point of discussion. In relation to the availability of food for developing countries one could argue that reflection on the impediments for agricultural production and trade in the context of WTO agreements could be more important that modern biotechnology. Furthermore, as in large scale agricultural production processes physical or biological containment is impossible, the environmental risks are another point of discussion.

Modern biotechnology can also be used to increase productivity in cattle-breeding and dairy-farming. It offers new tools for the toolbox that is used in the industrialization of the sector for almost a century already. Animal productivity is supported by animal health care, drugs, artificial insemination, manipulation of reproduction processes, embryo transplantation, mathematical processing of data on production and descent, the feed industry, mechanization, and automation. A relatively new possibility of the application of biotechnology in this sector is the production of drugs and xeno-transplants in transgenic animals. The ethical aspects of the latter applications have led to intensive debates.

56.4.3 Biotechnology and the Food Industry

Most agricultural products are processed before they are consumed. Processing can take place in the kitchen at home, but very often a number of process steps is carried out in the food industry. This sector has much experience with classical biotechnology (conservation, dairy products,

alcoholic beverages, meat-products, soy products). Many processes can be optimized using modern biotechnology and in addition to that new products are developed and waste streams are reduced or applied in other production processes. Also the newly developed analytical techniques are of great importance to this sector for the assessment and control of quality.

By applying good manufacturing practices (GMP) the environmental risks in the food industry generally can be managed and there is not much debate in society on that, but there is debate on health risks and on the right of consumers to buy biotech-free products. As nutrition has a high emotional value, and the availability of food is not a point of concern in industrialized societies, the acceptance of perceived potential health risks by consumers is low. This leads to the paradox that carefully controlled large scale production is perceived as less safe than artisan production, in spite of the fact that in the latter the number of mistakes per kilo will be greater. It must be remarked, however, that according to the Human Development Report 2001 [27] the aversion against genetically modified food is greater in Europe and the United States that in developing countries. An important reason may be that in developing countries food availability cannot be taken for granted.

56.4.4 Biotechnology and Industrial Production

In industrial production in general modern biotechnology creates new opportunities for new products, new production processes and process optimization. In, for instance, the chemical industry the use of biological raw materials to replace fossil raw materials and the replacement of chemical conversions by bio-conversions can greatly contribute to the improvement of both ecological and economic performance. There is not much debate in society on the application of modern biotechnology in industrial production in general. When appropriate GMP procedures are used the environmental risks can be managed, and furthermore in this sector there often is no direct contact with consumers. The risk of this "invisibility" is that the opportunities from the perspective of sustainable development are not discussed either. Reasoning from an ecological perspective the potential risks and benefits of modern biotechnology in large scale production processes should not only be considered at the level of specific production processes and products chains, but also at a systems level [29].

56.5 Biotechnology and Sustainable Development

It was described above that biotechnology can contribute to an optimization of production processes. As the products and production processes used in biotechnology are very similar to those in living nature there is certainly potential for an increase in sustainability of large scale production systems [10],[29]. But a more sustainable development is not only a matter of technology. Sustainable development is a complex process requiring co-operation between different players with differing and sometimes (at least on the short term) conflicting interests [12]. In the context of sustainable development it can be expected that future shortages and social and managerial risks will in the end result in radical changes in the nature and the sectoral and regional structure of economic activities. Before continuing the reflections of biotechnology developments in society a short historical introduction on the globalization of the economy and some of its consequences will be given.

56.5.1 Sustainable Development and Globalization

A reflection on sustainable development cannot be separated from a reflection on the processes of industrialization and globalization. In a historical perspective these developments cannot be detached from the developments that took place in Europe in the 17th century.

The "knowledge revolution" that took place in Europe in the 17th century [13] induced the Industrial Revolution because innovations based on fundamental knowledge developed in an enabling social environment made a different organization

of production processes and society possible. It resulted in drastic changes in technology, economy, and society and created welfare, at least in the industrialized societies. It also contributed to the development of nation states responsible for public interest, for a proper functioning of economic markets, for safety, and for the development of social institutions that constitute a safety net for their citizens. Welfare in these nations was to some extend shared among citizens and resulted over time in increased possibilities for individual development. These developments were also connected to the process of colonialism and globalization of the economy. In the second part of the 20th century the process of globalization has been boosted by developments in the field ICT and by a worldwide liberalization of trade. The liberal market paradigm since the end of the cold war contributed to ending colonialism and developments in ICT made it possible to organize human activities in a geographically spread way.

Also today technological innovations based on fundamental insights, like those in molecular sciences, taking place in an enabling social environment, constitute conditions for economic and social developments. However, they no longer take place mainly on a national level. The possibilities for transportation of persons, goods, and information leads to a world in which human activities are geographically spread, production chains cross national borders, and virtual space is increasingly becoming a space for activities complementary to physical space [2],[4],[5] and [7]. People and organizations will have to learn how to be part of a global society while remaining bound for most of their time to their physical environment. The emerging global space connects all places on earth and relates the human activities in different societies. The reach of choices made has consequences for others in other societies, which should be taken into account as well. Governments, organizations operating in the private domain, NGOs, and world citizens have a joint responsibility for the developments in the global space.

56.5.2 Sustainable Development, Policy, and Responsibility

Working on sustainable development implies dealing with dilemmas in complex societal environments and taking decisions under uncertainty. For many citizens it may be difficult to understand such complex problems, which makes it difficult for governments to get acceptance for drastic policy measures needed [33]. The legitimacy of policy measures also is a difficult question because the expected problems:

- may only become evident in the future ,
- will become manifest at remote places and thus ask for international solidarity,
- may not happen at all.

Policy development in such complex situations asks for weighting in which the use of the precautionary principle can be helpful [14]. In practice it will never be possible to exclude all risks and therefore the question is which level of knowledge is needed to take a responsible decision. This challenge for government policy has resulted in the development of innovative methods for policy making at the national level; open policy processes and stakeholder participation are examples of those developments [26],[33]. Because the sovereignty and power of nation states is bound to their territory a most urgent question is how, and via which actors, this responsibility can be “scaled up” to the global level. How can an “incubator” be created in which the different actors involved can develop in mutual interactions good practices fitting in the global reality?

For companies responsibility is expressed in concepts such as corporate social responsibility, which deals with concepts such as integrity, good governance, and a series of objectives desirable from the societal perspective [22].

NGO plays an important role in the globalization of civil society. The effectiveness of socially active NGOs lies in their flexibility and the dynamics of the network structures in which they operate. [1],[28] and [31].

World citizens can influence developments in the global space in at least three ways: as a citizen, as a consumer and as a producer. In practice the behavior of individuals in these different roles is not always consistent and sometimes even conflicting. In addition, choices on how to apply knowledge and capital are of great importance.

56.6 Innovations, Civil Society, and Global Space

Technologies based on knowledge of structures and systems at the molecular level (modern biotechnology, the "omics" domains, nanotechnology) can be seen as key technologies but they will not result in innovations if there is no interaction between technology and society. Society and technology are related via a process of co-evolution in which society influences innovations and innovations affect the societal context. The civil society therefore is an important "incubator" for innovation. New societal practices related to the innovations that develop in civil society will finally "coagulate" in laws and regulations. As long as developments take place at a national level, laws and regulations will co-develop with innovations and therefore will match, at least to a large extent, with norms and values broadly accepted in society. But what happens when technology is developing in a global networked society? There is no parallel to the process of co-evolution of technology and society at a global level.

56.6.1 Biotechnology and Governmental Policy

One could state that it is the task of governments to provide safety to their citizens their citizens and to contribute to (the generation of) welfare. The instruments for fulfilling those tasks are laws and regulations on the one hand and the creation of incentives on the other. In relation to biotechnology nations will thus try to develop regulation that will control the possible risks associated with genetic engineering and to create conditions for economic development.

Regulations in relation to a new technology like biotechnology have to deal with many values: sustainability, freedom of choice, biodiversity, the integrity of organisms, the dignity of human life, the protection of intellectual property rights, justice, and solidarity are all involved [9]. At a national or a community scale one could say that the formulation of regulations could be seen as the articulation of societal rules that have developed with time in a continuously evolving "civil society". Developed according to such a process laws and regulations will fit in with the economic, socio-cultural and political climate prevalent in society. But as technologies based on bio-molecular knowledge are developing in a globalize economy the developments may be less smooth.

Of course for every emerging technology the application of knowledge will display region-specific characteristics but the strong international dimension in economy, technology development, and trade ask for a supra-national dimension in the development of adequate regulation as well. This is true for the application of biotechnology in all sectors of the economy but at the moment it is perhaps most evident in relation to the use of modern biotechnology in agriculture and the food industry. The effects of the introduction of genetically modified organisms (GMOs) in these large scale production systems will not be held within national borders. The "co-development" of technology, "civil society", and regulations can no longer be taken for granted because there are a number of societies involved. We have to find out by and while doing this how this process can be orchestrated.

In the recent report "Genetic Engineering and Globalization" the COGEM, the advisory committee on genetic engineering to the Ministry of Housing, Spatial Planning and Environment in The Netherlands, reflected on the (often unintended) worldwide effects of national and European regulation with regard to genetic engineering. In the report they focused on the regulation of the cultivation of genetically modified (GM) crops and the resultant GM products.

56.7 Biotechnology, Agriculture, and Regulations

The cultivation of GM crops and the worldwide trade in the resultant GM products has increased from 1.7 million hectares in 1996 to 80.7 million hectares in 2004 and there appears to be no end yet to this tremendous rate of growth [6],[19]. At the moment GM agriculture is, for different reasons, being carried out on only a very small scale in Europe and Africa, while GM crops are being grown on a large scale in both North and Latin America, and GM agriculture is burgeoning in Asian countries. Of course these crops and their products are traded internationally as well.

At present, the cultivation of GM crops is mainly limited to herbicide-tolerant and insect-resistant maize, soy, cotton, and rape, but the cultivation of other crops with these and other properties can be anticipated. At the moment thousands of trials under field conditions are being carried out worldwide on tens of different crops with innumerable different properties. Examples are petunias with a modified bloom color, frost-tolerant potatoes, vaccine-producing alfalfa, and coffee with reduced caffeine content.

With regard to GM agriculture, the governmental tasks indicated above are translated in the Netherlands in particular and in Europe as a whole into a policy in which, in addition to the safety of food and the environment, the coexistence of different types of agriculture is taken care of and the freedom of choice of consumers and growers is guaranteed. But of course the cross-border nature of (the trade in) GM agricultural products means that national and European regulations can have (unwanted) effects in other parts of the world. On the other hand, practices and policies developed in other parts of the world will have consequences for Europe as well

For instance, strict regulatory requirements emanating from a European concern for mankind and the environment, societal resistance, and nationally shared ethical principles and norms can constitute a barrier to commercial development of GM crops for other countries. The European consumer's resistance to GM food products is for some producers in other parts of the world a major barrier to cultivating GM crops. The very limited extent of consumers' acceptance in Europe has resulted in regulations that are far more restrictive than those in other parts of the world. European regulations can lead to the adoption of western assessment regimes in other countries. This is not of necessity an intended effect but it can be a consequence of the standards set on imports which affect the country's trading position. It can also be a psychological effect: if they are so cautious in countries where the technology was developed then maybe their example should be followed. For instance, in Africa genetic engineering is applied to agriculture at only a minor scale. There are social, cultural and geographic reasons for that, but also European regulation with regard to GM crops may contribute.

The opinions on the usefulness of GM agriculture for developing countries differ. Some stakeholders state that GM agriculture has much to offer to developing countries such as resistance to plagues and insects, reductions in the use of pesticides (if these are used), harvest increase and drought tolerance. Others believe that GM agriculture has very little to offer to developing countries and will only increase their degree of dependence as GM agriculture is a form of industrialized farming that for the greater part is not attuned with the economic balances and socio-cultural beliefs in these countries. Industrialized agriculture produces for the world market and focuses on bulk crops and uniformity. Is countries where small-scale agriculture is predominant were to adopt the industrialized production model the loss of local agrarian know-how and the disappearance of locally adapted varieties could be a consequence. From the perspective of sustainable development a different approach to the development of agriculture, supported by a different form of biotechnology might be more attractive. Of course producers and citizens in developing countries should have both the right and the opportunity to make their own assessments and choices [9],[20],[24],[25],[30].

In Latin America the influence of opinions from within the EU is much smaller as there the US rather forms the frame of reference. GM crops are cultivated on a large scale in Latin America on the

basis of technology principally developed in the US. In Asian countries such as China and India the dependence on other countries is much less because of their own large markets and because of the fact that major developments of the own knowledge and technology have been set in motion by recent political developments. As a consequence these countries will develop their own GM crops and the accompanying regulatory regimes. In some aspects they are ahead of developments in Europe.

As to regulations relevant to GM agriculture with a supra-national dimension the following can be mentioned: the Carthagena Protocol on Biosafety (CPB, a supplementary agreement to the UN Biodiversity convention), the Codex Alimentarius (dealing with food safety) and the conventions within the framework of the World Trade Organization (WTO).

The CPB makes provisions for procedures for the supply of information of an exporting party to an importing party, in order that the latter can make a well-considered decision about the possible import of GMOs. It is the intention to promote the exchange of information about GMOs and regulations via a so-called Biosafety Clearing House and to help countries in the implementation of regulatory systems that contribute to the objectives of the CPB. Also the United Nations Environment Programme (UNEP) and the Global Environment Facility (GEF) offer help, such as the so-called UNEP-GEF Toolkit, to countries in their design of a National Biosafety Framework (NBF). However, this type of help has its drawbacks. It may lead to the institution of a complex and extensive system of regulation that does not tie in with the local needs and capacity. Also many countries involved have nothing to do with the cross-border movement of GMOs, or do not have at their disposal the means to maintain an administrative system such as NBF. Instead capacity-building should be adapted to suit regional resources and needs and should also take into account the local parties involved. In its report the COGEM states that technology and society shape each other in a process of co-evolution and when that is not taken into account during the transfer of regulatory concepts inefficient solutions will be the result. An approach in which the context of local policy is furthered in the development of regulatory structures could be far more promising.

56.8 Conclusions

The author wants to state that she sees the process of sustainable development as a race against time during which mankind will have to learn by and while doing to organize society and its processes and institutions in a way that is more sustainable than it is now. Individuals and organizations will have to develop the ability to think, communicate, learn and collaborate across the boundaries that divide different disciplinary, social and cultural perspectives. Some key notions in this respect are dialogue, mutual respect, creativity and willingness to change.It would be a shame not to use the potential of biotechnology in this context.

References

[1] Arquilla J, Ronfeld D. Networks and netwars. Rand, Santa Monica, CA, 2001.

[2] Beck U. Was ist Globalisierung? Suhrkamp Verlag, Frankfurt, 1997.

[3] Belt H van den, Reekum R van. Issues rond octrooien en genen (Issues around patents and genes). Essays NWO MCG Themadag 26 September, 2002: 5–28.

[4] Breton G. Higher education: From internationalization to globalization. In: Breton G, Lambert M, editors. Universities and globalization. Private linkages, public trust. UNESCO/Université Laval, Economica, 2003; 21–33.

[5] Brooks CW. Globalization: A political perspective. In: Breton G, Lambert M, editors. Universities and globalization. Private linkages, public trust. UNESCO/Université Laval, Economica, 2003;45–50

[6] Brookes and Barfoot , GM crops: the global socio-economic and environmental impact – The first nine years 1996–2004, PGEconomics, 2005; October.

[7] Castells M. The rise of the network society. The Information Age / Volume 1: Economy, Society and Culture, Blackwell, Oxford, 1996

[8] CBD (Commissie Biotechnologie bij Dieren), CCMO (Centrale Commissie Mensgebonden Onderzoek), COGEM (Commissie Genetische Modificatie) (2004), Trendanalyse Biotechnologie 2004

[9] COGEM (Commissie Genetiasche Modificatie), Genetic engineering and globalization. Suggestions for government policy in the field of genetic engineering in the light of increasing globalization. COGEM Report CGM/060202-02, Bilthoven, 2006.

[10] Dam-Mieras, Van MCE, Leach CK, Mijnbeek G, Middelbeek E. Biotechnology applications in an environmental perspective. In: Misra K.B, ed. Clean production. environmental and economic perspectives. Springer Berlin, 1996; 355-386.

[11] Dam-Mieras, Van MCE. Biotechnology in Maatschappelijk perpsectief. WRR, The Hague, 2001.

[12] Jansen, L., Weaver, P. Dam-Mieras, R. van. Education to meet new challenges in a networked Society in: Innovation in Education, J. E. Larkeley and V. B. Maynhard (eds.), Nova Science Publishers Inc., Hauppauge, NY 11788, forthcoming.

[13] Dijstelbloem H, en Schuyt,K. De publieke dimensie van kennis, H. Dijstelbloem en Schuyt CJM (red), Sdu Uitgevers, Den Haag; 2002:7–29.

[14] European Commission (2000), Communication from the Commission on the precautionary principle, 2 Feb. 2001.

[15] Fukuyama F. De nieuwe mens (original title: Posthuman Society, translated by Huizen P. Van, Uitgeverij Contact, Amsterdam/Antwerpen, 2002.

[16] Gaskell G. *et al*., Europeans and biotechnology in 2005: Patterns and trends. Eurobarometer 64.3, A report to the European Commission's Directorate-General for Research, 2005. http://www.ec.europa.eu/research/press/2006/pdf/pr1906_eb_64_3_final_report-may2006_en.pdf#search=%22Eurobarometer%2064.3%22.

[17] Graef M de Verrips Th. Genomics 2030: Part of everyday life. STT/Beweton, The Hague, 2005.

[18] Helmuth L. Map of the human genome 3.0. Science 2001; 27 July, 293, 5530:583–585.

[19] James C. Global status of commercialized biotech/GM crops: 2004, ISAAA Briefs No. 32, Ithaca, NY. Backgrounders: Biotech Crop Area by Country, 2004.

[20] Magnaghi A. Local self-sustainable development: subjects of transformation. Tailoring Biotechnologies. Potentialities, Actualities and Spaces 2005; 1: 79–102.

[21] Maskus K. Regulatory standards in the WTO, Working Paper, 00-1. 2000. http://www.iie.com/publications/wp/wp.cfm?ResearchID=121

[22] OECD. The OECD guidelines for multinational enterprises, Paris, 2000. http://www.oecd.org/

[23] Rifkin J. The biotech century: Harnessing the gene and remaking the world. Tarcher Putnam, New York, 1998.

[24] Rosset PM. Genetically modified crops for a hungry world: How useful are they really? Tailoring Biotechnologies. Potentialities, Actualities and Spaces 2006; 2; 79–94.

[25] Ruivenkamp G. Tailor-made biotechnologies: Between bio-power and sub-politics, tailoring biotechnologies. Potentialities, Actualities and Spaces 2005; 1:11–33.

[26] Scharpf FW. Notes toward a theory of multilevel governing in Europe, Max-Planck Institut für Gesellschaftsforschung, Köln, 2000.

[27] UNDP (United Nations Development Program) Human Development Report 2001. Making new technologies work for human development, New York: 2001. http://www.undp.org/dpa/index.html

[28] Warkentin C. Reshaping world politics. NGOs, the Internet, and global civil society, Rowman and Littlefield, Lanham, MD, 2001.

[29] Weaver P, Jansen L, van Grootveld G, van Spiegel E, Ph.Vergragt. Sustainable technology development. Greenleaf, Sheffield, UK, 2000

[30] Wekundah JM. Genomics for the poor: An analysis of the constraints and possibilities for social choices in genomics for developing countries.Tailoring Biotechnologies. Potentialities, Actualities and Spaces 2005; 1:119–138.

[31] Wilde R de, Vermeulen N, Reithler M. Bezeten van genen. Een essay over de innovatieoorlog rondom genetisch gemodificeerd voedsel, Sdu Uitgevers, Den Haag, 2003.

[32] Williamson AR. Gene patents: socially acceptable onopolies or an unnecessary hindrance to research? Trends in Genetics 2001; 17:670–673.

[33] WRR (Wetenschappelijke Raad voor het Regeringsbeleid). Naar nieuwe wegen in het milieubeleid, Sdu Uitgevers, The Hague, 2003.

Nanotechnology: A New Technological Revolution in the 21st Century

Ronald Wennersten, Jan Fidler and Anna Spitsyna

Royal Institute of Technology, School of Energy and Environmental Technology,
Department of Industrial Ecology, Sweden

Abstract: Nanotechnology is going to be a major driving force behind the impending technological revolution in the 21st century. Both private and public sector spendings are constantly increasing. The size of the market for nanotechnology products is already comparable to the biotechnology sector, while the expected growth rates over the next few years are far higher. Nanotechnology manufacturing is a fundamentally new process in which structures are built from the bottom up, one atom at a time. Nanotechnology has the potential of producing new materials and products that may revolutionize all areas of life. Nanotechnology protagonists believe that nanotechnology will provide unsurpassed benefits for the society. Meanwhile, its antagonists believe that nanotechnology may pose serious health and environmental risks and advocate that the precautionary principle should govern the development and deployment of such products. Although it is difficult to predict precisely how nanotechnology will impact society, current understanding, under either the spectacular benefit or the serious risk scenarios, presages a huge impact on society in areas that include the environment, healthcare, energy, and electronics.

57.1 Introduction

The term “nanotechnology” describes a range of technologies performed on a nanometer scale with widespread applications across all sectors, from textiles to biosciences and consumer preparations such as cosmetics. Nanotechnology refers to several technologies of the very small, with dimensions in the range of nanometers and exploits specific properties that arise from structuring matter at a length scale characterized by the interplay of classical physics and quantum mechanics. Nanotechnology is an underlying technology ennabling other technologies.

Nanotechnology has been around for two decades, but the first wave of applications is only now beginning to break. It will affect everything from the batteries we use to the pants we wear to the way we treat cancer. The term “nannos” is a prefix that means “little old man”, “dwarf” in Greek. One nanometer (nm) is one thousand millionth of a meter. This comma, for instance, spans about half a million nanometers, a dollar bill is 100,000 nanometers thick, a human hair is about 80,000 nanometers wide, and a water molecule almost 0.3 nm.

The vision and inspiration for nanotechnology came from Nobel laureate Richard Feynman in a 1959 speech entitled “There's Plenty of Room at

the Bottom". His vision was that there are enough places on the molecular level that we could in future use a focused electron beam to write "the entire 24 volumes of the Encyclopedia Britannica on the head of the pin". He also saw the possibility to arrange the atoms one by one; in other words "bottom-up" manufacturing on the molecular level [1].

Nanotechnology starts at the bottom and builds up one atom at a time. Apart from making things that are very small, nanotechnology promises "absolutely perfect copies" of a device. Broadly speaking, nanotechnology may be divided into two areas: *nanomaterials*, and *nanodevices*. Norio Taniguchi of Tokyo University created the term "nanotechnology" in 1974 to describe the precision manufacture of materials with nanometer tolerances [2].

At the nano size familiar materials begin to develop odd properties when they are of nano size. If a piece of aluminium foil is torn into tiny strips, it will still behave like aluminium, even after the strips become so small that a microscope is needed to see them. But if one keeps chopping them smaller and smaller, at some point, 20 to 30 nm, the pieces can explode. Nano aluminium could be an additive to rocket fuel [3].

Not all materials change properties, but the fact that some do is an advantage; new materials can be engineered, such as plastic that conducts electricity and coating that prevents iron from rusting. The reason why substances behave differently at the nanoscale is because that is where the essential properties of matter are determined. If we arrange calcium carbonate molecules in a saw tooth pattern, for instance, we will get a fragile chalk. If the same molecules are stacked like bricks, they help form the layers of the tough shell of an abalone.

There is a growing interest in nanoscience and nanotechnology because they are seen as having the potential to bring changes in many fields of research and application. These emerging technologies meet with both optimism and pessimism among experts. Nanotechnology has the potential of producing new materials and products that may revolutionize all areas of life. Meanwhile, its critics believe that nanotechnology may pose serious health and environmental risks, and advocate that the precautionary principle should govern the development and deployment of such products. Although it is difficult to predict precisely how nanotechnology will impact society, current understanding, under either the spectacular benefit or the serious risk scenarios, presages a huge impact on society in areas that include the environment, healthcare, energy, and electronics.

Nanoscale materials have been used for decades in a range of applications. Modern industrial nanotechnology had its origins in the 1930s, in processes used to create silver coatings for photographic film; and chemists have been making polymers, which are large molecules made up of nanoscale subunits [3].

Today's nanotechnology, for example the planned manipulation of materials and properties on a nanoscale, exploits the interaction of three technological streams [3]:

- the control of the size and manipulation of nanoscale building blocks,
- the characterization of materials on a nanoscale (for example, spatial resolution, chemical sensitivity), and
- the understanding of the relationships between nanostructure and properties and how these can be engineered.

The properties of materials can be different on a nanoscale for two main reasons:

First, nanomaterials have, a relatively larger surface area than the same mass of material produced in a larger form. This can make materials more chemically reactive (in some cases, materials that are inert in their larger form are reactive when produced in their nanoscale form), and affect their strength or electrical properties.

Second, below 50 nm, the laws of classical physics give way to quantum effects, provoking optical, electrical, and magnetic behaviors different from those of the same material at a larger scale. These effects can give materials very useful physical properties such as exceptional electrical conduction or resistance, or a high capacity for storing or transferring heat, and can even modify biological properties, with silver for example becoming a bactericide on a nanoscale. These

properties, however, can be very difficult to control. For example, if nanoparticles touch each other, they can fuse, losing both their shape and those special properties—such as magnetism—that scientists hope to exploit for a new generation of microelectronic devices and sensors.

57.2 Top-down and Bottom-up Design

For assembling nanoscale materials and devices two approaches can be used: top-down and bottom-up. Bottom-up approaches means that smaller components arrange themselves into more complex assemblies, while top-down approaches means to create nanoscale devices by using larger, externally-controlled ones to direct their assembly.

The top-down approach often uses the traditional workshop or microfabrication methods where externally-controlled tools are used to cut, mill and shape materials into the desired shape and order.

Bottom-up approaches, in contrast, use the chemical properties of single molecules to cause single-molecule components to automatically arrange themselves into some useful conformation.

The current state-of-the-art in nanotechnology uses micro-electro-mechanical Systems (MEMS) processes to produce nanoparticles such as carbon nanotubes and buckyballs. MEMS manufacturing is a top-down method that starts by gathering the materials needed to manufacture the product, but many of the parts that make up the product are formed by chemical reactions, photolithography, and other lithographic techniques.

MEMS manufacturing is capable of producing features that are not visible to the human eye without the assistance of a microscope and may be capable of producing some of the same products that will be produced by nanotechnology in the future.

One eventual goal of nanotechnology is to use molecular manufacturing to individually place each atom. Although MEMS technology already produces objects in the range of 1–100 nanometers, molecular manufacturing will provide advantages over MEMS. Molecular manufacturing will produce nanomaterials with no impurities because atom placement is individually controlled. Molecular manufacturing requires nanodevices, as will be discussed below. Nanomaterials may also serve as the raw material for products manufactured using traditional or MEMS techniques.

Although nanomaterials hold great potential, nanodevices are where the true potential of nanotechnology lies. Currently, nanotechnology uses tools, such as scanning tunneling microscopes or atomic force microscopes, to arrange atoms one at a time. The process is slow, expensive, and limited in its potential to build from the bottom.

However, nanotechnology visionary, Eric Drexler [4], contemplating the marvels of the ribosome, foresees a vastly different method of building at the bottom. Drexler proposed an atomic assembler, similar to a robotic arm, capable of grasping a single atom and bonding it to other atoms. A microscopic robot arm receiving instructions, possibly from a computer, is the basis of molecular manufacturing.

Drexler [4] refers to a device capable of molecular manufacturing as a nanofactory. The first nanofactories are likely to be about the size of a desktop printer, requiring specialized feedstock, an external energy source, and an external computer. Inside the robot factory, the robot arm will arrange the feedstock into nanodevices. The devices produced by a nanofactory will be microscopic because a molecular fabricator, even with an assembler that works at a million cycles per second, produces only about a nanogram of product per year. Drexler proposes that a nanofactory should be capable of building the parts for additional nanofactories, so that multiple nanofactories can operate simultaneously to produce related parts that may be assembled into macroscopic objects [3].

However, the concept of assemblers and molecular manufacturing is not without its detractors. In a 2001 issue of Scientific America, Richard E. Smalley, 1996 Nobel Laureate in chemistry (co-discoverer of buckminsterfullerene), maintained that the atomic forces between atoms make it impossible for an assembler to precisely position atoms. He contends that putting “every atom in its place ... would require magic fingers” [4]. Smalley concedes that the ribosome does

precise and reliable chemistry, but that it "can occur only under water" and that "molecular manufacturing will forever be severely limited." To be sure, eminent scientists have aligned themselves on both sides of the debate and except for their rhetoric and the ribosome; there is no evidence that assemblers will ever be a reality.

57.3 Applications of Nanotechnology

An enormous improvement for a variety of product properties due to nanoscale effects has been achieved over the past few years; although a distinct onset of nanotechnology in the past cannot be defined. This apparent contradiction is based on the fact that today's common definitions of nanotechnology enclose long existing products, which are based, for example, on thin layers or small particles. Therefore, products that are either based on nanosized features or on nanoscale properties might just match the current "nano" requirements by chance. Wide-spread products like computer hard drives are indeed based on nanotechnology, but were not associated with the term "nano" when they were launched. Modern hard disk drives, with their enormous capacity of up to several 100 Gb would not be possible without the so called GMR effect (giant magneto resistance), which is based on the coupling of magnetic layers, separated by an ultra thin "nano"-spacer and was discovered in the late 1980s. Therefore, it is clear that the boundary between products related to the prominent term "nanotechnology" and others is fuzzy.

Besides the traditional fields of high technology, life sciences are expected to undergo a vivid change due to the impact of "nanobiotechnology". In biology the word "nanotechnology" is of particular importance; it is nature's intrinsic way to build on the nanometer scale molecule by molecule through self-organization. This "assembling" method is extremely efficient and may be helpful for the conservation of nature and natural resources. It is expected that the concept of "self-assembly" will be an approach for a sustainable development in the future. However, such futuristic concepts are far from being realized at present or in a medium term view.

The increasing need for energy in the world is accompanied by a surge in air and water pollution. Nanotechnology may provide solutions for improving renewable energy systems, such as fuel cells, solar cells or hydrogen storage, and help to foster their implementation in the future. Below the potential applications of nanotechnology for some sectors are given more in detail.

57.4 Applications in the Energy Sector

Breakthroughs in nanotechnology may provide technologies that will contribute to worldwide energy security and supply. A report published by Rice University (Texas) in February 2005 [4] identified numerous areas in which nano-technology may contribute to more efficient, inexpensive, and environmentally sound tech-nologies than are readily available. Although the most significant contributions may be to unglamorous applications such as better materials for exploration equipment used in the oil and gas industry or improved catalysis, nanotechnology is being proposed in numerous energy domains, including solar power; wind; clean coal; fusion reactors; new generation fission reactors; fuel cells; batteries; hydrogen production, storage and transportation; and a new electrical grid that ties all the power sources together.

The possible main contributions of nano-technology may be to:

- lower the costs of photovoltaic solar energy tenfold,
- achieve commercial photocatalytic reduction of CO_2 to methanol,
- create a commercial process for direct photoconversion of light and water to produce hydrogen,
- lower the costs of fuel cells between tenfold and a hundredfold and create new, sturdier materials,
- improve the efficiency and storage capacity of batteries and supercapacitors between tenfold and a hundredfold for automotive and distributed generation applications,

- create new lightweight materials for hydrogen storage for pressure tanks, liquid hydrogen vessels, and an easily reversible hydrogen chemisorptions system,
- develop power cables, superconductors or quantum conductors made of new nano-materials to rewire the electricity grid and enable long-distance, continental and even international electrical energy transport,
- reduce or eliminate thermal sag failures, eddy current losses and resistive losses by replacing copper and aluminium wires,
- develop thermochemical processes with catalysts to generate hydrogen from water at temperatures lower than 900 C° at commercial costs,
- create super strong, lightweight materials that can be used to improve energy efficiency in cars, planes and in space travel; the latter, if combined with nanoelectronics based robotics, possibly enabling space solar structures on the moon or in space,
- create efficient lighting to replace incandescent and fluorescent lights,
- develop nanomaterials and coatings that will enable deep drilling at lower costs to tap energy resources, including geo-thermal heat, in deep strata, and
- create CO_2 mineralization methods that can work on a vast scale without waste streams.

57.5 Environmental Applications

As applications of nanotechnology develop over time, they have the potential to help shrink the human footprint on the environment. This is important, because over the next 50 years, according to according to World Resources 2000 and United Nations press releases, the world's population is expected to grow by 50%, global economic activity is expected to grow by 500%, and global energy and materials use is expected to grow by 300%. So far, increased levels of production and consumption have offset our gains in cleaner and more-efficient technologies. This has been true for municipal waste generation, as well as for environmental impacts associated with vehicle travel, groundwater pollution, and agricultural runoff. Below is a short summary of how nanotechnology can create materials and products that will not only directly advance our ability to detect, monitor, and clean up environmental contaminants, but also help us avoid creating pollution in the first place. By more effectively using materials and energy throughout a product lifecycle, nanotechnology may contribute to reducing pollution or energy intensity per unit of economic output.

Examples of where nanotechnology can be used for environmental prevention are:

- synthetic or manufacturing processes that can occur at ambient temperature and pressure,
- the use of non-toxic catalysts with mini-mal production of resultant pollutants,
- the use of aqueous-based reactions thus avoiding organic solvent,
- building of molecules as needed –"just in time", and
- nanoscale information technologies for product identification and tracking to manage recycling, remanufacture, and end of life disposal of solvents.

Many promising features of nanoscaled objects have been identified, leading to superior product functionality and thus providing means for a better life. In general, nanotechnologically improved products rely on a change in the physical properties when the feature sizes are shrunk. Nanoparticles, for example, take advantage of their dramatically increased surface area to volume ratio. Their optical properties, for example fluorescence, become a function of the particle diameter. When brought into a bulk material, nanoparticles can strongly influence the mechanical properties, such as the stiffness or elasticity. Such "nanomaterials" will enable a weight reduction accompanied by an increase in stability and an improved functionality, such as "easy-to-clean", "anti-fog", "anti-finger-print" or "scratch-resistance", to name a few.

Other environmental contributions from nanotechnology can be selective membranes that can filter decontaminants or even salt from water, nanostructured traps for removing pollutants from industrial effluents, characterization of the effects of nanostructures in the environment, maintenance of industrial sustainability by significant reductions in materials and energy use, reduced sources of pollution, increased opportunities for recycling.

57.6 Other Areas of Applications

In the OECD report an overview is given [3] of the many domains where nanotechnology is expected to fundamentally change products and how they are produced over the next two decades.

Nanoscale materials, as mentioned above, have been used for a long time in several applications and are already present in a wide range of products, including mass-market consumer products. Among the most well known is a type of glass for windows which is coated with titanium oxide nanoparticles that react to sunlight to break down dirt. When water hits the glass, it spreads evenly over the surface, instead of forming droplets, and runs off rapidly, taking the dirt with it. Nanotechnologies are used by the car industry to reinforce certain properties of car bumpers and to improve the adhesive properties of paints.

Examples of fields from the above report which are expected to develop are given below.

Semiconductors and Computing

The computer industry is already working on a nanoscale. Although the current production range is at 90 nm, 5 nm gates have been proven in labs, although they cannot be manufactured yet. By 2015, semiconductor development priorities will have changed, as the focus shifts from scaling and speed to system architecture and integration, with user specific applications for bio-nanodevices, the food industry and construction applications. Another trend is the convergence between IT, nanotechnology, biotechnology, and cognitive sciences. The higher speeds at which information will be disseminated will change how we work with computers, and also perhaps how we deal with things like damaged nerves, possibly by developing direct interfaces with the nervous system and electronic circuits, so-called neuromorphic engineering, where signals are directly transmitted from a human organism to a machine.

Electronics and Communications

Recording using nanolayers and dots, flat-panel displays, wireless technology, new devices and processes across the entire range of communication and information technologies, factors of thousands to millions improvements in both data storage capacity and processing speeds and at lower cost and improved power efficiency compared to present electronic circuits are available today.

Chemicals and Materials

Catalysts that increase the energy efficiency of chemical plants and improve the combustion efficiency (thus lowering pollution emission) of motor vehicles, super-hard and tough (in other words not brittle) drill bits and cutting tools, “"smart” magnetic fluids for vacuum seals and lubricants are the examples.

Pharmaceuticals, Healthcare, and Life Sciences

Because of their small size, nanoscale devices can readily interact with biomolecules on both the surface of cells and inside of cells. By gaining access to so many areas of the body, they have the potential to detect disease and deliver treatment in new ways. Nanotechnology offers the opportunity to study and interact with cells at the molecular and cellular scales in real time, and during the earliest stages of the development of a disease. Since nanocomponents can be made to share some of the same properties as natural nanoscale structures, it is hoped that it will be possible to develop artificial nanostructures that sense and repair damage to the organism, just as naturally occurring biological nanostructures such as white blood cells do. Examples of potential applications are: drugs, gene and drug delivery systems targeted to specific sites in the body, bio-compatible replacements for body parts and fluids, self-diagnostics for use in the home, sensors for labs-on-a-chip, and material for bone and tissue regeneration.

Food and Agriculture

Nanotechnology is rapidly converging with biotech and information technology to radically change food and agricultural systems. Over the next two decades, the impacts of nano-scale convergence on farmers and food may even exceed that of farm mechanization or of the Green Revolution. Food and nutrition products containing nano-scale additives are already commercially available. Likewise, a number of pesticides formulated at the nanoscale are on the market and have been released in the environment.

Textiles

The textile industry may be affected quite heavily by nanotechnology, with some estimates market impact of hundreds of billions the next decade. Nanoscience already has stain-resistant and wrinkle-resistant clothing, and developments will focus on upgrading existing and performances of textile materials; "smart" textiles with unprecedented functions such as:

- sensors and information acquisition,
- multiple and sophisticated protection,
- health-care and wound-healing functions, and
- self-cleaning and repair functions.

Manufacturing

Precision engineering based on new generations of microscopes and measuring techniques, new processes and tools to manipulate matter at an atomic level, nanopowders that are sintered into bulk materials with special properties that may include sensors to detect incipient failures and actuators to repair problems, chemical-mechanical polishing with nanoparticles, self-assembling of structures from molecules, bio-inspired materials and biostructures.

Space Exploration

In this sphere, we may see developments of lightweight space vehicles, economic energy generation and management, and ultra small and capable robotic systems.

57.7 Market Prospects

The first winners in the nanotechnology industry are likely to be the manufacturers of instruments allowing work on a nanoscale. According to market researchers, the nanotechnology tools industry ($245 million in the US alone) will grow by 30% annually over the next few years. The following projected three-phase growth path seems credible [4]:

- In the present phase, nanotechnology is incorporated selectively into high-end products, especially in automotive and aerospace applications.
- By 2009, commercial breakthroughs will unlock markets for nanotechnology innovations. Electronics and IT applications will dominate as microprocessors and memory chips built using new nanoscale processes come on to the market.
- From 2010 onwards, nanotechnology will be commonplace in manufactured goods. Health care and life sciences applications will finally be significant as nano-enabled pharmaceuticals and medical devices emerge from lengthy human trials.

As the OECD survey emphasizes, most statistical offices do not collect data on nanotechnology R&D, human resources or industrial development, in part because nanotechnology remains a relatively new field of science and technology, and also because of its interdisciplinary and cross-sectorial character. Given this, estimates of potential nanotech markets tend to come from private sources such as specialized consultancy firms that survey a wide number of actors in the field. Lux Research, for example, states that:

"Sales of products incorporating emerging nanotechnology will rise from less than 0.1% of global manufacturing output today to 15% in 2014, totalling $2.6 trillion. This value will approach the size of the information technology and telecom industries combined and will be ten times larger than biotechnology revenues". Insurers SwissRe echo this: "Sales revenues from products manufactured using nanotechnology have already reached 11-digit figures and are projected to

generate 12-digit sums by 2010, even 13-digit sums by 2015."

57.8 Nanotechnology for Sustainability

Nanotechnology offers the potential, as many other technologies, to be used for the benefit of human beeing or for destructive means. We can only speculate what the actual future of nanotechnology will be.

The term "sustainability" can be described as the ability to achieve economic growth with protection of natural systems and provision of a high quality of life for people in the long run. As was mentioned above, technology plays an important role in the transition towards sustainable development, as it is one of the most significant ways in which we interact with our environment. We use technologies to extract natural resources, to modify them for human purposes. We need to develop and use technologies with sustainability in mind.

To be able to assess and understand whether a technology is sustainable or not it is important to provide an assessment against a number of different criteria, which are not actually developed yet.

To create such criteria, firstly we need to define, what sustainable technology is. By technologies we understand not just individual technologies, but total systems, which include processes goods and services, equipment, and organizational and managerial procedures. The technology that fits well with the goal of sustainable development and has the potential to protect or pollute the environment less, use resources in sustainable manner, recycle more wastes and products, and promotes a societal move towards sustainability; this is sustainable technology.

The evaluation criteria for sustainable technologies require different indicators that cover all sustainability aspects:

1. Social and economic conditions.
2. Productive capacity and production organization.
3. Ecosystem health.

One way of identifying the potential of nanotechnology, regarding sustainability effects is to use the criteria developed by the UN called the millennium development goals (MDG):

1. Eradicate extreme poverty and huger.
2. Achieve universal primary education.
3. Promote gender equality and empower women, which means to eliminate gender disparities in primary and secondary education.
4. Reduce child mortality, *i.e.*, reduce the number of children who die from water-borne diseases.
5. Improve maternal health, *i.e.*, reduce the ratio of maternal mortality.
6. Combat HIV/AIDS, malaria, and other diseases, *i.e.*, to stop the spread of major diseases.
7. Ensure environmental sustainability, *i.e.*, integrate the sustainable development principles into country programs and policies, stop the loss of environmental resources. Archive the improvement in lives by reducing the proportion of people without access to safe drinking water.
8. Develop a global partnership for development, *i.e.*, develop open and rule-based trading.

Following the described potentials of nanotechnology the impacts from nanotechnology could be on goals 1, 4, 6 and 7:

1. Nanotechnology has the potential to bring major improvements in the living standards of people in the developing world through the development of technologies within the agriculture and food sector. As with GMO this is, of course, dependent on who will control the technology, if it will be available for poor countries without too high costs.

4. Two million children die each year from water-related diseases, such as diarrhea, cholera, typhoid, and schistosomiasis, which result from a lack of adequate water sources and sanitation. Nanotechnology offers the potential of developing new and cheap water treatment technologies.

6. New methods for prevention, diagnosis and treatment of diseases. The Australian company,

Starpharma™ is developing a HIV microbicide gel, based on dendrimer nanotechnology, that will remain effective when applied by women up to four hours in advance of sexual intercourse, and the Austin Research Institute has conducted successful trials into nano-vaccines for malaria. Nanotechnologies include the "lab-on-a-chip", which offers all the diagnostic functions of a medical laboratory, and other biosensors based on nanosized tubes, wires, magnetic particles and semiconductor crystals. These inexpensive, hand-held diagnostic kits detect the presence of several pathogens at once and may be used for wide-range screening in small peripheral clinics.

7. Air pollution remediation: including nanotech-based innovations that destroy air pollutants with light; make catalytic converters more efficient, cheaper and better controlled; detect toxic materials and leaks; reduce fossil fuel emissions; and separate gases.

57.9 Risks to the Environment and Human Health

The potential risk with nanomaterials concerning negative effects on the environment and human health is another aspect of trying to assess it from a perspective of sustainable development. Here we can draw many conclusions from the experiences around genetically modified organisms (GMO). We also all have in mind the story of DDT where the initial positive effects ended in an environmental disaster.

Nanotechnology, is now maturing rapidly with more than 300 claimed nano-technology products already on the market [4]. Yet concerns have been raised that the very properties of nanostructured materials that make them so attractive could potentially lead to unforeseen health or environmental hazards. Along with the discussion of their enormous technological and economic potential, a debate about new and specific risks related to nanotechnologies has started. The catch-all term "nanotechnology" is so broad as to be ineffective as a guide to tackling issues of risk management, risk governance and insurance. A more differentiated approach is needed regarding all the relevant risk management aspects.

As it is stated in the OECD report [4] the spectre of possible harm—whether real or imagined—is threatening to slow the development of nano-technology unless sound, independent, and authoritative information is developed on what the risks are, and how to avoid them. In what may be unprecedented pre-emptive action in the face of a new technology, governments, industries, and research organizations around the world are beginning to address how the benefits of emerging nanotechnologies may be realized while minimizing potential risks.

In particular the health, environmental, and safety risks related to free rather than fixed manufactured nanoparticles have been identified. There is already a recognized health risk. Epidemiological studies on ambient fine and ultrafine particles incidentally produced in industrial processes and from traffic show a correlation between ambient air concentration and mortality rates. The health effects of ultrafine particles on respiratory and cardiovascular endpoints highlight the need for research also on manufacture nanoparticles that are intentionally produced.

The implications of the special properties of nanoparticles with respect to health and safety have not yet been taken into account by regulators. Size effects are not addressed in the framework of the new European chemicals policy REACH. Nanoparticles raise a number of safety and regulatory issues that governments are now starting to tackle. A review of current legislation and continuous monitoring by the authorities is needed.

At present, the exposure of the general population to nanoparticles originating from the dedicated industrial processes is marginal in relation to those produced and released unintentionally such as through combustion processes. The exposure to manufactured nanoparticles is mainly concentrated on workers in nanotechnology research and nanotechnology companies. Over the next few years, more and more consumers will be exposed to manufactured nanoparticles. Labeling requirements for nano-particles do not exist. It is inevitable that in future

manufactured nanoparticles will be released gradually and accidentally into the environment. Studies on biopersistence, bioaccumulation and ecotoxicity have only just started.

With respect to health, environmental and safety risks, almost all concerns that have been raised are related to free, rather than fixed manufactured nanoparticles. The risk and safety discussion related to free nanoparticles will be relevant only for a certain portion of the widespread applications of nanotechnologies. In initial studies, manufactured nanoparticles have shown toxic properties. These can enter the human body in various ways, reach vital organs via the blood stream, and possibly damage tissue. Due to their small size, the properties of nanoparticles not only differ from bulk material of the same composition but also show different interaction patterns with the human body. A risk assessment for bulk materials is, therefore, not sufficient to characterize the same material in nanoparticulate form.

57.10 Conclusions

According to its advocates nanotechnology offers an immense potential in many industrial sectors, *e.g.*, in energy and environmental areas. Following these positive evaluations of the potentials of nanotechnology it should lead to major contributions to a more sustainable development of our industrialized societies. The prospects for controversies over nanotechnology are very dependent on the uses to which it is put. Addressing the underlying governance issues will be the key issues. One of the most intelligent ways to address this is to dedicate further research to widely shared goals that are amenable to technological innovation like climate change and to take on board the lessons from a real engagement with public concerns. The risk is that large multinational companies will control nanotechnology and that the public influence will be very limited. For those involved in scientific policy making and funding this may be uncomfortable, but as recently pointed out "we cannot carry on ignorantly lurching from one mess to the next".

Many experiences show that the most fruitful way of handling potential conflicts is to use upstream conflict resolution that is to handle potential conflicts before they become intractable. This will demand more research on the environmental, health, social, and economic impacts of nanotechnology. The problem, however, is that the ratio of research money going into these areas compared to into the pure technological sector is very low. Today there is a positive attitude to nanotechnology and we can see products marketed as "contains nanoparticles". We only need some products showing toxic properties to drastically change such a positive attitude among the public. At the end of the 19th century there were found labels on spring water bottles saying "contains natural radioactivity". Who would use this today?

References

[1] California Institute of Technology, http://www.its.caltech.edu/~feynman/plenty.html

[2] Taniguchi N. On the basic concept of nanotechnology. Proceedings International Conference on Production Engineering. Tokyo, JSPE. Part II, Japan Society of Precision Engineering, 1974: 18–23.

[3] Quantum Sphere, http://www.qsinano.com/news/hitech-pr-2006_03_01.html
Opportunities and risks of Nanotechnologies, Report in co-operation with the OECD International Futures Programme, http://www.oecd.org/dataoecd/4/38/35081968.

[4] Foresight.org News release, Nobel winner Smalley responds to Drexler's challenge, http://www.nanotechwire.com/news.asp?nid=550

[5] Energy and Nanotechnology: Strategy for the future, Conference Report February 2005 http://www.rice.edu/energy/publications/energynanotechnology.html

58

An Overview of Reliability and Failure Mode Analysis of Microelectromechanical Systems (MEMS)

Yuanbo Li and Zhibin Jiang

Department of Industrial Engineering and Management
School of Mechanical Engineering, Shanghai Jiao Tong University
800 Dong Chuan Road, Min Hang District, 200240 Shanghai China

Abstract: The reliability issues concerning on microelectromechanical systems (MEMS) have steadily developed in recent years. One of the processes to understand MEMS reliability is to know the failure modes of these microdevices. In this chapter, we seek to report on both well known and unknown failure modes of MEMS. Most of the failure patterns are the same in nanoelectromechanical systems (NEMS), because NEMS followed a developmental path similar to that of MEMS in functional design, materials, and fabrication. Therefore, the existing results of MEMS failure modes can be used as a reference to nano-scale system reliability research. The failure modes discussed in this chapter contain stiction, wear, fracture, crystallographic defect, creep, degradation of dielectrics, environmentally induced failure, electric related failure, parasitic capacitance, dampening effects, delamination, and packaging.

58.1 Introduction

Reliability is the characteristic of a device concerning its ability to achieve specified requirements under well-defined conditions over a given period of time [1]. The goal of the reliability process is to understand the effect of design, processing, and post-processing on the device lifetime. Thus, issues on MEMS reliability are seeking to discover numerous methods and new technologies to increase the lifetime of MEMS.

In this chapter, we first provide a brief overview of MEMS and its reliability research methodologies, and itemize a list of MEMS failure modes that are commonly encountered.

Then we particularly discuss stiction, wear, fracture, crystallographic defect, creep, degradation of dielectrics, environmentally induced failure, electric related failure, parasitic capacitance, dampening effects, delamination, and packaging.

58.2 MEMS and Reliability

A variety of MEMS devices have been produced and some are commercially used in biomedical, aerospace, IT, industrial, defense, and automobile applications, such as accelerometers and digital micromirror devices, which were sold in 85 million units and $400 million from 2001 to 2002. These technologies allow numerous novel designs to be

Table 58.1. MEMS component categories based on their applications

Name	Definition
Micro sensors	Devices designed to detect physical or environmental changes
Infrared sensors; pressure sensors, inertial sensors, accelerometers, gyroscopes, chemical sensors, gas sensors, motion, thermal, and optical sensors.	
Micro actuators	Devices designed to activate or stimulate other MEMS component devices
Electrostatic actuators, thermal stimulus actuators	
Radio frequency (RF) MEMS	Devices used to switch, transmit, filter, and manipulate radio frequency (RF) signals
Metal contact switches, tunable capacitors, tunable filters, micro-resonators, RF switches	
Optical MEMS	Devices designed to direct, reflect, filter, or amplify light
Optical reflectors, micro-mirrors, optical switches, attenuators	
Micro-fluidic MEMS	Devices designed to interact with fluid-based systems
Pumps; Valves; Channels.	
Bio MEMS	Devices designed to interact with biological samples such as proteins, biological cells, medical reagents, *etc*.
DNA chips, microsurgical instruments, intra-vascular devices, laprascopic procedures, microfluidic chips	
Power MEMS	Devices designed to generate and store on-chip power or energy for portable systems
Microscale turbochargers, power generators, micro thrusters	
MEMS-based data storage systems	Small storage systems with large capacity
Micro-positioning and tracking devices, optical, thermal, or atomic force data tracks	

developed, and these new products will probably have serious economic, social, environmental, and military implications. Their names and applications are showed in Table 58.1 [2],[3].

Reliability issues are becoming increasingly important as MEMS devices shrink in size and become more complex, because failures are discovered at a late phase of fabrication, which causes high costs and waste of manufacturing resources. It is essential to reconsider reliability aspects from the traditional reactive way to the proactive way. In this chapter, we pay more attention to the failure physics approach. This is due to the fact that failure modes are governed by mechanical, electrical, thermal, and chemical processes or a combination of them all. Reliability of microsystems is dependent on their structure, material properties, fabrication process, and the life cycle environment. By understanding these possible failure modes, potential reliability problems can be identified and solved. Material design, characterization, and process evaluation therefore play an important role in assuring product reliability. A general scheme of the methodology is presented in Figure 58.1 for the study of micro-system reliability issues.

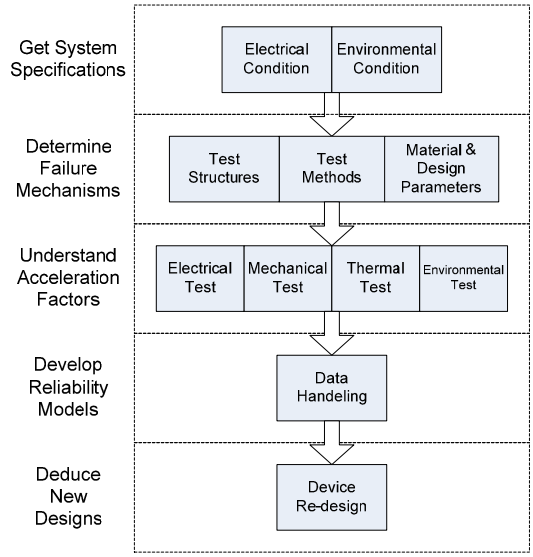


Figure 58.1. Scheme of microsystem reliability issues analysis methodology

58.3 MEMS Failures Mode and Mechanism Analysis

As mentioned above, a critical part of under-standing the reliability of any system comes from

Table 58.2. MEMS component categories based on their application

Failure modes	Failure mechanisms
Stiction	•Capillary forces •Van der Waals molecular forces •Casimir forces •Hydrogen bridging (H-bridging) • Electrostatic forces
Wear	•Adhesion •Abrasion •Corrosion •Friction
Fracture	•Stress induced bending, shearing, torsional •Shock induced •Fatigue
Crystallographic defect	•Point defects •Dislocations •Planar defects •Bulk defects
Creep	•Applied stress •Intrinsic stress •Stray stresses (thermal, residual)
Degradation of dielectrics	•Leakage •Charging •Breakdown
Environmentally induced failure	•Vibration •Shock •Humidity effects •Radiation effects •Contamination •Temperature changes
Electric-related failures	•Electrostatic discharge (ESD) •Electrical overstress (EOS) •Electromigration •Electrical breakdown •Electromagnetic pulses (EMP)
Packaging reliability	•Hermeticity and vacuum maintenance •Thermal issues
Other failure modes	•Parasitic capacitance •Dampening effects •Delamination

understanding the possible ways in which the system may fail. In MEMS, there are several failure modes that have been found to be the primary sources of failure within devices. In this section, we will give a short overview of the most common encountered failure modes and their modes.

Most MEMS are designed with some basic parts, such as cantilever beams (single side clamped, double side clamped), membranes (either closed at the sides to another structural member, or as a free floating plate), springs (often doubling as cantilever beams), hinges, *etc*. Unassailably, these elements often suffer from the same degradation or failure modes, regardless of their application. A list of common degradation or failure modes of MEMS is given in Table 58.2.

58.3.1 Stiction

One of the most important and almost unavoidable problems in MEMS is stiction, which was first reported in 1950 by Bowden and Tabor. Stiction is the adhesion of contacting surfaces due to surface forces, which mainly contain capillary forces, van der Waals molecular forces, Casimir forces, hydrogen bridging, and electrostatic forces [4].

The sticion problem of MEMS can be divided into two categories, one is release-related stiction and the other is in-use stiction [5]. Release-related stiction occurs during the process of the sacrificial layer removal in fabrication of microstructures, and such stiction is caused primarily by capillary forces.

In-use stiction usually occurs when micro-structures are exposed to a humid environment [6]. The relation between the capillary stiction force and the relative humidity is given in Figure 58.2. The model of single side clamped cantilever beams sticking to the substrate over a certain length at the

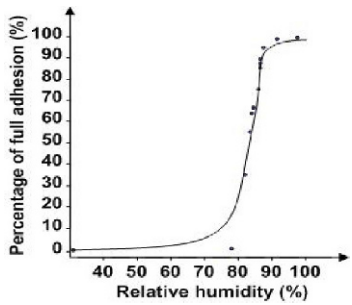


Figure 58.2. Function between adhesion and relative humidity [11]

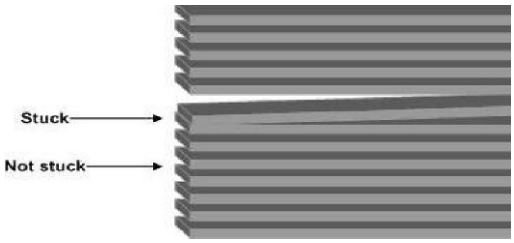


Figure 58.3. Cantilever beams stuck at the free end [12]

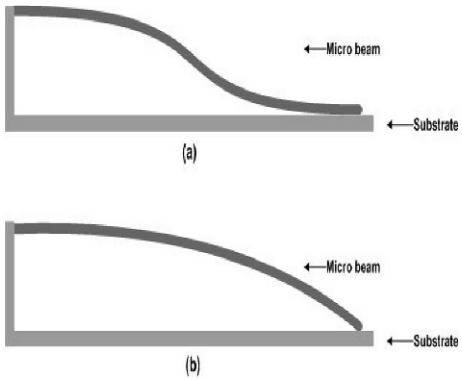


Figure 58.4. (a) S-shaped beam and (b) arc-shaped beam [8]

tip was used to calculate the adhesive forces (Figure 58.3). Yee *et al*. [7] later modifications to the model to include residual stress gradients in the free-standing thin film beams. De Boer [8],[9] and [10] first distinguished two kinds of adhered beams (Figures 58.4(a) and (b)): the deflected beam can be S-shaped or arc-shaped.

Van der Waals forces will become important for the adhesion behavior when the surfaces of the MEMS device are in a completely waterless environment, or when hydrophobic surfaces are used. If there is water between the surfaces, capillary forces will completely dominate the van der Waals forces, unless the surfaces are exceptionally smooth.

The Casimir force is the attractive pressure between two flat, parallel metal plates placed very near to each other in a vacuum. The Casimir force is reduced to the so-called nonretarded van der Waals force when the separation between the metallic surfaces is small compared to the characteristic wavelength of their absorption spectra [13]. Svetovoy *et al.* [14], Pinto [15] and Lamoreaux [16] reported calculations of the Casimir force. Sernelius *et al*. [17] complemented some flaws in Lamoreaux' findings.

H-bridging may increase the surface interaction energy, when MEMS surfaces are covered with OH bonds. When the ambient temperature is below 200°C, a surface with molecules of H-bridging will certainly be a hydrophilic surface, which will intrigue significant capillary condensation, unless the relative humidity is extremely low [18]. From wafer bonding experiments, Spierings *et al*. [19] and Backlund *et al*. [20] calculated that the adhesion energy was between 0.6 Jm^{-2} and 0.27 Jm^{-2} based on this bonding model. Legtenberg *et al*. calculated, for Si MEMS, that adhesion energies for flat surfaces are between 0.1 Jm^{-2} and 0.3 Jm^{-2}. Due to the surface roughness, the real interaction energy is much lower and H-bridging may only be observable for hydrophilic, OH terminated surfaces in a waterless environment [18].

Theoretically, stiction due to electrostatic forces can be categorized as temporary electrostatic charging and permanent charge accumulation. Temporary charging can occur during processing or operation as a result of differences in contact potential, tribocharging of rubbing surfaces, and ion trapping in oxide layers [21]. Permanent charging is not expected due to these effects because the non-equilibrium charging will relax in time [22].

58.3.2 Wear

Wear occurs when the material is removed from a solid surface as the result of mechanical action [23]. Wear involves not only the mechanical properties and chemistry of the objects in contact, but also the pressure, the adhered lengths, and the interfacial velocity, as well as the lubrication condition under which these objects make contact [24]. Wear can be categorized into three broad branches: adhesive wear, abrasive wear, and corrosive wear.

Adhesive wear occurs when one surface pulling fragments off of another surface while they are sliding. The surface forces finally resulting adhesion originate from a number of attractive or repulsive forces, including capillary, van der Waals, electrostatic forces and so on. When studying the adhesion forces and contact types, the sub-

boundary lubrication (SBL) adhesion model, the sidewall adhesion model [25], the elastic-plastic model [26], adhesive contact model, and the three-dimensional fractal surface geometry model [27] are usually used. Experiments show that the adhered length, rest time, relative humidity, temperature, and sliding velocity of a micro-cantilever can affect the adhesion forces between two contacting surfaces [28],[29]. Ali and Phinney [28] indicated that only beams that have adhered lengths during actuation smaller than 0.4–0.5 of their length are able to free themselves after the actuating voltage is removed. A study at Sandia National Laboratories found that wear related failure rates can be described by the lognormal and the Weibull models.

Abrasive wear occurs when a hard, rough surface slides on top of a softer surface and strips away underlying material. While less prevalent in MEMS than adhesive wear, it can occur if particulates are caught in microgears and this can tear a surface apart. Abrasive wear was calculated on the basis of statistical data and elaborated formulas have been given [30],[31] and [32].

Corrosive wear occurs when two surfaces chemicall Corrosive wear occurs when two surfaces chemically interact with one another, and the sliding process strips away one of the reaction products. This type of wear may cause failure in chemically active MEMS. Certain types of microfluidic systems and biological MEMS are susceptible to corrosive wear. Ovchinnikov and Pochtman [33] specifically reviewed this field. Zwierzycki and Stachowiak [34] discussed some mathematical models describing corrosive and mechanical wear, and compared their model with others.

Friction becomes dominant over the inertial and gravitational forces when the device size shrinks. The important investigated tribological properties of MEMS include the adhesive force and friction force dependence on operating parameters such as rest time and sliding velocity, and environmental conditions such as relative humidity and temperature [29].

58.3.3 Fracture

One of the most important and almost unavoidable problems in MEMS is fracture. Fracture is most likely to occur in structural beams with long thin pieces of material that often serves as the supporting basis for a structure, which are a basic building block of most MEMS devices. Stress and shock are recognized as the two factors that induce fracture. It has been investigated that stress induced fracture is due to three ways things: bending stress [35],[36], shearing stress [37],[38] and torsional stress [39].

When analyzing bending stress on a structural beam (with one or two sides clamped), the critical issue is to understand how the beams bend under different loadings. The most common method to determine this involves the Euler–Bernoulli equation. When calculating the shearing stress, the average shearing stress and the vertical shear in a section of a beam should be calculated. When calculating torsional stress, it is useful to relate a torque to the angle of twist, also the length of the beam, the modulus of rigidity, the longer side of the surface and the shorter side of the surface. When analyzing shock induced fracture, we can refer to shock impact as an environmentally induced failure.

Fatigue is caused by the cyclic loading of a structure below the yield or fracture stress of a material, which is shown to be a major failure mechanism in polysilicon MEMS structures [40]. This loading leads to the formation of surface microcracks that cause the slow weakening of the material over time and create localized plastic deformations. Doubly clamped silicon micro-components models are used in the research. Recent research reported that water and water vapor can also accelerate fatigue processes in Si MEMS structures, ultimately leading to premature fracture of polysilicon components under cyclic loading conditions [41]. Stress cycles, local micro-cracking originating on the surface of silicon films create tensile residual stress, which strongly influence the fatigue strength [42]. Another fatigue mechanism termed reaction-layer fatigue suggests that fatigue of silicon-based microfilms occurs through a process of sequential, mechanically

induced oxidation and environmentally assisted cracking of the surface layer of the material. This progressive accumulation of fatigue damage is accompanied with a decrease in the stiffness of microfilms of silicon materials.

58.3.4 Crystallographic Defects

Many materials used for MEMS are produced by means of crystalline methods, which may induce many kinds of defects, which are recognized as crystallographic defects. Crystallographic defects may be classified as point defects, dislocations, planar defects, and bulk defects.

Point defects are departures from symmetry in the alignment of atoms in a crystal that affects only one or two lattice sites. These defects are created in semiconductors during growth, where their formation is governed by thermodynamics and growth kinetics [43],[44]and [45]. Point defects are categorized into the following groups: vacancies, interstitial, point replacement, impurities, anti-site defects, and complexes [45],[46]. A dislocation is a one-dimensional array of point defects in an otherwise perfect crystal and can be observed using transmission electron microscopy, field ion microscopy, and atom probe techniques. They occur when a crystal is subjected to stresses that exceed the elastic limits of materials. The two basic types of dislocations are screw dislocation and the edge dislocation caused by the termination of a plane of atoms in the middle of a crystal. Planar defects have three types of defects called grain boundaries occurring where the crystallographic direction of the lattice abruptly changes, anti-phase boundaries occurring in ordered alloys, and stacking faults occurring in a number of crystal structures. Bulk defects contain voids and impurities.

58.3.5 Creep

Creep, the slow movement of atoms under mechanical stress, is expected to be one of the major reliability problems for certain types of MEMS, such as RF MEMS switches, especially at high RF powers.

Recent research reported that both increases in temperature and stress are shown to increase the creep rate. According to Tregilgas' report, the creep effect in Al thin films is so large that other materials should be found to replace it. In order to achieve a high melting point where the probability of creep is low, a number of Al compounds have been developed, such as Al_3Ti, AlTi, AlN and a mixture of Al_3Ti and AlN [47]. Modlinski *et al*. used substrate curvature measurements to study the creep properties of Al, $Al_{98.3}Cu_{1.7}$, $Al_{99.7}V_{0.2}Pd_{0.1}$ and $Al_{93.5}Cu_{4.4}Mg_{1.5}Mn_{0.6}$ films using isothermal tensile stress relaxation [48],[49], and [50]. They found that $Al_{93.5}Cu_{4.4}Mg_{1.5}Mn_{0.6}$ is the alloy that is most resistive to creep. Tuck *et al*. [51] investigated creep in polysilicon at high temperatures under stress. They showed that with the appropriate temperature and stress levels, the material begins to creep and the data follow a typical curve as shown in Figure 58.5. The strain *versus* time curve illustrates three stages of creep in polysilicon, the transient creep region, the steady state strain region, and the strain acceleration region. The first stage is identified by a continuously decreasing strain rate. The second stage has a constant strain rate due to the two competing processes of strain hardening and recovery. The third stage ultimately leads to failure, which is characterized by grain boundary separation, internal crack, cavities, and possibly necking in the deformation region.

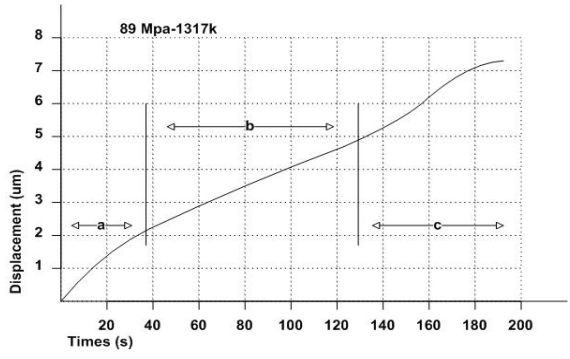


Figure 58.5. A typical creep curve illustrating three stages of creep in polysilicon [51]

Stray stresses are a failure mechanism that is endemic to thin film structures. In MEMS, small

stresses will cause noise in sensor outputs and large stresses will lead to mechanical deformation. Thermal and residual stresses are the two sources of stray stress in MEMS.

Thermal stress is a process-induced factor caused by bimetallic warping. Residual stresses are a result of the energy configuration of thin films. If these films are not in their lowest energy state, residual stress can either shrink or expand the substrate. While there are high-temperature techniques for annealing out residual stress, these methods are not always compatible with MEMS processing.

58.3.6 Degradation of Dielectrics

A well-known problem with MEMS containing dielectric layers is the charging that may occur in the dielectric layer. Silicon dioxide and silicon nitride coatings are commonly used as dielectric layers for short-circuit protection in capacitive silicon microsensors and microactuators, as well as RF MEMS [52].

The most obvious source of dielectric charging is ionizing (nuclear) radiation, the effect of which has been tested on electrostatic, electrothermal and bimorph actuators. The two types of radiation used in experiment are low-energy X-ray and Co-60 gamma. For electrostatic actuators, they exhibited a decrease in capacitance and thereby an increase in voltage per deflection when subjected to the low-energy X-ray radiation environment but no changes in Co-60 gamma environment. For the electrothermal actuators, neither X-ray nor gamma irradiation affected their operation [53].

In order to prevent degradation of the dielectrics phenomenon, new coating materials, the high-k gate dielectric materials are used. They are dielectric materials with a dielectric constant greater than the dielectric constant of silicon dioxide, normally k > 4. A review of high-k dielectrics reliability issues has been made by Ribes *et al*. [54].

The separate consideration of soft gate oxide breakdown (SBD), progressive (PBD), and hard (HBD) breakdown events is necessary to set up an adequate application specific reliability assessment methodology. SBD and the HBD are localized and randomly distributed all over the device area [55]. SBD and the HBD both coexist, soft and hard breakdowns being spatially uncorrelated. The PBD is the initiator of SBD or HBD. Various breakdown occurrences are shown in Figure 58.6. The first stack wear-out is the interfacial layer breakdown. It is characterized by a progressive breakdown (PBD). The charge to breakdown of this event is dependent on the gate current and thuso to the high-k layer thickness. The gate current increases until second breakdown, which can be soft (SBD) or hard (HBD) depending on the spot size. Both breakdowns have been identified as the breakdown of the high- layer [54].

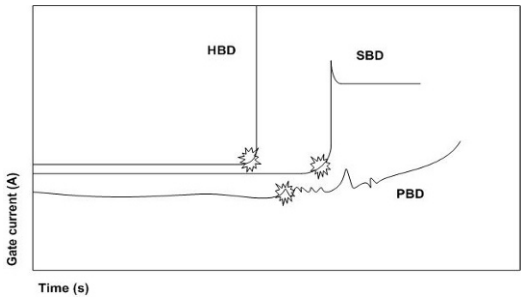


Figure 58.6. The three different occurrences of breakdown (HBD, SBD, PBD) [54]

Wen Luo, Yue Kuo and Way Kuo [56] investigated the intrinsic reliability of some promising high-k gate dielectric candidates, TaO_x, HfO_x, ZrO_x, Hf-doped TaO_x, and Zr-doped TaO_x thin films. The result of their research indicated that high-*k* thin films showed a lower leakage current than SiO_2, but they had the disadvantage of a higher relaxation current. Additionally, measurements of PZT/HfO_2 multi-layered dielectrics showed the expected high dielectric constant for high switching isolation and low leakage current for very low operating power consumption. From bias-stressing tests, PZT/HfO_2 was verified as having significantly better dielectric characteristics in very low charging effects and a long lifetime in comparison to Si_3N_4 [57].

58.3.7 Environmentally Induced Failure

Environmentally induced failure mechanisms are external effects that can also cause failure in

MEMS. The most important failures induced by environment are vibration, shock, humidity, and radiation.

For micromirror clamped situation, when the vibration frequencies are between 200 Hz and 10 kHz, it works properly [58],[59]. When the actuator is not clamped, vibration causes motion in the actuator promoting the surfaces to rub, and this generates wear debris leading to failure [60]. To ensure accurate detection and measurement of MEMS vibration, many vehicles and testing methods have been invented and fabricated, for example, the piezoelectric actuator (PZT) method [61], optical microscopy combined with image processing [62], laser TV holography [63], and spin-valve sensors [64].

Shock differs from vibration in that it is a single mechanical impact instead of a rhythmic event. Exposure of MEMS to shock environments can occur during fabrication, deployment, or operation. These may lead to failures in different modes, inducing fracture, delamination, and stiction, especially in microactuators [65]. When analyzing the failure modes of shock loaded MEMS, a single clamped beam model (microstructures attached to elastic substrates) [66], clamped-clamped beam model (microstructures attached to solid surface) [67], and dynamic finite element analysis (FEA) method [68],[69] are used.

Humidity can induce brittle fatigue, adhesion, and wear. As mentioned before, adhesion increases exponentially with relative humidity [70]; and wear debris decreases as the humidity increases, because when the humidity level is high, the formation of surface hydroxides may act as a lubricant [71].

The knowledge of radiation effects on MEMS is still limited. Many researchers have studied the radiation effect on thermal actuators [72], accelerometer [73],[74], actuators [53]. Recent work indicates that because dielectric layers trap charged particles, creating a permanent electric field under radiation environment, radiation-tolerant designs must limit the use of dielectrics, which could be a challenging design problem [73],[74].

Contamination due to inappropriate packaging may interfere with the operation of moving MEMS structures [75]. The effects of random contamination have been modeled in the CAD program CARAMEL (contamination and reliability analysis of microelectromechanical layout) [76]. The results of CARMEL simulations indicate that a wide range of defective structures are due to the presence of particulate contaminations [76],[77]. These particles have been known to electrically short out MEMS and can also induce stiction and adhesion. Defects induced by particulates are classified into three categories: surface, anchor, and broken structures [78]. Other forms of contamination include ionic contamination [79] and lead contamination [80].

Temperature changes have serious effects on MEMS. High temperatures may cause buckling of the switch structure, which may lead to device failure. By contrast, low temperatures may result in an undesirably high pull-in voltage, which can compromise the device life by charge build-up or lead to other failure modes [81],[82], and [83].

58.3.8 Electric-related Failures

Another failure mechanism is electric charge induced failure. It includes four failure models: electrostatic discharge (ESD), electrical overstress (EOS), electromigration, electrical breakdown, and electromagnetic pulses (EMP).

ESD is the transfer of electrical charge between two bodies at different potentials, either through direct contact or through an induced electrical field. Such an event accounts for more than 25% of failures in microelectronic devices, including gate oxide breakdown, junction spiking, and latch-up [84]. In general, ESD can be characterized by the different origins of the charges generated and thus by three different models: the human body model (HBM), the charge device model (CDM), and the machine model (MM) [85]. Preventing ESD damage to components involves two approaches: (1) control of the manufacturing environment to suppress electrostatic charge generation and damaging discharge events, and (2) modification of the component design to increase the ability to withstand an ESD event [86].

EOS is caused by thermal overstress to a component's circuitry. The amount of damage caused by EOS depends on the magnitude and

duration of electrical transient pulse widths, which can be broadly classified into long (>100 ms) and short (<100 ms) types. For short pulse widths, the most common failure mode is junction spiking; for long electrical pulse widths, the most common failure modes are melted metallization and open bond wires [87]. Preventing EOS damage involves three approaches: (1) ensure proper testing of components and boards; (2) use quality power supplies with the following features: over voltage protection, proper heat dissipation, use of fuses at critical locations; (3) adhere to a strict equipment maintenance program to ensure that equipment is properly grounded and there are no loose connections.

Electromigration is mass transport due to momentum exchange between conducting electrons and diffusing metal atoms. Eelectromigration-induced failure involves flux divergence, vacancy, and atom accumulation with or without compositional variations, void and hillock nucleation, and growth and shape changes [88],[89]. Ambient temperature, current density, and the direction of electron flow are three important factors leading to electromigration of MEMS [90],[91], and [92].

Electrical breakdown leads to disruption in a polymer and occurs when an applied voltage can no longer be maintained across material without excessive flow of current and physical disruption. EMP induces a broadband, high-intensity, short-duration burst of electromagnetic energy, which leads to disruption in a polymer [93],[94],[95],[96], and [97].

58.3.9 Packaging Reliability

The two key issues related to MEMS packaging reliability are hermeticity and vacuum maintenance, and thermal issues. We discuss them separately.

Vacuum packaging is important because several MEMS devices such as resonators, gyroscope sensors, and pressure sensors need to maintain the frequency response and quality factor (Q-factor). Degradation of the vacuum and hermetic condition may induce internal friction, charge separation in capacitive devices, and moisture corrosion in metallization, or electrolytic conduction [98],[99]. Currently, vacuum packaging can be accomplished on the wafer level by the glass-silicon anodic bonding technique [100],[101]. However, few methods exist to ensure the reliability of anodically bonded vacuum packaging. Sung-Hoon Choa [102] found that leakage and outgassing are the two dominant failure mechanisms of anodic vacuum packaging.

Two key thermal issues related to MEMS packaging are: heat dissipation from actuators and integrated circuitry components; and thermal stress generated during the packaging process. When the size of transistor on a chip shrinks, heat dissipation becomes a serious problem. Inefficient power dissipation may raise the working temperature and affect device performance. Moreover, thermal stress may cause deformation of the MEMS structure, resulting in frequency change, or even breakage of the structure [103]. Because most MEMS packages still follow the typical IC packaging architecture, a thermal management device called a heat pipe is used in MEMS fabrication.

58.3.10 Other Failure Mechanisms

Many other factors, such as parasitic capacitance, dampening effects, and delamination, may also induce MEMS failure. Parasitic capacitance does not cause failure in and of itself, but it can cause unexpected electrical and mechanical behavior in devices. MEMS damping is usually caused by the presence of gaseous molecules. There are multiple kinds of damping caused by the atmosphere, and the type of damping depends largely upon the device geometry. For closely packed parallel surfaces, squeeze film dampening will be predominant; for a device moving in plane, there will be structural dampening. The way to prevent damping is to utilize vacuum packaging. Delamination can be induced by a number of means, from mask misalignments to particulates on the wafer during processing. It can also arise as the result of fatigue induced by the long term cycling of structures with mismatched coefficients of thermal expansion. Acoustic microimaging (AMI) and the scanning acoustic microscope (SAM) are

commonly used to assess the delamination in plastic encapsulated microcircuits [104],[105].

58.4 Conclusions

Although reliability issues of MEMS have been researched in recent years, they are still in the initial stage and are not yet mature. The knowledge of failure modes and failure mechanisms of MEMS is still limited and much work is urgently needed. One possible way to study reliability issues of MEMS would be to identify the failure phenomenon with different patterns, because many failure modes are not seen in the IC industry. In this case, the expectations and perceptions of MEMS failure issues have become important in industrial manufacturing and laboratory researching scopes, which requires carefully identification experiments on MEMS devices to gain insightful knowledge of different failure modes and mechanisms.

In addition, researchers must take into account MEMS failure issues such as stiction, wear, fracture, crystallographic defect, creep, degradation of dielectrics, environmentally induced failure, electric related failure, parasitic capacitance, dampening effects, and delamination and packaing. To gain a better understanding of these failures, many observation and testing instruments should be used in the semiconductor industry to study MEMS, such as scanning electron microscopy (SEM), focused ion beams (FIB), atomic force microscopy (AFM) [106], and ballistic-electron-emission microscopy (BEEM) [107]. Simulation, modeling methods, and an interrelated mathematical approach, such as the neural-network method [108], and the unified quantum correction model [109], should be used to study MEMS failure modes and improve MEMS performance. MEMS device failure mechanism research should stress the characteristics of the basic materials, and the physical disciplines behind them before this industry can become a successful commercialization.

Moreover, MEMS reliability does not merely contain failure mechanism analysis. As we mentioned in Section 58.2, it is just part of the MEMS reliability process. Traditionally “input” reliability research should be changed to an “output” research method, which requires researchers to consider reliability aspects in all phases of the product development.

References

[1] Silva GA. Introduction to nanotechnology and its applications to medicine. Surgical Neurology 2004; 61(3):216–220.

[2] Petersen K. Bringing MEMS to market. IEEE Solid State Sensors and Actuators Workshop 2000; 60–64.

[3] Walraven JA, Introduction to applications and industries for microelectromechanical systems (MEMS). Sandia National Laboratories, Albuquerque, NM, 2000.

[4] Maboudian R, Howe RT. Critical review: Adhesion in surface micromechanical structures. Journal of Vacuum Science and Technology 1997;15(1): 1–20

[5] Kim BH, Chung TD, Oh CH. A new organic modifier for anti-stiction. Journal of Microelectromechanical Systems 2001;10(1):33–40.

[6] Zhao YP. Stiction and anti-stiction in MEMS and NEMS. Acta Mechanica Sinica 2003;19(1)1:1–10.

[7] Yee Y, Park M, Chun K, A sticking model of suspended polysilicon microstructure including residual stress gradient and postrelease temperature. Journal of Microelectromechanical Systems 1998;7(3):339–344.

[8] de Boer MP, Tabbara MR, Dugger MT, Clews PJ, Michalske TA. Measuring and modeling electrostatic adhesion in micromachines.IEEE International Conference on Solid State Sensors and Actuators 1997;1:229–232.

[9] de Boer MP, Knapp JA, Mayer TM, Michalske TA. The role of interfacial properties on MEMS Performance and Reliability. Proceedings SPIE 1999; 3825:2–15.

[10] de Boer MP, Michalske TA. Accurate method for determining adhesion of cantilever beams. Journal of Applied Physics 1999;86(22):817–827.

[11] Bowden FP, Tabor D. Friction and lubrication of solids. Clarendon Press, Oxford, 1950.

[12] Mastrangelo CH, Hsu CH. A simple experimental technique for the measurement of the work of adhesion of microstructures. Proceedings IEEE Solid-State Sensor and Actuator Workshop 1992;208–214.

[13] Buks E, Roukes ML, Stiction. Adhesion energy, and the Casimir effect in micromechanical systems. Physical Review B 2001; 63(3): 033402.
[14] Svetovoy VB, Lokhanin MV. Precise calculation of the Casimir force between gold surfaces. Modern Physics Letters A 2000; 15(22–23):1437–1444.
[15] Pinto F. Computational considerations in the calculation of the Casimir force between multilayered systems. International Journal of Modern Physics A 2004;19(24):4069–4084.
[16] Lamoreaux SK. Calculation of the Casimir force between imperfectly conducting plates. Physical Review A – Atomic, Molecular, and Optical Physics 1999;59(5):3149–3153.
[17] Boström M, Sernelius BE. Comment on ‘‘Calculation of the Casimir force between imperfectly conducting plates’’. Physical Review A – Atomic, Molecular, and Optical Physics 2000; 61(4): 461011–461013.
[18] van Spengen WM, Puers R, de Wolf I. A physical model to predict stiction in MEMS. Journal of Micromechanical and Microengineering 2002;12: 702–713.
[19] Spierings GACM, Haisma J, Diversity and interfacial phenomena in direct bonding. Proceedings of the First International Symposium on Semiconductor Wafer Bonding: Science, Technology and Applications, Phoenix, AZ 1991; 92(7):18–32.
[20] Backlund Y, Hermansson K, Smith L. Bond-strength measurements related to silicon surface hydrophilicity. Journal of the Electrochemical Society 1992;139(8):2299–2301.
[21] Alley RL, Cuan GJ, Howe RT, Komvopoulus K. The effect of release-etch processing on surface microstructure stiction. Proceedings IEEE Solid-State Sensors and Actuators Workshop 1992; 202–207.
[22] Tasy N, Sonnenberg T, Jansen H, Legtenberg R, Elwenspoek M. Stiction in surface micromachining. Jounal of Micromechical Microengineering 1996; 6:385–397.
[23] DiBenedetto AT. The structure and properties of materials. McGraw-Hill, New York, 1967.
[24] Tanner DM, Dugger MT. Wear mechanisms in a reliability methodology. Proceedings of SPIE – The International Society for Optical Engineering 2003; 4980:22–40.
[25] Ashursta WR, de Boer MP, Carraro C, Maboudian R. An investigation of sidewall adhesion in MEMS. Applied Surface Science 2003;212:735–741.
[26] Suh AY, Polycarpou AA. Adhesion and pull-off forces for polysilicon MEMS surfaces using the sub-boundary lubrication model. Journal of Tribology 2003;125:193–199.
[27] Morrow CA, Lovell MR. A solution for lightly loaded adhesive rough surfaces with application to MEMS. Transactions of the ASME 2005;127: 206–212.
[28] Ali SM, Phinney LM. Investigation of adhesion during operation of MEMS cantilevers. Proceedings of SPIE 2004;5343.
[29] Tambe NS, Bhushan B. Scale dependence of micro/nano-friction and adhesion of MEMS/ NEMS materials, coatings and lubricants. Nanotechnology 2004;15:1561–1570.
[30] Ikramov U, Machkamov KC, Calculation and Prediction of Abrasive Wear. Verlag Technik, Berlin, 1987.
[31] Winter H, Plewe HJ. Abrasive wear and endurance calculation for lubricated, low-speed gears, part II: Calculation methods and damages limits. Anteriebstechnik 1982;21: 282–286.
[32] Putilov YY, Putilova IV. Calculations of the abrasive wear of pipelines of the ash and coal dust pneumatic-transport facilities of thermal power stations. Thermal Engineering 2003;50(9):765–771.
[33] Ovchinnikov IG, Pochtman YM. Calculation and rational design of structures subjected to corrosive wear. Soviet Materials Science 1991;27(2):105–116.
[34] Zwierzycki W, Stachowiak A. Corrosive and mechanical wear calculation. Scientific Papers of the Institute of Machine Design and Operation of the Technical University of Wroclaw 2002; 87(27): 366–371.
[35] Jones PT, *et al*., Statistical characterization of fracture of brittle MEMS materials. Proceedings SPIE 1999; 3880: 20–29.
[36] Hu S. Critical Stress in silicon brittle fracture, and effect of ion implantation and other surface treatments. Journal of Applied Physics 1982; 53: 3576–3580.
[37] Tas NR, Gui C, Elwenspoek M. Static friction in elastic adhesive MEMS contacts, models and experiment. Proceedings of IEEE Transactions on Electron Packaging Manuf. 2000; 193–198.
[38] Cauley TH III, Rosario JD, Pisano AP. Feasibility study of a MEMS viscous rotary engine power system (VREPS). American Society of Mechanical Engineers, Fluids Engineering Division (Publication) FED 2004; 260:301–308
[39] Wolter A, Schenk H, Korth H, Lakner H. Torsional stress, fatigue and fracture strength in

silicon hinges of a micro scanning mirror. Proceedings of SPIE 2004; 5343:176–185.
[40] Allameh SM, Shrotriya P, Butterwick A, Brown SB, Soboyejo WO. Surface topography evolution and fatigue fracture in polysilicon MEMS structures. Journal of Microelectromechanical Systems 2003;12(3): 313–324.
[41] Jones PT, Johnson GC, Howe RT. Fracture strength of polycrystalline silicon. Microelectromechanical Structures for Materials Research 1998; 27: 197–202.
[42] Varvani-Farahani A. Silicon MEMS components: a fatigue life assessment approach. Microsystem Technologies 2005;11:129–134.
[43] Hu B, Takahashi H. Effects of helium on behavior of point defect produced by irradiation in low activation Fe-Cr-Mn (M, V) alloys. Acta Metallurgica Sinica 2004; 40(9): 955–961.
[44] Hao YL, Yang R, Song Y, Cui YY, Li D, Niinomi M. Concentration of point defect and site occupancy behavior in ternary NiAl alloys. Materials Science and Engineering A 2004; 365;(1–2): 85–89.
[45] Tuomisto F, Saarinen K. Introduction and recovery of point defects in electron-irradiated ZnO. Physical Review B 2005; 72: 85206–85206.
[46] Cândido L, Phillips P, Ceperley DM. Single and paired point defects in a 2D Wigner crystal. Physical Review Letters 2001; 86(3): 492–495.
[47] Tregilgas JH. Micromechanical device having an improved beam. Texas Instruments Inc., United States Patent, 1996; 5:552,924.
[48] Modlinski R, Witvrouw A, Ratchev P, Jourdain A, Simons V, Tilmans HAC, den Toonder JMJ, Puers R, de Wolf I. Creep as a Reliability problem in MEMS. Microelectronics Reliability 2004:44; 1733–1738.
[49] Modlinski R, Witvrouw A, Ratchev P, Puers R, den Toonder JMJ, de Wolf I. Creep characterization of Al alloy thin films for use in MEMS applications. Microelectronic Engineering 2004; 76: 272–278.
[50] Modlinski R, Ratchev P, Witvrouw A, Puers R, de Wolf I. Creep-resistant aluminum alloys for use in MEMS. Journal of Micromechanical Microengineering 2005; 15: 165–170.
[51] Tuck K, Jungen A, Geisberger A, Ellis M, Skidmore G. A study of creep in polysilicon MEMS devices. Journal of Engineering Materials and Technology 2005; 127: 90–96.
[52] Wibbeler J, Pfeifer G, Hietschold M. Parasitic charging of dielectric surfaces in capacitive microelectromechanical systems (MEMS). Sensors and Actuators A 1998; 71: 74–80.
[53] Caffey JR, Kladitis PE. The effects of ionizing radiation on microelectromechanical systems (MEMS) actuators: Electrostatic, electrothermal, and bimorph. Proceedings of the IEEE International Conference on Micro Electro Mechanical Systems (MEMS) 2004; 133–136.
[54] Ribes G, Mitard J, Denais M, Bruyere S, Monsieur F, Parthasarathy C, *et al.,* Review on high-k dielectrics reliability issues. IEEE Transactions on Device and Materials Reliability 2005; 5(1):5–19.
[55] Bruyère S, Vincent E, Ghibaudo G. Quasibreakdown in ultrathin SiO films: Occurrence characterization and reliability assessment methodology. Proceedings of the IEEE International Reliability Physics Symposium, San Jose, CA April 10–12, 2000; 48–54.
[56] Luo W, Kuo Y, Kuo W. Dielectric relaxation and breakdown detection of doped tantalum oxide high-k thin films. IEEE Transactions on Device and Materials Reliability 2004; 4(3): 488–494.
[57] Tsaur J, Onodera K, Kobayashi T, Ichiki M, Maeda R, Suga T. Wideband and high reliability RF-MEMS switches using PZT/HFO_2 multi-layered high-k dielectrics. Proceedings of 42nd Annual IEEE International Reliability Physics Symposium June 2004; 259–264.
[58] Lee SS, Motamedi E, Wu MC. G-performance characterization of surface-micromachined FDDT Optical Bypas Switches. Proceedings of SPIE 1997; 3226: 94–101.
[59] Huang LS, Lee SS, Motamedi E, Wu MC, Kim CJ. MEMS packaging for micro mirror switches. Proceedings of 4th Electronic Components and Technology Conference, Seattle, WA, May 25–28 1998; 593–597.
[60] Tanner DM, Walraven JA, Helgesen KS, Irwin LW, Gregory DL, Stake JR, *et al.,* MEMS reliability in a vibration environment. IEEE International Reliability Physics Symposium 2000; 139–145.
[61] Zhang W, Meng G. Active vibration control of micro-cantilever beam in MEMS. Proceedings of the 2004 International Conference on Intelligent Mechatronics and Automation, Chengdu, China August 2004: 272–276.
[62] Petitgrand S, Bosseboeuf A. Simultaneous mapping of out-of-plane and in-plane vibrations of MEMS with (sub)nanometer resolution. Journal of Micromechical Microengineering 2004;14:S97–S101.
[63] van Spengen WM, Puers R, Mertens R, de Wolf I. Characterization and failure analysis of MEMS: High resolution optical investigation of small out-

of-plane movements and fast vibrations. Microsystem Technologies 2004;10: 89–96.

[64] Li HH, Gaspar J, Freitas PP, Chu V, Conde JP. MEMS microbridge vibration monitoring using spin-valve sensors. IEEE Transactions on Magnetics 2002;38(5):3371–3373.

[65] Tanner DM, Walraven JA, Helgesen K, Irwin LW, Brown F, Smith NF, *et al.,* MEMS reliability in shock environments. IEEE International Reliability Physics Symposium in San Jose, CA 2000; 129–138.

[66] Millet O, Collard D, Buchaillot L. Reliability of packaged MEMS in shock environment. Crack and stiction modeling. Proceedings of SPIE 2002; 4755: 696–703.

[67] de Coster J, Tilmans HAC, van Beek JTM, Rijks TGSM, Puers R. The influence of mechanical shock on the operation of electrostatically driven RF-MEMS switches. Journal of Micromechical Microengineering 2004;14: S49–S54.

[68] Wagner U, Franz J, Schweiker M, Bernhard W, Müller-Fiedler R, Michel B, *et al.,* Mechanical reliability of MEMS-structures under shock load. Microelectronics Reliability 2001;41:1657–1662.

[69] Jiang YQ, Du MH, Huang WD, Xu W, Luo L. Simulation on the encapsulation effect of the high-G shock MEMS accelerometer. Proceedings of the Sixth IEEE CPMT Conference on High Density Microsystem Design and Packaging and Component Failure Analysis 2004; 353–358.

[70] de Boer MP, Clews PJ, Smith BK, Michalske TA. Adhesion of polysilicon microbeams in controlled humidity ambients. Materials Research Society Symposium – Proceedings 1998; 518: 131–136.

[71] Tanner DM, Walraven JA, Irwin LW, Dugger MT, Smith NF, Eaton WP, Miller WM, Miller SL. The effect of humidity on the reliability of a surface micromachined microengine. Proc. of IEEE International Reliability Physics Symposium 1999: 189–197

[72] Phinney LM, Klody KA, Sackos JT, Walraven JA, Repair of stiction-failed, surface-micromachined polycrystalline silicon cantilevers using pulsed lasers. Proceedings of SPIE 2000; 4174: 279–287.

[73] Edmonds LD, Swift GM, Lee CI. Radiation response of a MEMS accelerometer: An electrostatic force. IEEE Transactions on Nuclear Science 1995;45(6): 2779–2788.

[74] Knudson AR, Buchner S, McDonald P, Stapor WJ, Campbell AB, Grabowski KS, *et al.,* The effects of radiation on MEMS accelerometers. IEEE Transactions on Nuclear Science1996; 43(6): 3122–3126.

[75] van Spengen WM. MEMS reliability from a failure mechanisms perspective. Microelectronics Reliability 2003; 43: 1049–1060.

[76] Kolpekwar A, Jiang T, Blanton RDS. CARAMEL: contamination and reliability analysis of micro-electromechanical layout. Journal of Micro-electromechanical Systems 1999;8(3):309–318.

[77] Sellars AG, Farish O, Hampton BF. Assessing the risk of failure due to particle contamination of GIS using the UHF technique. IEEE Transactions on Dielectrics and Electrical Insulation 1994; 1(2): 323–331.

[78] Jiang T, Blanton RDS. Particulate failures for surface-micromachined MEMS. IEEE International Test Conference (TC) 1999; 329–337.

[79] Schjolberg-Henriksen K, Jensen GU, Hanneborg A, Jakobsen H. Sodium contamination in integrated MEMS packaged by anodic bonding. Proceedings of the IEEE Micro Electro Mechanical Systems (MEMS) 2003;626–629.

[80] Willis B. Secondary reflow failure-another lead contamination defect. Global SMT and Packaging 2003;4(1): 4–5.

[81] Zhu Y, Espinosa HD. Reliability of capacitive RF MEMS switches at high and low temperatures. International Journal of RF and Microwave Computer-Aided Engineering 2004; 14(4):317–328.

[82] Jennings JM, Phinney LM. The effects of temperature on surface adhesion in MEMS Structures. Proceedings of SPIE 2000; 4180:66–75.

[83] Lian K, Jiang JC, Ling ZG, Meletis EI. Temperature effects on microstructural evolution and resulting surface mechanical properties of Ni-based MEMS structures. Proceedings of SPIE 2003; 4980: 192–199.

[84] Duvvury C, Amerasekera A. ESD: A pervasive rreliability concern for IC technologies. IEEE Proceedings. 1993; 8: 690–702.

[85] Lee JC, Hoque A, Croft GD, Liou JJ, Young R, Bernier JC. An electrostatic discharge failure mechanism in semiconductor devices, with applications to electrostatic discharge measurements using transmission line pulsing technique. Solid-State Electronics 2000;44: 1771–1781

[86] Wairaven JA, Soden JM, Tanner DM, Tangyunyong P, Cole EI Jr., Anderson RE, *et al.,* Electrostatic discharge/electrical overstress susceptibility in MEMS: A new failure mode. Proceedings of SPIE 2000; 4180: 30–39.

[87] Walraven JA, Weiss J, Baker MS, Plass RA, Shaw MJ, Aldridge C. Failure analysis of electrothermal actuators subjected to electrical overstress (EOS)

and electrostatic discharge (ESD). Proceedings of the 30th International Symposium for Testing and Failure Analysis, Worcester, MA; 2004: 225–231.

[88] Yeh ECC, Choi WJ, Tu KN, Elenius P, Balkan H. Current-crowding-induced electromigration failure in flip chip solder joints. Applied Physics Letters 2002; 80(4): 580–582.

[89] Ogurtani TO, Oren EE. Electromigration-induced void grain-boundary interactions: The mean time to failure for copper interconnects with bamboo and near-bamboo structures. Journal of Applied Physics 2004; 96(12): 7246–7253.

[90] Lin YH, Tsai CM, Hu YC, Lin YL, Kao CR. Electromigration-induced failure in flip-chip solder joints. Journal of Electronic Materials 2005; 34(1): 27–33.

[91] Nah JW, Suh JO, Tu KN. Effect of current crowding and joule heating on electromigration-induced failure in flip chip composite solder joints tested at room temperature. Journal of Applied Physics 2005;98: 13715.

[92] Padhia D, Dixit G. Effect of electron flow direction on model parameters of electro-migration-induced failure of copper interconnects. Journal of Applied Physics 2003; 94(10): 6463–6467.

[93] Waliash A, Levit L. Electrical breakdown and ESD phenomena for devices with nanometer-to-micron gaps. Proceedings of SPIE 2003; 4980: 87–96.

[94] Vorobev GA, Ekhanin SG, Nesmelov NS. Electrical breakdown in solid dielectrics. Physics of the Solid State 2005; 47(6): 1083–1087.

[95] Edward GP. Preventing EMP/EMI sheilding failure in cables resulting from backshell adapter coupling separations. Annual Connectors and Interconnection Technology Symposium Proceedings, San Diego, CA; 1991:445–453.

[96] Shoup RW, Hanson RJ, Durgin DL. Evaluation of EMP failure models for discrete semiconductor devices. IEEE Transactions on Nuclear Science NS-1981; 28(6): 4328–4333.

[97] Rabinovitch A, Frid V, Bahat D. Note on the Amplitude-frequency relation of electromagnetic radiation pulses induced by material failure. Philosophical Magazine Letters 1999;79(4):195–200.

[98] Gooch R, Schimert T. Low-cost wafer level vacuum packaging for MEMS. MRS Bulletin 2003; 28(1): 55–59.

[99] Chavan AV, Wise DW. Batch-processed vacuum-sealed capacitive pressure sensors. Journal of Microelectromechanical Systems 2001;10(4): 580–588.

[100] Kobayashi S, Hara T, Oguchi T, Asaji Y, Yaji K, Ohwada K. Double-frame silicon gyroscope packaged under low pressure by wafer bonding. Transducers Sendai, Japan; 1999; 910–913.

[101] Esashi M, Ura N, Matsumoto Y. Anodic bonding for integrated capacitive sensors. Proceedings MicroelectroMech Systems 1992; 92:43–48.

[102] Sung-Hoon Choa. Reliability of MEMS packaging: Vacuum maintenance and packaging induced stress. Microsystem Technology 2005; 11: 1187–1196.

[103] Li G, Tseng A. Low stress packaging of a micromachined accelerometer. IEEE Transactions on Electronics Packaging Manufacturing 2001; 24(1): 18–25.

[104] Lin L. MEMS Post-packaging by localized heating and bonding. IEEE Transactions on Advanced Packaging 2000; 23: 608–616.

[105] Mahajan R, Pecht M. Reliability assessment of a plastic encapsulated RF switching device. Microelectronics Reliability 1997; 38:1607–1610.

[106] Tambe NS, Bhushan B. A new atomic force microscopy based technique for studying nanoscale friction at high sliding velocities. Journal of Physics D: Applied Physics 2005;38: 764–773.

[107] von Känel H, Meyer T. Nano-scale defect analysis by BEEM. Journal of Crystal Growth 2000;210: 401–407.

[108] Liang YC, Lin WZ, Lee HP, Lim SP, Lee KH, Feng DP. A neural-network-based method of model reduction for the dynamic simulation of MEMS. Journal of Micromechanics and Microengineering 2001;11: 226–233.

[109] Li YM, Yu SM. A Unified quantum correction model for nanoscale single-and double-gate MOSFETs under inversion conditions. Nano-technology 2004;15:1009–1016.

59

Amorphous Hydrogenated Carbon Nanofilm

Dechun Ba and Zeng Lin

Northeastern University, Shenyang, P.R. China

Abstract: Amorphous hydrogenated carbon (a-C:H) nanofilm is a metastable form of amorphous carbon with significant sp3 bonding. a-C:H is a semiconductor with a high mechanical hardness, chemical inertness, and optical transparency. This chapter will describe the deposition methods, deposition mechanisms, characterization methods, electronic structure, gap states, defects, doping, luminescence, field emission, mechanical properties, and some applications of a-C:H. The films have widespread applications as protective coatings in areas such as magnetic storage disks, optical windows, and micro-electromechanical devices (MEMs).

59.1 Introduction

Amorphous hydrogenated carbon (a-C:H) nanofilm is a metastable form of amorphous carbon containing a significant fraction of sp^3 bonds. It can have a high hardness, wearability, thermal conductivity, chemical inertness, optical transparency, and a low friction coefficient, and it is a wide band gap semiconductor. A-C:H films have widespread applications as protective coatings in areas such as car parts, biomedical coatings, and micro-electromechanical devices (MEMS), and have practical applications in optical windows and magnetic disks [1].

There have been great developments in the field of disordered carbons. New ways have been developed to synthesize a-C:H nanofilms, while a range of disordered carbons with local fullerene-like order on a nanometer length scale have been discovered. a-C:H nanofilms have now been characterized in great detail. The ways to grow the most diamond-like nanofilms are now understood. Their growth mechanism is broadly understood in terms of the subplantation of incident ions.

A-C:H nanofilm has some extreme properties similar to diamonds, such as hardness, elastic modulus, and chemical inertness; however, these are achieved in an isotropic disordered thin film with no grain boundaries. It is much cheaper to produce than diamond itself. This has great advantages for many applications.

It is convenient to display the compositions of the various forms of amorphous C-H alloys on a ternary phase diagram as in Figure 59.1 [1],[2]. A range of deposition methods, such as plasma enhanced chemical vapor deposition (PECVD), is able to reach into the interior of the triangle. This produces a-C:H nanofilm. Although it is diamond-like, as is seen from Figure 59.1 the content of sp^3 bonding is actually not so large, and its hydrogen content is rather large. Thus, a more sp^3 bonded material with less hydrogen, which can be

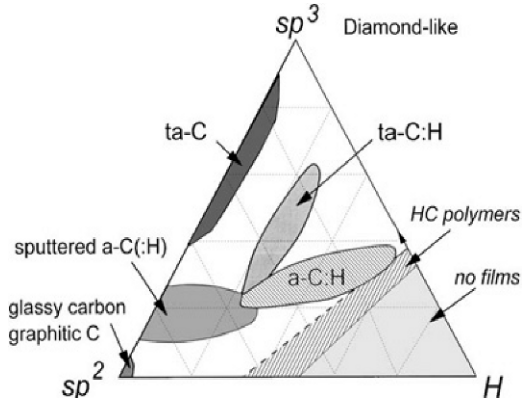


Figure 59.1. Ternary phase diagram of bonding in amorphous carbon-hydrogen alloys

produced by high plasma density PECVD reactors, is called hydrogenated tetrahedral amorphous carbon (ta-C:H) [3].

59.2 Deposition Methods

59.2.1 Ion Beams

The first a-C:H nanofilms were prepared as thin films using ion beam deposition [4]. It is possible to produce a-C:H nanofilms by a wide range of deposition methods. The methods can be categorized according to whether they are most suitable for laboratory studies or industrial production. The common feature of these methods is that the a-C:H nanofilm is condensed from a beam containing medium energy (~100 eV) carbon or hydrocarbon ions. It is the impact of these ions on the growing film that induces the sp^3 bonding. The best deposition process for a-C:H nanofilms will provide a carbon ion flux at about 100 eV *per* carbon atom., with a narrow energy distribution, a single energetic species, and a minimum number of non-energetic (generally neutral) species [3].

In a typical ion beam deposition system, carbon ions are produced by the plasma sputtering of a graphite cathode in an ion source. Alternatively, as in the Kaufman source, a hydrocarbon gas such as methane is ionized in a plasma [5],[6]. An ion beam is then extracted through a grid from the plasma source by a bias voltage. The carbon ions or hydrocarbon ions are then accelerated to form the ion beam in the high vacuum deposition chamber. In both cases, the ion source runs at a finite pressure, so that the beam also contains a large flux of unionized neutral species. This can reduce the flux ratio of ions to neutrals to as low as 2–10%. Ion beam sources tend to run best at higher ion energies of 100–1000 eV.

A variant of ion beam deposition is the cascade arc source [7]. Here, a high-pressure source produces intense plasma, which then expands supersonically into a high vacuum, giving rise to large fluxes of ions and radicals.

59.2.2 Sputtering

The most common industrial process for the deposition of carbon nanofilm is sputtering. The most common form uses the dc or rf sputtering of a graphite electrode by an Ar plasma. Because of the low sputter yield of graphite, magnetron sputtering is often used to increase the deposition rate. Magnets are placed behind the target to cause the electrons to spiral and increase their path length, and thus to increase the degree of ionization of the plasma. As ion bombardment helps the formation of sp^3 bonding, the magnetic field can be configured to pass across to the substrate, which causes the Ar ions to also bombard the substrate, to give an “unbalanced magnetron”. A dc bias can be applied to the substrate to vary the ion energy. A-C:H nanofilm can be produced by reactive sputtering, by using a plasma of Ar and hydrogen or methane, and a-CNx can be produced using an argon-nitrogen plasma.

Alternatively, in ion beam sputtering, a beam of Ar ions can be used to sputter from the graphite target to create the carbon flux. A second Ar ion beam can be used to bombard the growing film, to densify the film or encourage sp^3 bonding. This is called ion beam assisted deposition (IBAD) or ion plating.

Sputtering is preferred in industrial applications because of its versatility, its widespread use to sputter many materials, and its ease of scale up. Also, the deposition conditions can be controlled by the plasma power and gas pressure but they are

reasonably independent of the substrate geometry or condition. A disadvantage of sputtering is, like ion beam deposition, that it can have a relatively low ratio of energetic ions to neutral species, so that it does not produce the hardest DLC films. However, sputtering methods with a very high fraction of ions have been developed by Schwan *et al*. [8] and Cuomo *et al*. [9] to produce a-C with a relatively large sp^3 fraction, but this is at the expense of a low growth rate.

59.2.3 PECVD

The most popular laboratory deposition method is RFPECVD (radio frequency plasma enhanced chemical vapor deposition) [10]–[19]. The reactor consists of two electrodes of different areas. The rf power is usually capacitively coupled to the smaller electrodes on which the substrate is mounted, and the other electrode (often including the reactor walls) is earthed. The rf power produces a plasma between the electrodes. The higher mobility of electrons compared to the ions in the plasma creates a sheath next to the electrodes with an excess of ions. This has a positive space charge, so the plasma develops a positive voltage with respect to the electrodes, which equalizes the mean electron and ion current to the wall [1], as shown in Figure 59.2.

The sheaths act as diodes, so that the electrodes acquire dc self-bias voltage equal to their peak rf voltage. The rf voltage is divided between the sheaths of the two electrodes as in a capacitive divider, according to their inverse capacitance. Thus, the dc self bias voltage varies inversely with the electrodes areas [1],

$$\frac{V_1}{V_2} = \left(\frac{A_2}{A_1}\right)^2 \tag{59.1}$$

The smaller electrode with smaller capacitance acquires the larger bias voltage and becomes negative with respect to the larger electrode. This makes the substrate electrode. The negative sheath voltage accelerates the positive ions to give the bombardment needed to create the sp^3 bonding.

The gas used in PECVD has a significant effect on the a-C:H properties. In the early days, precursors with low ionization potentials such as benzene were chosen, as this gave a much higher growth rate. The deposition rate increases roughly exponentially with decreasing ionization energy as shown in Figure 59.3. For mechanical applications, it is desirable to maximize the hardness, which we shall see means minimizing the incorporation of hydrogen. This requires using a precursor with small H/C ratio such as acetylene, as this strongly affects the H/C ratio of the resulting film.

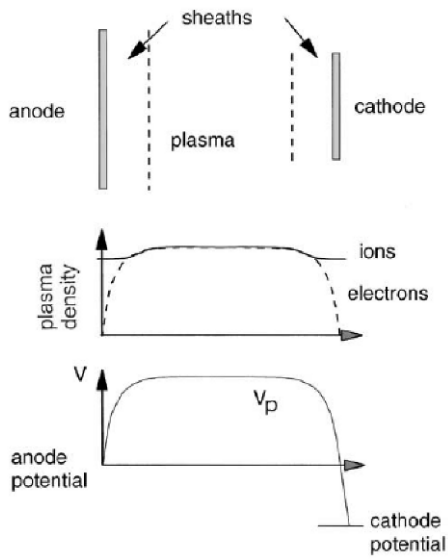


Figure 59.2. Electron and ion distributions that create sheaths between the neutral plasma and the walls

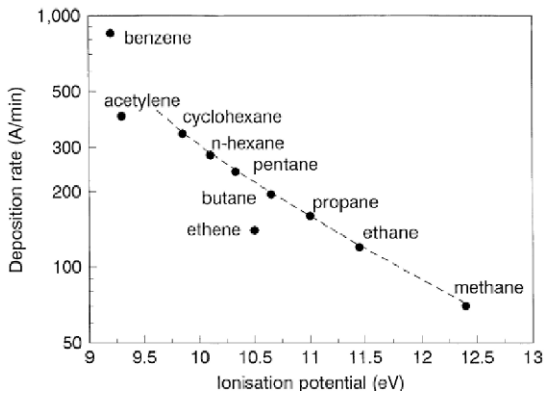


Figure 59.3. Growth rate of a-C:H by PECVD *vs.* ionization potential of the precursor gas

It is now known that a-C:H properties depend on the ion energy *per* C atom. Thus, a benzene ion $C_6H_n^+$ with six carbons requires high bias voltages to reach the desired 100 V *per* atom. Acetylene is more acceptable because 200 V is easier to handle. Acetylene is in fact a very useful source gas for low pressure deposition, because its strong C≡C bond means it has a simple dissociation pattern, giving mainly $C_2H_n^+$ ions [3]. There is also less plasma polymerization than as occurs with methane. Acetylene is the preferred source gas for mechanical applications. However, acetylene is unsatisfactory for electronic applications because it is not available in a high purity form and possesses a substantial nitrogen impurity [20], which can cause a doping effect particularly if used in high-density plasmas. Methane remains a popular choice for electronic applications because it is available in high purity.

59.3 Deposition Mechanism of a-C:H

The key property of a-C:H nanofilm is its sp^3 bonding. The deposition process that promotes sp^3 bonding is a physical process, ion bombardment. The highest sp^3 fractions are formed by C+ ions with ion energy around 100 eV.

There are many processes in the deposition of a-C:H, as shown in Figure 59.4. The strong dependence of the properties of plasma deposited a-C:H on the bias voltage and hence on the ion energy indicates that ions play a critical role in the deposition of a-C:H. The ion flux fraction is much less than 100% and may be typically 10%. The a-C:H can be deposited from different source gases such as CH_4, C_2H_2, C_2H_4, and C_6H_6. The variation of the film density with bias voltage for each source gas can be redrawn on a scale of bias voltage *per* C atom in the molecule. When this is done, the maxima in density lie at a similar energy. This indicates that the action of ions is still *via* subplantation. This can be understood as follows. An energetic molecular ion incident at the film surface will break up into atomic ions and the energy will be distributed evenly. Thus, each atomic ion will subplant independently with that energy.

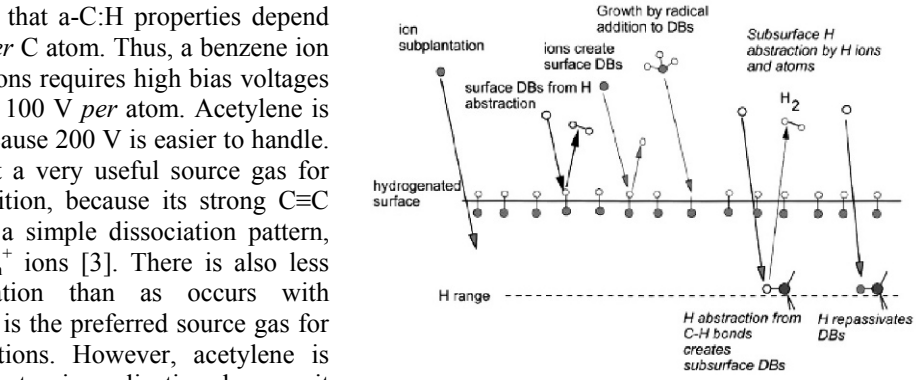


Figure 59.4. Component processes in the growth mechanism of a-C:H

A complete model of the growth of a-C:H requires us to also describe the chemical processes of neutral species and of dehydrogenation [21]−[29], as well as the physical process of subplantation. There are three general stages of the plasma deposition; the reactions in the plasma (dissociation, ionization, *etc*.), the plasma-surface interaction and the subsurface reactions in the film. The plasma reactions are driven by the energetic electrons, as defined by the electron energy distribution (EED). There will be other species formed in secondary reactions such as polymerization. These tend to be less important at the lower pressures used for a-C:H deposition. Except in the case of high-density plasmas, the mass spectrometer analyses show that undissociated source gas molecules are still the dominant species in the plasma.

The plasma species incident on the growing film will consist of ions and neutrals. The neutrals will be closed shell molecules such as undissociated precursor gas, monoradicals such as CH_3, di-radicals, and other unsaturated species such as C_2H_4 or C_2H_2. The plasma also contains significant amounts of atomic hydrogen.

It is known that neutral species contribute to growth because the mass deposition rate exceeds the rate due to ions alone. The first effect of note is that the growth rate decreases with increasing temperature. This was first thought to be because the neutrals were weakly adsorbed on the surface, which would desorb at higher temperatures. It is now known that this temperature dependence is

due to the etching of the film by atomic hydrogen [23]−[25]. Growth itself is independent of temperature. The etching rate increases with temperature, so the net growth rate decreases with temperature.

The contribution of each neutral species to the growth rate depends on their sticking coefficient. The a-C:H surface is essentially fully covered with C-H bonds, so it is chemically passive. Di-radicals and other unsaturated species can insert directly into surface C-C or C-H bonds, so these species react strongly with the film and their sticking coefficients approach 1. On the other hand, closed shell neutrals like CH_4 have very low sticking coefficients of under 10^{-4} and their effect is negligible. The monoradicals have a moderate effect. They cannot insert directly into a bond, they can only react with the film if there is an existing dangling bond on the surface. They will add to this bond to form a C–C bond. The dangling bond must be created by removal of an H from a surface C–H bond. This can occur by an ion displacing an H from the bond, or by an H atom abstracting H from the bond,

$$\equiv C - + H^{'} \rightarrow \equiv C^{'} - + H_2 \qquad (59.2)$$

or by another radical like CH_3 abstracting H from the C–H bond. Measurements have found that atomic H′ is the most efficient species for abstraction (30 times faster than CH_3) [28]. CH_3 then adds to this dangling bond. Thus, the effective sticking coefficient of CH_3 is small, but it is high in the presence of atomic hydrogen [27],[28]. This leads to a synergistic effect of H′ on the sticking probability of CH_3 [28].

Neutral hydrocarbon species can only react at the surface, they cannot penetrate the film. Hydrogen atom and ions are different. H atoms being so small, they can penetrate about 2 nm into the film. There, they can again abstract H from C–H bonds and create subsurface dangling bonds and H_2 molecules. Some of these dangling bonds will be re-saturated by incoming atomic H [1].

Ions can also penetrate the film. Carbon and hydrocarbon ions can cause subplantation. A more typical role of ions in a-C:H is to displace H from C-H bonds. This H can then recombines with other H′ to form H_2 molecules, and desorbs from the film. This is the main process, which causes the H content of PECVD a-C:H to decrease with increasing bias voltage. Some of the atomic H′ does not recombine, but finds dangling bonds to re-saturate.

Because of their low mass, hydrogen ions interact weakly with C atoms. Thus, H+ ions have the longest range and penetrate deepest into the film. They undergo the same reactions as atomic H′, but to a greater depth. Thus, it was noted that a-C:H films have three characteristic depths; the surface itself is controlled by reactions of hydrocarbon and hydrogen species; the upper 2 nm in which chemistry is controlled by reactions of atomic H`, and a larger depth depending on ion energy in which reactions are controlled by H^+ ions [1].

59.4 Bulk Properties of a-C:H

The properties of a-C:H have been studied by many researchers [15],[16],[30]–[67]. Figure 59.5 shows the variation of the main properties, the sp^3 fraction, hydrogen content, mass density, and optical gap with the bias voltage V_b for a-C:H films deposited from different source gases: methane, acetylene and benzene [15],[34], and [45]. Most properties of a-C:H depend on the incident ion energy *per* C atom. For conventional PECVD, the incident ion energy is about 0.4 times the bias voltage V_b [13],[14].

The bonding configurations in a-C:H deposited from methane have been studied in detail by Tamor *et al*. [34] using NMR to derive the fractions of the various C:H configurations as a function of V_b. The result shows how the total sp^3 fraction and hydrogen content both decrease continuously with increasing V_b, and also how the hydrogen is preferentially bonded to the sp^3 sites.

The bonding and properties of a-C:H films fall into three regimes defined by the ion energy or bias voltage V_b used in deposition. The actual value of V_b for these regimes depends on the precursor gas and the deposition pressure. At low bias voltages, the films have a large hydrogen content, a large sp^3 content and a low density. The films are called polymeric a-C:H or soft a-C:H.

The optical gap is over 1.8 eV and it can even extend up to 3.5 or 4 eV [58]. This is a very wide gap. At intermediate bias voltages, the H content has fallen, the sp^3 content is less and the films have a maximum in density. In this regime, the amount of C–C sp^3 bonding reaches its maximum and the films have their highest diamond-like character. The optical gap lies in the range 1.2–1.7 eV. At high bias voltages, the H content has fallen further and the bonding has become increasingly sp^2-like. The Raman spectra now possess a D peak, and this shows that some sp^2 sites are aromatic [40]. The films can be called graphitic.

The bonding in a-C:H can be described as follows. The C sp^3 sites form a continuous network of C−C bonds. Most sp^3 sites are bonded to one or more hydrogens. A large part of the sp^3 bonding in a-C:H is due to the saturation of bonding by hydrogen. The sp^2 sites in a-C:H form small clusters in this matrix. The cluster sizes or sp^2 site distortions increase with increasing V_b, which causes the band gap to decrease. In soft a-C:H, the clusters tend to be olefinic and do not give a Raman D peak [38]. In a-C:H deposited at high bias, the sp^2 clusters become larger and increasingly aromatic, and so give rise to the observed D peak. The dispersive Raman spectra confirm this. The G peak position saturates at 1600 cm^{-1} at high photon energies for high bias samples, while it continues above1 1600 cm^{-1} for polymeric a-C:H.

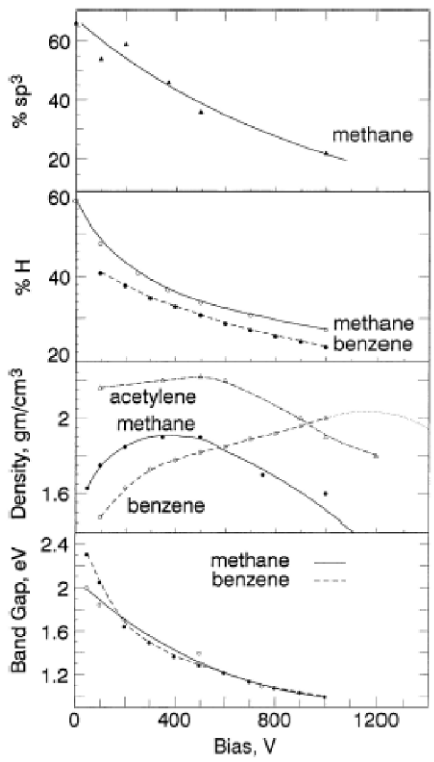


Figure 59.5. Variation of sp^3 fraction, hydrogen content, density, and optical gap with deposition bias voltage

The properties of a-C:H depend on the ion energy *per* C atom, E. Often the depositing species is a molecular ion $C_mH_n^+$. When the molecular ion hits the film surface, it breaks up and shares their kinetic energy between the individual daughter carbon atoms. The effective energy *per* C atom is then

$$E = \frac{E_i}{m}. \tag{59.3}$$

This means that the properties of a-C:H will depend on the precursor molecule, when scaled according to this reduced ion energy *per* C atom. Thus the maximum in density for a-C:H prepared from acetylene will occur at about twice the bias voltage of that from methane, and that from benzene at about six times it. The hydrogen content of the a-C:H film is always slightly lower than that of the precursor molecules. Hydrogen is lost during growth by chemical sputtering-the displacement of H from C-H bonds by incoming ions. This process is roughly proportional to the molecular ion energy. The H content of a-C:H prepared from methane is larger than that prepared from other precursors, largely because the H/C ratio of methane is so large.

59.5 Electronic Applications

In silicon complementary metal-oxide-semiconductor (CMOS) device technology, the device dimensions are continually shrinking, in a process known as Moore's Law. At present, the insulator used between data lines is silicon dioxide. However, RD associated with the capacitance of these lines is becoming too significant. It is necessary to replace SiO_2 with an insulator with a

lower dielectric constant (k) to reduce this capacitance. The (low frequency) k of SiO_2 is 3.9. Various carbon-based films are candidate dielectrics [68][69]. These materials must satisfy other criteria as well as low k. They must be thermally stable to 400°C, have adequate rigidity, low mechanical stress, low dissipation, low leakage, good adhesion, and be processable using acceptable means. The industry first used fluorinated SiO_2 but there is a lower limit to its k. Various carbon-based materials have been tried, such as a-C:H, fluorinated amorphous carbon (a-C:F). The aim is to find materials to reach k values of 1.5–2.1.

There are two components to k, the electronic part and the lattice part. The lattice part is minimized by avoiding ionic bonds. The electronic part is minimized by using low atom densities and strong, less polarizable bonds. A-C:H can reach k values down to 2.6 by deposition at low bias voltages and higher pressures. The main problem with these polymeric a-C:H is that they have low thermal stability and evolve hydrogen and hydrocarbons at below 400°C. The k of a-C:H follows the same trend as the loss of thermal stability, and only films with k above 3.3 are sufficiently stable [69].

59.6 Mechanical and Other Properties

The mechanical properties of a-C:H nanofilms are of great importance because of the use of a-C:H as a protective coating[70]−[77]. A great advantage of a-C:H compared to CVD polycrystalline diamond is that it is amorphous with no grain boundaries. This means the films are extremely smooth. A-C:H is also deposited at room temperature, which is an advantage for temperature sensitive substrate such as plastic. A-C:H nanofilms also have extremely good coverage, so they act as good corrosion barrier. This is particularly useful in a major application, which is to coat disks and recording heads in the magnetic storage technology [75]–[77]. The disadvantages of a-C:H nanofilms are their intrinsic stress and thermal stability. These problems are now being circumvented.

59.6.1 Elastic Properties

Many of the mechanical properties of a-C:H nanofilms are measured by a nanoindenter [78],[79]. In this experiment, a small diamond tip is progressively forced into the film, and the force–displacement curve is measured. Figure 59.6, shows a typical curve for a-C:H. The curve is also measured for the unloaded cycle. The hardness is defined as the pressure under the tip, given by the ratio of force to the projected area of plastic deformation. It is well known that for accuracy, the indentation depth must be limited to a fraction of order 10% of the total film thickness. This is particularly important for the case of hard on soft films, such as a-C:H. The hardness is found with reasonable accuracy by this procedure.

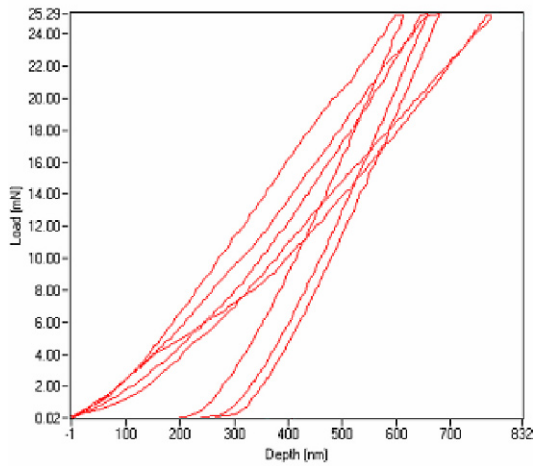


Figure 59.6. Load-unloading curve for a nano-indentation measurement of a-C:H

59.6.2 Hardness

The hardness is a measure of the yield stress of a material. Figure 59.7 shows the hardness of a-C:H deposited by PECVD from methane and benzene precursors. The hardness is low at low bias voltage, for the polymeric a-C:H films [1]. The hardness then rises to a maximum corresponding to the maximum diamond-like character, and then it decreases as the films acquire a more graphitic bonding. The hardness reaches a maximum at low

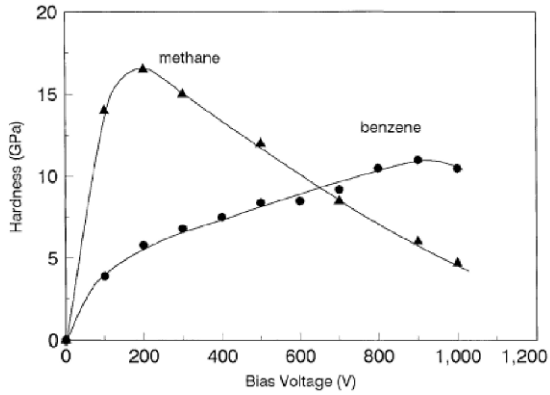


Figure 59.7. Variation of nanohardness of a-C:H with deposition bias voltage

bias voltages for methane a-C:H, while the hardness for the benzene-derived film reaches a maximum around 1000 V.

Note that the maximum nanohardness of the a-C:H in Figure 59.5 is 17 GPa. The importance of using a nanoindenter and small indent depth is well known. If conventional microindenters are used on a-C:H, these give hardness values of typically three times higher than the nanoindenter. Thus, hardness values for a-C:H nanofilms over 20 GPa should be viewed as exaggeration unless there is some reason in terms of improved bonding or low hydrogen content to account for them.

59.6.3 Adhesion

The major use of a-C:H is for protective coatings. Thick films are preferred for this, to maximize the wear life. The compressive stress limits the maximum thickness of adhesive films. A film of thickness h will delaminate when the elastic energy *per* unit volume due to the stress σ exceeds the surface fracture energy γ *per* surface, so for adhesion

$$2\gamma > \frac{\sigma^2 h}{2E}, \tag{59.4}$$

or

$$h < \frac{4\gamma E}{\sigma^2}. \tag{59.5}$$

This sets an upper limit of film thickness. Now, it is known that the stress, Young's modulus and hardness all tend to be proportional to each other. Maximizing the hardness means that the stress is a maximum. Thus, maximizing the hardness will minimize the thickness of an adherent layer, so that little is gained.

Various strategies are used to maximize the film thickness. First, it is essential to ensure there is good adhesion between the film and the substrate. The film should fail by fracture within the substrate. This can be achieved by cleaning the surface by Ar ion bombardment before deposition. Another method is to use a high ion energy for the first stage of deposition, to cause ion beam mixing between film and substrate in order to ensure a mixed interface.

Second, a carbide-forming adhesion layer such as Si, Cr or W can be deposited first before the carbon [70]–[80]. Silicon works well for glass substrates used in sunglasses and bar-code scanners, on which a wider gap a-C:H may not adhere. Films can be made that are inhomogeneous or graded, so that they have internal stress relief mechanisms.

Third, it is possible to use multi-layers to provide internal stress relief. This has been used by Lin Zeng [81] *et al*., for a-C:H films and by Meneve *et al.* [82] for a-CSi_x:H.

A major effort has been made to reduce stress by alloying with, for example, Si[83] or metals[84]. Si has three beneficial effects. It can promote sp^3 bonding by chemical means, as it does not exert sp^2 hybridization, so it is not necessary to use as much ion bombardment to get sp^3 bonding. It increases the thermal stability of the hydrogen. It also improves the friction performance, as discussed shortly, by maintaining a low friction to higher humidity.

59.6.4 Friction

A-C:H nanofilms are notable for their low friction coefficients[70],[71],[85]–[95]. It has been found that a-C:H in a vacuum can have a friction coefficient μ as low as 0.01 [94]. For a-C:H, μ depends strongly on the relative humidity. Values of μ below 0.05 are found in a vacuum and at low humidity and μ increases strongly at high humidity. It is found that the friction coefficient in

low humidity regime depends on the precursor used to make the a-C:H [94]. It varies with the ratio of H/C in the precursor, with a-C:H from CH_4 having the lowest μ and a-C:H from C_2H_2 having the largest μ. The a-C:H prepared from hydrogen-diluted methane has the lowest friction coefficient. μ increases to 0.1–0.15 when the humidity rises to normal atmospheric values of 30% and above. *In situ* studies have shown that the higher μ arises from the water, not oxygen, in the atmosphere.

59.6.5 Wear

It is found a-C:H has a low wear rate of order 10^{-7} mm^3N^{-1} [96]. The wear mechanism of a-C:H is the friction mechanism, adhesive wear *via* transfer layer. The sp^3 bonding transforms by stress-induced transformation to a graphite overlayer, which acts as a lubricant, and then a-C:H forms a C:H transfer on the counter surface [90].

59.6.6 Surface Properties

A-C:H is also notable for its small surface energy [84]. The surface energy is usually measured using the contact angle. Low surface energies give large contact angles. Surface energies are typically 40-44 mNm^{-1}. a-C:H generally has a contact angle with water of 55–70°. Unusually, this is found to be independent of deposition bias voltage [97],[98].

Dimigen and coworkers [98] tested the effects of alloying elements on the surface energy of a-C:H. They found the surface energy of a-C:H increased from 41 mNm^{-1} for pure a-C:H to 52 mNm^{-1} with oxygen addition, but decreased to 19–24 mNm^{-1} with the addition of Si or F.

59.6.7 Biocompatible Coatings

There is considerable interest in using various forms of a-C:H as biocompatible coatings, on parts such as replacement hip joints, heart valves, and so on [99]–[102]. This arises from the low friction coefficient of a-C:H and the belief that a carbon material must be biologically compatible. In many coatings, the main requirement is that a-C:H has good adhesion to the underlying unit and does not produce metallic wear debris. Deeper investigations have studied the attachment of blood cells, proteins, *etc*.

59.6.8 Coatings of Magnetic Hard Disks

One of the most important uses of a-C:H nanofilms is as protective coating on magnetic storage disks [75]–[77]. A-C:H is used because it makes extremely smooth, continuous, and chemically inert films, with a surface roughness below 1 nm. A-C:H nanofilms have no competitors as a coating material for this application.

The first role of a-C:H film was to provide protection against corrosion. Simple a-C was used, deposited by magnetron sputtering. Later, a-C:H was used, produced by the reactive sputtering in an Ar/hydrogen atmosphere. Its role was to provide also protection against mechanical wear and damage during head crashes. The best performing a-C:H contained more hydrogen than needed to maximize its hardness. This indicated that the role is not simple protection against dry wear, but that the interaction with the lubricant is critical. The surface termination of a-C:H immediately after deposition is important for its surface properties and the interaction with the lubricant.

59.6.9 Surface Property Modification of Steel

A-C:H films have practical applications in optical windows and magnetic disks [103],[104]. In this respect, the process of a-C:H film deposition on steel substrate has actual and potential importance in that it can be applied further to drills, gears, bearings, moulds/dies, punches, and medical devices. Thus, a systematic study on the process applied to depositing a-C:H film on steel substrates is indispensable, along with relevant mechanical properties and frictional characteristics involved.

When depositing a-C:H film on steel substrate, an interdiffusion effect of carbon atoms takes place on the interface to adversely affect the film adhesion strength because of the reaction in contact with Fe. On investigation it was found that introducing a transition interlayer between a-C:H film and substrate is an effective way to prevent

the interdiffusion so as to increase adhesion strength, and many kinds of interlayers have all been proved feasible, such as Si, Al, Cr, Mo, Ti, TiN, TiC, CrN, Si_3N_4 and SiC layers [105],[106]. Lately, the composite interlayers with functional gradient predeposited on substrates, such as Ti/Ti_xC_y and Ti/TiN/TiCN/TiC films, have been developed to increase the film adhesion strength, especially to enhance the bearing capacity of the top layer (a-C:H film) [107]. The change in the gradient and hierarchical structure of the transition interlayer will optimize the distribution of internal stresses to allow the film to work under severe rubbing/scratching conditions.

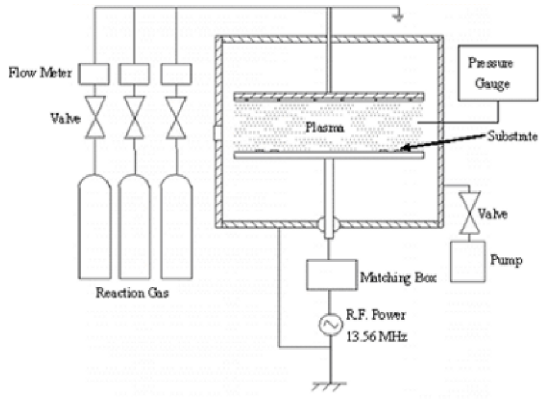


Figure 59.8. Schematic of RFPECVD setup for a-C:H film deposition

In the PECVD deposition process, a gas mixture of butane with argon was used to deposit a-C:H film on stainless steel substrate in an experimental setup as shown in Figure 59.8. The size of substrate was 10 mm *10mm *3 mm, and the surface had been polished. To improve the adhesion strength between the a-C:H film and substrate, an ion beam assisted deposition technique was used to predeposit Ti/TiN/TiC film with a functional gradient on the substrate, of which the thickness of the Ti, TiN, and TiC film was 100 nm, 100 nm, and 200 nm, respectively. Then, a-C:H film with a certain thickness was deposited on the transition interlayer by the rf PECVD process; the deposition parameters are shown in Table 59.1.

Table 59.1. Deposition parameters of a-C:H film on an underlayer film

Step No.	Operation	Condition
1	Prepumping	P～2Pa
2	Plasma cleaning	Ar U=1500V P～4Pa
3	Filling in reaction gas	Ar/C_4H_{10}
4	a-C:H grain growth	Ar/C_4H_{10} U=2000V-2800V
5	a-C:H film deposition	Ar/C_4H_{10} U=1000V

The properties of a-C:H films were measured or characterized at room temperature by various apparatus, such as Raman spectra by with Labram HR800 laser Raman spectrometer supplied by Jobin Yvon in France. The adhesion strength was tested by UMT-2M sliding tribometer supplied by CETR in the USA. The film surface morphology was observed using the Nanoscope III atomic force microscope (AFM) supplied by DI, USA. The tribological properties of a-C:H films were tested by the SurfTest SJ-201 ball-on-disc tribometer on which the diamond probe or hardened stainless steel ball may be taken as the counterpart. The testing was carried out in dry conditions at room temperature in such a way that a dry sliding motion was done repeatedly between the counterpart and the disk specimen. It was thus possible to measure the friction coefficient continuously *via* on-line monitoring, with different friction loads chosen as 1, 2, 5 and 10 N, and different rotating speeds as 30, 60, 120, 180, 240 and 300 rpm in testing. After the testing, the surface morphology in the worn area was observed by the SSX-500 SEM supplied by Shimatsu in Japan, and the structural change in the same area was analyzed by laser Raman spectroscopy, as well as the wear-out condition of steel balls taken as the counterpart.

In the test, we tried to polish the substrate thoroughly and changed the deposition parameters to a great extent, but the results showed that it was impossible to deposit directly a-C:H film on the

steel substrate bythe rf PECVD process. The films deposited in such conditions were presented in powder form and were rubbed off very easily. The cause was possibly that the carbon atoms had a strong diffusion effect on the steel substrate. For this reason, a predeposition technique was used in the experiment, *i.e.*, a Ti/TiN/TiC film with a functional gradient by which both the structure and composition of the film will change gradually, was predeposited on substrate as a transition interlayer of a-C:H film. The hardness and Young's modules of such a transition interlayer were 20 and 220 GPa, respectively. As a result, a-C:H films were successfully deposited on the stainless steel substrates. The adhesion strength of such a-C:H film was 6.0 N by the sliding test.

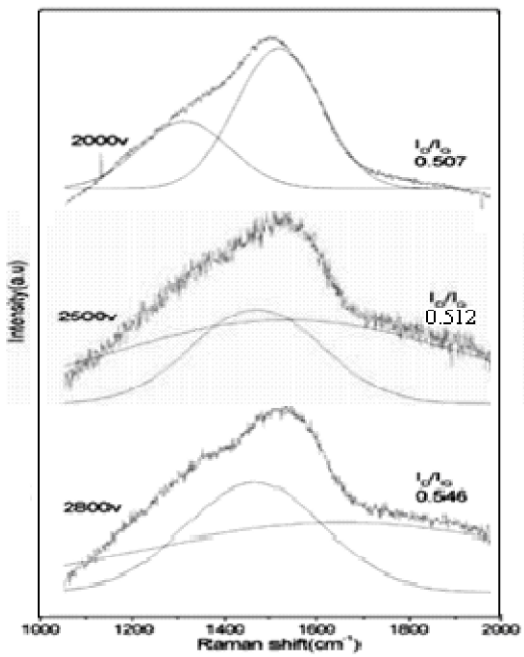


Figure 59.9. Raman spectra of a-C:H films deposited on stainless steel substrates with transition layers at different voltages

Figure 59.9 shows the laser Raman spectra of a-C:H film deposited on stainless steel substrates under different voltages. It can be seen that there is a broad peak with its center at about 1560 cm^{-1} along the abscissa.

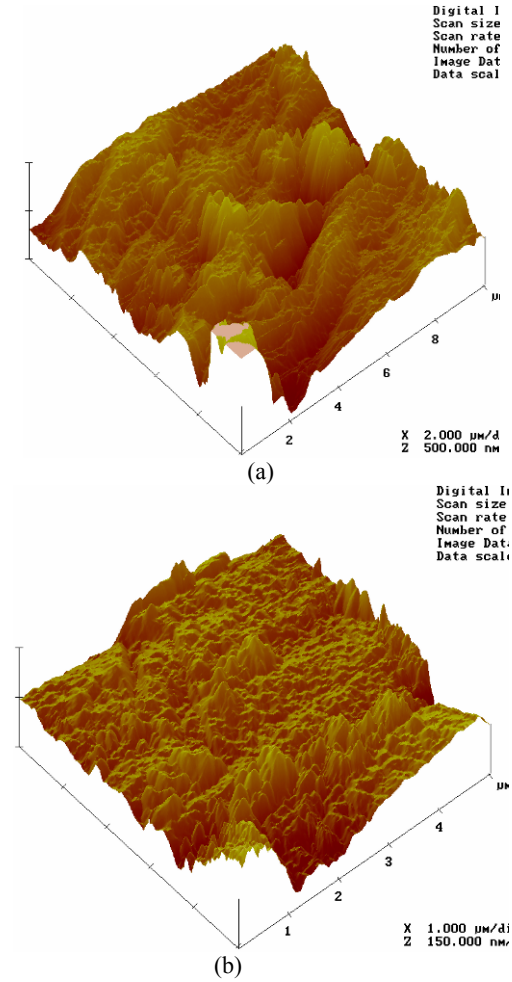


Figure 59.10. AFM images of the transition interlayer and a-C:H film: **(a)** surface of TiN transition interlayer, **(b)** surface of a-C:H film

This provides a typical Raman spectrum for a-C:H film, which can be decomposed into two Gaussian curves, *i.e.*, a G-peak with its center at 1580 cm^{-1} and a D-peak with its center at 1330 cm^{-1}. Comparing the three spectral lines with each other, we can see that the D-peak increases to 1430 cm^{-1} from 1315 cm^{-1} and the G-peak increases to 1735 cm^{-1} from 1520 cm^{-1}, accompanied with a voltage increase to 2800 V from 2000 V. In addition, the area ratio of D-peak to G-peak, I_D/I_G, increases with the increasing deposition voltage.

Figure 59.10 shows the difference between the transition interlayer and a-C:H film by means of an AFM image. Figure 59.10(a) shows the image of the transition interlayer, of which the scanned area is 10 μm*10 μm. As shown, the surface is rather rough mainly because in ion deposition process the sputtering action is so strong that a lot of pores and cracks formed there. Figure 59.10(b) shows the image of a a-C:H film deposited under 2500 V by the rf PECVD process, of which the scanned area is 5 μm*5 μm which means a double magnification in comparison with that shown in Figure 59.10(a). As shown, the surface of the ra-C:H film is comparatively flat, and the compactness of the film is improved as a whole except the area with one or two big island-like points.

Table 59.2. Tribological properties of stainless steel with different top layers

No.	Material	Friction coefficient	Wear rate (mm^3/Nm)
1	steel	0.9	7.67×10^{-6}
2	Steel/TiN	0.7	2.11×10^{-9}
4	Steel/TiN/a-C:H	0.5	1.03×10^{-10}

From the friction test, it was found that the friction coefficient of a-C:H film is relatively stable within 600 cycles, which shows the good quality of a-C:H film. Table 59.2 shows the tribological properties of stainless steel with different top layers. From the friction test, it was found that the hard layer TiN and a-C:H can both decrease the friction coefficient and wear rate, while a-C:H top layer has a better performance. In addition, from Table 59.2, it is clear that the a-C:H layer with TiN/TiC as the interlayer has the best tribological properties.

To reveal further the surface morphology of scratched areas, SEM was used to observe it on both film and ball surfaces, and the results are shown in Figure 59.11. In Figures 59.11(a) and (b) the SEM images of a-C:H film sample before and after wear-off, respectively, are shown. It can be seen that the sample surface before wear-off is smooth with even grain distribution, but cracks and scraps are found in scratched area after wear-off. This fact reveals that there is a strong plastic deformation of the film sample after the frictional sliding process [108]. The SEM images in Figures 59.11(c) and (d) are the ball as counterpart before and after wear-off, respectively, from which it can be seen that, similar to the film sample, cracks and scraps are found on surface after wear-off. This shows that there is also a plastic deformation of the ball after the frictional sliding process. According to the Hertz theory, the local contact stress between the two counterfaces can exceed the compressive strengths of both materials at some contact points [109]. Therefore, surface damage of both the film and the counterpart during the dry sliding test can be expected.

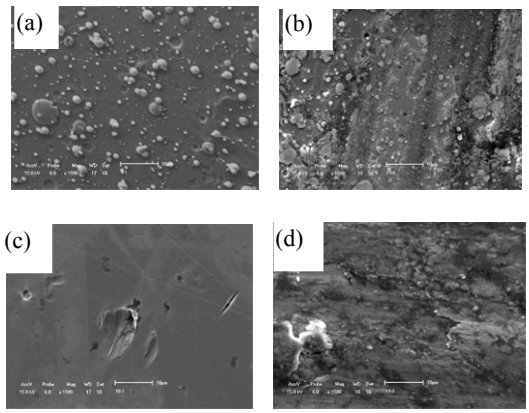


Figure 59.11. SEM images of the surface morphologies of a-C:H film and TiC ball coated with a-C:H before and after the wear-off testing: **(a)** Surface of a-C:H film before testing; **(b)** surface of wear track after the testing; **(c)** surface of the ball before testing; **(d)** surface of the ball after testing

On the other hand, from the Raman spectra of a-C:H film before and after wear-off in the dry sliding test, as shown in Figure 59.12, it can be seen that the Raman spectra of all wear tracks display a distinctly double peaked structure, with the D peak located at ~1400 cm^{-1} and the G peak at ~1580 cm^{-1}. The spectrum from the wear debris has a similar structure. Furthermore, the ratio of I_D/I_G has a much higher value compared to the data before the sliding test. Such a variation tendency in the Raman spectrum is similar to the case that a-C:H film is annealed at higher temperatures [110]. It was observed that upon annealing the trans-

formation of sp^3 bonded carbon to sp^2 bonded carbon occurred, and a more conspicuous D peak appeared simultaneously. Therefore, it is proposed that the sliding-induced heat accumulation on local contact areas between the two counterfaces can probably cause a gradual destabilization of the sp^3 C-H bonds, and thus promote the transformation of the sp3 bonded structure to the graphite-like sp^2 structure [111]. The tribological behavior of a-C:H film appears to be controlled by the graphite transfer layer formed by the thermal and strain effects during the sliding wear test, and a self-lubricating effect on sliding friction can be achieved [112]. The low friction and low wear rate of a-C:H film and the counterpart may be explained by the formation of this transfer layer with low shear strength.

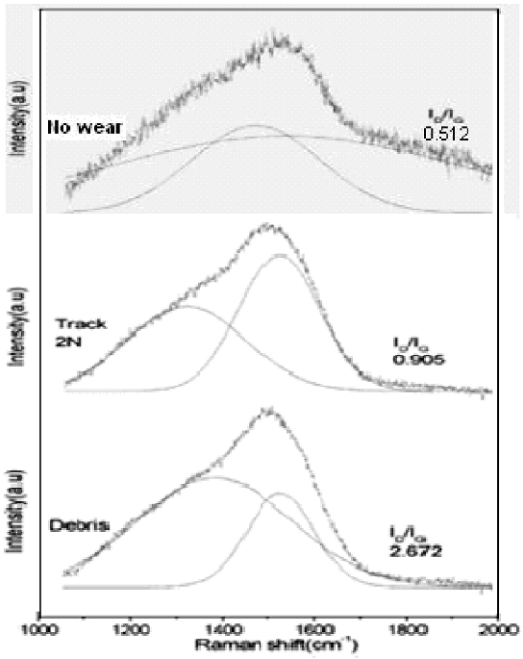


Figure: 59.12. Raman spectra of a-C:H film before and after wear-off

In summary, the rf PECVD process was used in a C_4H_{10}/Ar plasma atmosphere for a-C:H film deposition on stainless steel substrate. The adhesion strength between the film and substrate was improved effectively by resorting to a Ti/TiN/TiC transition interlayer with a functional gradient. By properly choosing the different deposition parameters, *e.g.*, voltage, we can change the tribological properties of a-C:H film, and by optimizing the technological parameters we can lower the friction coefficient and the wear rate of a-C:H film to be less than 0.2 and 1.07×10^{-12} mm^3/Nm, respectively. In particular the friction coefficient of a-C:H film can be kept stable for 600 cycles in a rotary sliding test without lubrication. Moreover, the friction and wear behavior of the a-C:H film was dependent on its friction-induced graphite transfer film formed on the worn surface of the counterpart parts during the sliding wear test. In the end, a-C:H film and the counterpart are both deformed plastically after wear-off.

References

[1] Robertson J. Diamond-like amorphous carbon. Journal of Materials Science and Engineering 2002; 37:129–281.

[2] Jacob W, Moller W. On the structure of thin hydrocarbon films. Applied Physics Letters 1993; 63(13):1772–1773.

[3] Weiler M, Sattel S, Jung K, Ehrhardt H, Veerasamy VS, Robertson J. Highly tetrahedral diamond-like amorphous hydrogenated carbon prepared from a plasma beam source. Applied Physics Letters 1994; 64(21): 2797–2799.

[4] Aisenberg Sol, Chabot Ronald. Ion-Beam deposition of thin films of diamond like carbon. Journal of Applied Physics 1971; 42(7): 2953–2958.

[5] Locher R, Wild C, Koidl P. Direct ion-beam deposition of amorphous hydrogenated carbon films. Surface and Coatings Technology 1991; 47(1–3): 426–432.

[6] Druz B, Ostan R, Distefano S, Hayes A., Kanarov V, Polyakov V, *et al.,* Diamond-like carbon films deposited using a broad, uniform ion beam from an RF inductively coupled CH4-plasma source. Diamond and Related Materials 1998; 7(7):965–972.

[7] Gielen JWAM, van de Sanden MCM, Schram MC. Plasma beam deposited amorphous hydrogenated carbon: Improved film quality at higher growth rate. Applied Physics Letters 1996; 69(2):152–154.

[8] Savvides N. Deposition parameters and film properties of hydrogenated amorphous silicon prepared by high rate dc planar magnetron reactive sputtering. Journal of Applied Physics 1984; 55(12): 4232–4238.
[9] Schwan J, Ulrich S, Roth H, Ehrhardt H, Silva SRP, Robertson J, *et al.,* Tetrahedral amorphous carbon films prepared by magnetron sputtering and dc ion plating. Journal of Applied Physics 1996; 79(3):1416–1422.
[10] Holland L, Ohja SM. Deposition of hard and insulating carbonaceous films on an r.f. target in a butane plasma. Thin Solid Films 1976; 38(2):L17–L19.
[11] Catherine Y, Couderc C. Electrical characteristics and growth kinetics in discharges used for plasma deposition of amorphous carbon. Thin Solid Films 1986; 144(2):265–280.
[12] Bubenzer A, Dischler B, Brandt G, Koidl P. rf-plasma deposited amorphous hydrogenated hard carbon thin films: Preparation, properties, and applications. Journal of Applied Physics 1983; 54(8):4590–4595.
[13] Wild C, Koidl P. Structured ion energy distribution in radio frequency glow-discharge systems. [J]. Applied Physics Letters 1989; 54:505–507.
[14] Wild C, Koidl P. Ion and electron dynamics in the sheath of radio-frequency glow discharges. Journal of Applied Physics 1991; 69(5):2909–2922.
[15] Zou JW, Reichelt K, Schmidt K, Dischler B. The deposition and study of hard carbon films [J]. Journal of Applied Physics 1989; 65(10): 3914–3918.
[16] Zou JW, Schmidt K, Reichelt K, Dischler D. The properties of a-C:H films deposited by plasma decomposition of C2H2. Journal of Applied Physics 1989; 67(1):487–494.
[17] Zarrabian M, Fourches-Coulon N, Turban G. Observation of nanocrystalline diamond in diamondlike carbon films deposited at room temperature in electron cyclotron resonance plasma. Applied Physics Letters 1997; 70(19):2535–2537.
[18] Weiler M, Sattel S, Giessen T, Jung K, Ehrhardt H, Veerasamy VS, Robertson J. Preparation and properties of highly tetrahedral hydrogenated amorphous carbon. Physical Review B 1996; 53(3–15):1594–1608.
[19] Weiler M, Lang K, Li E, Robertson J. Deposition of tetrahedral hydrogenated amorphous carbon using a novel electron cyclotron wave resonance reactor. Applied Physics Letters 1998; 72(11):1314–1316.
[20] Conway NMJ, Ferrari AC, Flewitt AJ, Robertson J, Milne WI, Tagliaferro A, *et al.,* Defect and disorder reduction by annealing in hydrogenated tetrahedral amorphous carbon. Diamond and Related Materials 2000; 9(3–6):765–770.
[21] Mantzaris NV, Goloides E, Boudouvis AG, Turban G. Surface and plasma simulation of deposition processes: CH4 plasmas for the growth of diamondlike carbon. Journal of Applied Physics 1996; 79(7):3718–3729.
[22] Jacob W. Surface reactions during growth and erosion of hydrocarbon films. [J]. Thin Solid Films 1998; 326(1–2):1–42.
[23] von Keudell A, Jacob W. Growth and erosion of hydrocarbon films investigated by *in situ* ellipsometry. Journal of Applied Physics 1996; 79(2):1092–1098.
[24] von Keudell A, Jacob W. Surface relaxation during plasma-enhanced chemical vapor deposition of hydrocarbon films, investigated by *in situ* ellipsometry. Journal of Applied Physics 1997; 81(3):1531–1535.
[25] Kessels WMM, Gielen JMCM, Sanden van de, Ijzendoom van, Schram DC. A model for the deposition of a-C:H using an expanding thermal arc. Surface and Coatings Technology 1998; 98:1584–1589.
[26] Boutard D, Moller W, Scherzer JBMU. Influence of H–C bonds on the stopping power of hard and soft carbonized layers. Physical Review B 1998; 38(5–15):2988–2994.
[27] Hopf C, Schwarz-Sellinger T, Jacob W, von Keudell A. Surface loss probabilities of hydrocarbon radicals on amorphous hydrogenated carbon film surfaces. Journal of Applied Physics 2000; 87(6):2719–2725.
[28] von Keudell A, Schwarz-Sellinger T, Jacob W. Simultaneous interaction of methyl radicals and atomic hydrogen with amorphous hydrogenated carbon films. Journal of Applied Physics 2001; 89(5):2979–2986.
[29] Kuppers J. The hydrogen surface chemistry of carbon as a plasma facing material [J]. Surface Science Reports 1995; 22:249–321.
[30] Kaplan S, Jansen F, Machonkin M. Characterization of amorphous carbon-hydrogen films by solid-state nuclear magnetic resonance. Applied Physics Letters 1985; 47(7):750–753.
[31] Jarman RH, Ray GJ, Stadley RW. Determination of bonding in amorphous carbon films: A quantitative comparison of core-electron energy-loss spectroscopy and 13C nuclear magnetic

resonance spectroscopy. Applied Physics Letters 1986; 49(17):1065–1067.
[32] Grill A, Meyerson BS, Patel VV, Reimer JA, Petrich MA. Inhomogeneous carbon bonding in hydrogenated amorphous carbon films. Journal of Applied Physics 1987; 61(8):2874–2877.
[33] Jager C, Gottwald J, Spiess HW, Newport RJ. Structural properties of amorphous hydrogenated carbon. III. NMR investigations. Physical Review B 1994; 50(2–1):846–852.
[34] Tamor MA, Vassell WC, Carduner KR. Atomic constraint in hydrogenated "diamond-like" carbon. Applied Physics Letters 1991; 58(6):592–594.
[35] Kleber R, Jung K, Ehrhardt H, Muhling I, Breuer K, Metz H, *et al.,* Characterization of the sp2 bonds network in a-C:H layers with nuclear magnetic resonance, electron energy loss spectroscopy and electron spin resonance. [J]. Thin Solid Films 1991; 205(2):274–278.
[36] Donnet C, Fontaine J, Lefbvre F, Grill A, Patel V, Jahnes C. Solid state 13C and 1H nuclear magnetic resonance investigations of hydrogenated amorphous carbon. Journal of Applied Physics, 1999; 85(6):3264–3270.
[37] Ferrari AC, LiBassi A, Tanner BK, Stolojan V, Yuan J, Brown LM, *et al.,* Density, sp3 fraction, and cross-sectional structure of amorphous carbon films determined by x-ray reflectivity and electron energy-loss spectroscopy. Physical Review B 2000; 62(16–15):11089–11103.
[38] Ferrari AC, Robertson J. Interpretation of Raman spectra of disordered and amorphous carbon. Physical Review B 2000; 61(20–15):14095–14107.
[39] Tamor MA, Haire JA, Wu CH, Hass KC. Correlation of the optical gaps and Raman spectra of hydrogenated amorphous carbon films. Applied Physics Letters 1989; 54(2):123–125.
[40] Tamor MA, Vassel WC. Raman "fingerprinting" of amorphous carbon films. Journal of Applied Physics 1994; 76(6):3823–3830.
[41] Ramsteiner M, Wagner J. Resonant Raman scattering of hydrogenated amorphous carbon: Evidence for π-bonded carbon clusters. Applied Physics Letters 1987; 51(17):1355–1357.
[42] Yoshikawa M, Katagiri G, Ishida H. Ishitani A. and Akamatsu T. Raman spectra of diamondlike amorphous carbon films. Solid State Communications 1988; 66(11):1177–1180.
[43] Dischler B, Bubenzer A, Koidl P. Bonding in hydrogenated hard carbon studied by optical spectroscopy. Solid State Communications 1983; 48(2):105–108.
[44] Heitz T, Drevillon B, Godet C, Bouree JE. Quantitative study of C—H bonding in polymerlike amorphous carbon films using *in situ* infrared ellipsometry. Physical Review B 1998; 58(20–15):13957–13973.
[45] Ristein J, Stief RT, Ley L, Beyer W. A comparative analysis of a-C:H by infrared spectroscopy and mass selected thermal effusion. Journal of Applied Physics 1998; 84(7):3836–3847.
[46] Beyer W. Incorporation and thermal stability of hydrogen in amorphous silicon and germanium. Journal of Non-Crystalline Solids 1996; 198(1):40–45.
[47] Jiang X, Beyer W, Reichelt K. Gas evolution from hydrogenated amorphous carbon films. Journal of Applied Physics 1990; 68(3):1378–1380.
[48] Jacob W, Unger M. Experimental determination of the absorption strength of C–H vibrations for infrared analysis of hydrogenated carbon films. Applied Physics Letters 1996; 68(4):475–477.
[49] Grill A, Patel V. Characterization of diamondlike carbon by infrared spectroscopy. Applied Physics Letters 1992; 60(17):2089–2091.
[50] DeMartino C, Demichelis F, Tagliaferro A. Determination of the sp3/sp2 ratio in a-C:H films by infrared spectrometry analysis. Diamond and Related Materials 1995; 4(10):1210–1215.
[51] Oppedisano C, Tagliaferro A. Relationship between sp2 carbon content and E04 optical gap in amorphous carbon-based materials. Applied Physics Letters 1999; 75(23):3650–3652.
[52] Dasgupta D, Demichelis F, Pirri CF, Tagliaferro A. π bands and gap states from optical absorption and electron-spin-resonance studies on amorphous carbon and amorphous hydrogenated carbon films. Physical Review B 1991; 43(3–15):2131–2135.
[53] Fanchini G, Tagliaferro A, Dowling DP, Donnelly K, McConnell ML, Flood R, *et al.,* Interdependency of optical constants in a–C and a-C:H thin films interpreted in light of the density of electronic states. Physical Review B 2000; 61(7–15):5002–5010.
[54] Bouzerar R, Amory C, Racine B, Zeinery A. Optical properties of amorphous hydrogenated carbon thin films. Journal of Non-Crystalline Solids 2001; 281(1–3):171–180.
[55] Dischler B, Bubenzer A, Koidl P. Hard carbon coatings with low optical absorption. Applied Physics Letters 1983; 42(8):636–638.
[56] Schutte S, Will S, Mell H, Fuhs W. Electronic properties of amorphous carbon (a-C:H).

Diamond and Related Materials 1993; 2(10):1360–1364.
[57] Xu S, Hundhausen M, Ristein J, Yan B, Ley L. Influence of substrate bias on the properties of a-C:H films prepared by plasma CVD. Journal of Non-Crystalline Solids 1993; 164(2):1127–1130.
[58] Rusli, Robertson J, Amaratunga G. Photoluminescence behavior of hydrogenated amorphous carbon. Journal of Applied Physics 1996; 80(5):2998–3003.
[59] Paret V, Sadki A, Bounouh Y, Alameh R, Naud C, Zarrabian M, *et al.,* Optical investigations of the microstructure of hydrogenated amorphous carbon films. Journal of Non-Crystalline Solids 1998; 227(1):583–587.
[60] Fourches N, Turban G. Plasma deposition of hydrogenated amorphous carbon: growth rates, properties and structures. [J]. Thin Solid Films, 1994; 240(1–2):28–38.
[61] Lacerda RG, Marques FC. Hard hydrogenated carbon films with low stress. Applied Physics Letters 1998; 73(5):617–619.
[62] Sattel S, Robertson J, Ehrhardt H. Effects of deposition temperature on the properties of hydrogenated tetrahedral amorphous carbon. Journal of Applied Physics 1997; 82(9):4566–4576.
[63] Conway NMJ, Ilie A, Robertson J, Milne WI. Reduction in defect density by annealing in hydrogenated tetrahedral amorphous carbon. Applied Physics Letters 1998; 73(17):2456–2458.
[64] Smith FW. Optical constants of a hydrogenated amorphous carbon film. Journal of Applied Physics 1984; 55(3):764–771.
[65] Beiner J, Schrenk A, Winter B, Schubert UA, Lutterloh C, Kuppers J. Spectroscopic investigation of electronic and vibronic properties of ion-beam-deposited and thermally treated ultrathin C:H films. Physical Review B 1994; 49(24–15):17307–17318.
[66] Wild C, Koidl P. Thermal gas effusion from hydrogenated amorphous carbon films. Applied Physics Letters 1987; 51(19):1506–1508.
[67] Camargo SS, Baia-Neto AL, Santos RA, Freire FL, Carius R, Finger F. Improved high-temperature stability of Si incorporated a-C:H films. Diamond and Related Materials 1998; 7(8):1155–1162.
[68] Grill A, Patel V. Low dielectric constant films prepared by plasma-enhanced chemical vapor deposition from tetramethylsilane. Journal of Applied Physics 1998; 85(6):3314–3318.
[69] Grill A. Amorphous carbon based materials as the interconnect dielectric in ULSI chips. Diamond and Related Materials 2001; 10(2):234–239.
[70] Dimigen H. Microstructure and wear behavior of metal-containing diamond-like coatings. Surface and Coatings Technology 1991; 49(1–3):543–547.
[71] Kimock FM, Knapp BJ. Commercial applications of ion beam deposited diamond-like carbon (DLC) coatings. Surface and Coatings Technology 1993; 56(3):273–279.
[72] Matthews A, Eskildsen SS. Engineering applications for diamond-like carbon. Diamond and Related Materials 1994; 3(4–6): 902–911.
[73] Bull SJ. Tribology of carbon coatings: DLC, diamond and beyond. Diamond and Related Materials 1995; 4(5–6):827–836.
[74] Grill A. Review of the tribology of diamond-like carbon [J]. Wear 1993; 168(1–2):143–153.
[75] Bhushan B. Chemical, mechanical and tribological characterization of ultra-thin and hard amorphous carbon coatings as thin as 3.5 nm: recent developments. Diamond and Related Materials 1999; 8(11):1985–2015.
[76] Robertson J. Ultrathin carbon coatings for magnetic storage technology [J]. Thin Solid Films 2000; 383(1–2):81–88.
[77] Goglia P, Berkowitz J, Hoehn J, Xidis A, Stover L. Diamond-like carbon applications in high density hard disc recording heads. Diamond and Related Materials 2001; 10(2): 271–277.
[78] Jiang X, Zou JW, Reichelt K, Grunberg P. The study of mechanical properties of a-C:H films by Brillouin scattering and ultralow load indentation. Journal of Applied Physics 1989; 66(10):4729–4735.
[79] Jiang X, Reichelt K, Stritzker B. The hardness and Young's modulus of amorphous hydrogenated carbon and silicon films measured with an ultralow load indenter. Journal of Applied Physics 1990; 66(12):5805–5808.
[80] Ugolini D, Eitle J, Oelhafen P. Influence of process gas and deposition energy on the atomic and electronic structure of diamond-like (a-C:H) films. [J]. Vacuum 1990;41(4–6):1374–1377.
[81] Zeng LIN, Dechun BA, Zhi WANG, Lishi WEN. Mechanical and tribological properties of diamond-like carbon films on stainless steel grown by RF plasma enhanced chemical vapor deposition. [J]. Chinese Journal of Vacuum Science and Technology 2004; 24(1): 77–80.
[82] Meneve J., Dekempeneer E., Wagner W. and Sneets J., Low friction and wear resistant a-C:H/a-Si1−xCx:H multilayer coatings. Surface and Coatings Technology, 1996; 86(2):617–621.

[83] Oguri K, Arai T. Tribological properties and characterization of diamond-like carbon coatings with silicon prepared by plasma-assisted chemical vapour deposition. Surface and Coatings Technology 1991; 47(1–3):710–721.

[84] Memming R, Tolle HJ, Wierenga PE. Properties of polymeric layers of hydrogenated amorphous carbon produced by a plasma-activated chemical vapour deposition process II: Tribological and mechanical properties [J]. Thin Solid Films 1986; 143(3):31–41.

[85] Grill A, Patel V. Stresses in diamond-like carbon films. Diamond and Related Materials 1993; 2(12):1519–1524.

[86] Grill A. Tribology of diamondlike carbon and related materials: an updated review. Surface and Coatings Technology 1997; 94:507–513.

[87] Gangopadhyay AK, Willermet PA, Vassell WC, Tamor MA. Amorphous hydrogenated carbon films for tribological applications. Tribology International 1997; 30(1):9–31.

[88] Koskinen J, Schneider D, Ronkainen H, Muukkonen T, Varjus S, Burck P, *et al.,* Microstructural changes in DLC films due to tribological contact. Surface and Coatings Technology 1998; 109(1–3):385–390.

[89] Enke K, Dimigen H, Hubsch H. Frictional properties of diamondlike carbon layers. Applied Physics Letters 1980; 36(4):291–292.

[90] Voevodin AA, Phelps AW, Zabinski JS. Donley MS. Friction induced phase transformation of pulsed laser deposited diamond-like carbon. Diamond and Related Materials 1996; 5(11):1264–1269.

[91] Donnet C. Recent progress on the tribology of doped diamond-like and carbon alloy coatings: A review. Surface and Coatings Technology 1998; 100:180–186.

[92] Ronkainen H, Varjus S, Holmberg K. Friction and wear properties in dry, water- and oil-lubricated DLC against alumina and DLC against steel contacts. [J]. Wear 1998; 222(2):120–128.

[93] Ronkainen H, Koskinen J, Varjus S, Holmberg K. Experimental design and modelling in the investigation of process parameter effects on the tribological and mechanical properties of r.f.-plasma-deposited a-C:H films. Surface and Coatings Technology 1999; 122(2–3):150–160.

[94] Erdemir A, Eryilmaz OL, Nilufer IB, Fenske GR. Effect of source gas chemistry on tribological performance of diamond-like carbon films. Diamond and Related Materials 2000: 9(3–6): 632–637.

[95] Racine B, Ferrari AC, Morrison NA, Hutchings I, Milne WI, Robertson J. Properties of amorphous carbon–silicon alloys deposited by a high plasma density source. Journal of Applied Physics 2001; 90(10):5002–5012.

[96] Zeng Lin, Shaobo Lv, Zhaoji YU, Ming Li, Fenf Wang, Dechun BA, In-Seop Lee. Effect of bias voltage on diamond-like carbon film. deposited on PMMA substrate. Surface and Coatings Technology, 2008 (accepted).

[97] Butter RS, Waterman DR, Lettington AH., Ramos RT, Fordham E.J. Production and wetting properties of fluorinated diamond-like carbon coatings. [J]. Thin Solid Films 1997; 311(1–2):107–113.

[98] Grischke M, Hieke A, Morgenweck F, Dimigen H. Variation of the wettability of DLC-coatings by network modification using silicon and oxygen. Diamond and Related Materials 1998; 7(2–5): 454–458.

[99] Lappalainen R, Heinonen H, Antla A, Santavirta S. Some relevant issues related to the use of amorphous diamond coatings for medical applications. Diamond and Related Materials 1998; 7(2–5): 482–485.

[100] Tiainen VM. Amorphous carbon as a bio-mechanical coating — mechanical properties and biological applications. Diamond and Related Materials 2001; 10(2):153–160.

[101] Jones MI, McColl IR, Grant DM, Parker KG, Parker TL. Haemocompatibility of DLC and TiC–TiN interlayers on titanium. Diamond and Related Materials 1999; 8(2–5):457–462.

[102] Parker TL, Parker KL, McColl IR., Grant DM, Wood JV. The biocompatibility of low temperature diamond-like carbon films: a transmission electron microscopy, scanning electron microscopy and cytotoxicity study. Diamond and Related Materials 1994; 3(8):1120–1123.

[103] Smietana M, Szmidt J, Dudek M, Niedzielski P. Optical properties of diamond-like cladding for optical fibres. Diamond and Related Materials 2004; 13:954–957.

[104] Casiraghi C, Ferrari AC, Ohr R, Chu D, Robertson J. Surface properties of ultra-thin tetrahedral amorphous carbon films for magnetic storage technology. Diamond and Related Materials 2004; 13:1416–1421.

[105] Chen Chun-Chin, Hong Franklin Chau-Nan. Interfacial studies for improving the adhesion of diamond-like carbon films on steel. Applied Surface Science 2005; 243(1–4):296–303.

[106] Wang JS, Sugimura Y, Evans AG, Tredway WK. The mechanical performance of DLC films on steel substrates. Thin Solid Films 1998; 325(1–2):163–174.
[107] Dittrich Karl-Heinz, Oelsner Daniel. Production and characterization of dry lubricant coatings for tools on the base of carbon. Refractory Metals and Hard Materials 2002; 20:121–127.
[108] Li KY, Zhou ZF, Chan CY, Bello I, Lee CS, Lee S.T. Mechanical and tribological properties of diamond-like carbon films prepared on steel by ECR-CVD process. Diamond and Related Materials 2001; 10:1855–1861.
[109] Jang Dong-Seob, Kim Dae Eun. Optimum film thickness of thin metallic coatings on silicon substrates for low load sliding applications. Tribology International 1996; 29(4):345–356.
[110] Wu WJ, Hon MH. Thermal stability of diamond-like carbon films with added silicon. Surface and Coatings Technology 1999; 111:134–140.
[111] Liu Y, Erdemir A, Meletis EI. A study of the wear mechanism of diamond-like carbon films. Surface and Coatings Technology 1996; 82:48–56.
[112] Grill A. Diamond-like carbon: state of the art. Diamond and Related Materials 1999; 8:428–434.

60

Applications of Performability Engineering Concepts

Krishna B. Misra

RAMS Consultants, Jaipur, India

Abstract: This chapter is intended to introduce some of the areas of applications of performability engineering that have been presented in this handbook. Only the areas of current interest and importance have been included. It is expected that the chapters will accelerate the process of bringing about synergetic interaction between the practioners of performability engineering in several other relevant areas of applications.

60.1 Introduction

Performability engineering is a composite index to reflect the holistic aspect of performance of any product, system, or services. The objective of initiating such a discussion is to make designers, producers, and users aware of various aspects of performability [1] including survivability and security, so that these aspects are not overlooked while planning any new product, or system.

In fact, there are a number of possible areas of applications and various models [2–9] are available, and it is no the intention to cover them all. Instead, we have selected only those areas that are considered important currently and where the area of application seems to be most appropriate. It is also not possible due to space limitations and the objective of the handbook to include all aspects of the problems in the chosen areas of applications. However, we have attempted to present at least one relevant application in the context of the present scenario from each of the selected constituent areas of performability engineering.

60.2 Areas of Application

For the sake of this handbook, we have chosen the following areas of applications:

60.2.1 Healthcare Sector

The health care industry is one of the world's largest and fastest-growing industries. It consumes over 10% of gross domestic product of most the developed nations. Healthcare can form an enormous part of a country's economy. In fact, in 2003, healthcare costs paid to hospitals, physicians, nursing homes, diagnostic laboratories, pharmacies, medical device manufacturers, and other components of the healthcare system, consumed 15.3% of the GDP of the United States (higher than in any other country) and is expected to rise to 19.6% of GDP by 2016. In fact, the medical industry is one of the fastest growing segments of US economy.

Another reason for higher spending in this sector all over the world is due to the increased life

expectancy and reduction in mortality during the 20th century, which have resulted in an increased aging population. This has snowballed in an increased demand for medical equipment and electronic gadgets for monitoring and diagnostic purposes. In fact, the number of old people will increase further as healthcare programs improve. It is estimated that by 2030, one in every five Americans will be an old person.

In this area of application, we have two chapters, *viz.,* Chapters 61 and 62, included in this handbook. The application has been chosen in view of the growth of this sector and its current importance.

60.2.1.1 Performance of Medical Devices

The first chapter deals with the high performance requirement of medical devices, which is becoming higher ever. Naturally, the quality, reliability, and maintainability of medical equipment and instruments are of great concern to performability engineers. The Chapter 61, from Respironics Inc. looks into all these aspects in detail.

60.2.1.2 Improvement of the Health Delivery System

The second area of application under this sector is on the use of Six Sigma in improving the performance of healthcare delivery system. Developed nations are working to improve these systems as their numbers keep growing. There are some 850 integrated healthcare delivery systems (IDSs) in the United States today. Currently, most systems are considered to be in an evolving state of integration as they attempt to provide a user-friendly service, a one-stop-shopping environment that eliminates costly intermediaries, promotes well-being and improves general health conditions.

It seems appropriate since the management of healthcare delivery systems has always been embroiled in several legal-politico and socio-economic influences and further requires new and innovative improvements due to spectacular advancements in healthcare technologies. Because it is customer-centric, Six Sigma seems the most appropriate methodology for application in suggesting improvements in activities involved in the case under examination. The authors have suggested new systems engineering tools such as CSQFD, VSM, LP, and queuing analysis for the Six Sigma framework and a case study demonstrating the application of this roadmap to improve the waiting times in a retail pharmacy has been presented. The authors claim that the proposed Six Sigma framework is expected to prove highly suitable in healthcare delivery systems, particularly for drug dispensing, radio-logical, admission, and laboratory services.

60.2.2 Structural Engineering

Techniques for the analysis of structures in mechanical engineering or civil engineering are very similar. This is another area of application that has lagged behind the electrical and electronic sector in the application of performability concepts. These applications have not yet fully matured and there is lot to do in this area.

Chapter 63 of this handbook deals with the reliability methodology as is applicable to civil engineering structures, which is equally applicable to mechanical members. The author, who has written a couple of books on the subject, presents in detail the theory and methodology used in probabilistic designs of structural members, which is different from the methodology used in the case of electronic and electrical systems. Probabilistic analysis and design using FORM, SORM, and Monte Carlo simulation is often used with mechanical and civil engineering structures in order to provide economical structures, which otherwise have often been over-designed using high safety factors at high cost with no surety of not failing under actual conditions of use.

60.2.3 Communications

Communication [10, 11] has become a very important technological area in the 21st century. The convenience advanced by wireless communication devices (*e.g*., cellular phones), and the technological advances in portable-lightweight computers (*e.g.*, laptops and PDAs), among others, have triggered the proliferations and set the upward

trends of the uses of WCN around the world. Perhaps the most common use is to connect laptop users who travel from location to location. Another common use is for mobile networks that connect *via* satellite. Wireless networking is used to meet a variety of needs. A wireless transmission method is a logical choice to network a LAN segment that must frequently change locations.

WCN introduces several communication network-related challenges that are different from those considered in traditionally wired CN. This chapter reviews the differences between their communication system performability issues.

A lot of research has been done in the performability analysis of wired CN, but not much is available related to WCN, possibly because the area is new, and the issues in WCN performability are application specific. The performability issues in a non-*ad hoc* and non-mobile WCN can be solved directly using the existing techniques for wired CN because nodes in both networks are stationary. However, the *ad hoc* nature and/or node mobility and the node's limited resources (*e.g.*, battery lifetime), which are typical characteristics of the other WCN models, require different treatments. Chapter 64 of this handbook describes the performability analysis of both the static topology WCN and MANET. It also surveys recent approaches to improving the path reliability in MANET.

60.2.4 Computing Systems

Grid computing is gaining a lot of attention and importance within the IT industry. Standards, enabling technologies, toolkits, and products are now becoming available that allow businesses to use and benefit from grid computing. The most common description of *grid computing* includes an analogy to a power grid where a utility company provides the interface to a complex network of generators and power sources. The vision of grid computing is similar. Once the proper kind of infrastructure is in place, a user will have access to a virtual computer that is reliable and adaptable to his needs. This virtual computer will consist of many diverse computing resources. But these individual resources will not be visible to the user. Grid computing is a newly developed technology for complex systems with large-scale resource sharing, wide-area communication, and multi-institutional collaboration. Many experts believe that grid technologies will offer a second chance to fulfil the promises of the Internet.

The real and specific problem that underlies the grid concept is coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations. Sharing that is not confined to file exchanges but rather direct access to computers, software, data, and other resources. This is required by a range of collaborative problem-solving and resource-brokering strategies emerging in industry, science, and engineering. This sharing is highly controlled by the resource management system, with resource providers and a consumer defining what is shared, who is allowed to share, and the conditions under which the sharing occurs.

The advantages of grid computing are that we can solve large, more complex problems in much shorter times, and collaboration with other organizations becomes easier and allows us to make better use of existing hardware. However, there are disadvantages as well, for example, the still evolving grid software and standards, the learning curve to get started, and non-interactive job submission. Generally there are three kinds of grids, *viz.*, the computational grid, specifically for computing power, the data grid, for housing and providing access to data across organizations, and the scavenging grid, which is the most commonly used. This has a large number of desktop machines and the owners of these machines are usually given control over when their resources are available to participate in the grid.

Chapter 65 in the handbook discusses all the associated problems, particularly as related to their performance.

60.2.5 Fault Tolerant Systems

Fault-tolerance is the property that enables a system to continue operating properly in the event of the failure of some of its components. Fault-tolerance [12] is particularly desired in high-availability or life-critical systems, or in essential

public concerns such as air, rail, and automobile traffic control, emergency response systems, airline flight controls, nuclear power plant safety systems, and most of all, our rapidly growing dependence on healthcare delivery *via* high-performance computing and communications. When these systems fail, lives and money may be lost. Sometimes, undiscovered design faults (such as software bugs and glitches) can cause system crashes during peak demand, resulting in service disruptions and financial losses. Complex systems may suffer stability problems due to unforeseen interactions of overlapping fault events and mismatched defense mechanisms. New threats from hackers and criminally minded individuals invade systems, causing disruptions, misuse, and damage. Accidents result in severed communication links, affecting entire regions. Finally, we face the possibility of system damage by these "info-terrorists." Fault tolerance is our best guarantee that high confidence systems will not betray the intentions of their designers and the trust of their users by succumbing to physical, design, or human-machine interaction faults.

The growing need for networked environments is setting new challenges to the designers of fault tolerance in systems. Fault tolerance covers areas like system architecture, hardware and software design, operating systems, Internet protocol (IP) network communications, parallel and grid processing, and verification and testing. Since fault tolerant systems are designed to perform even in the presence of faults, errors or attacks, their performance is evaluated by taking into account the consequences of the embedded fault handling actions.

A considerable amount of research is needed to tackle the problem of network performability in the networking environment. As new technologies are developed and new applications are discovered, new approaches in fault tolerance are also required. In a multi-technology, multi-network environment, in each of the networking layers, different types of failures/attacks and responses are possible. Research is needed to exploit the impact of the failure propagation from one network to another as layer restoration processes may affect each other.

As hardware and software systems are increasingly becoming large and complex, the concern for performance becomes more serious, particularly in many technological areas, such as space reconfigurable VLSI technology, cluster based FPGA architectures, and computing platforms with numerous processors. It is expected that the concern for performability in the research and application of fault tolerant systems will become more pronounced in future.

Chapter 66 discusses in great detail all aspects of this subject of current interest.

60.2.6 Prognostics and Health Monitoring

Equipment prognostics and health management as part of operations and maintenance can be used in accurately predicting impending failures and providing a mechanism for remedial measures such as replacing parts safely before failure. An ideal general purpose prognostic system would use data driven prognostics approaches that do not require *a priori* knowledge of the system. The prognostic system would learn the characteristics of the monitored system with use, so that anomalies could be detected quickly as it learned and remaining life estimates could be given with smaller associated uncertainty.

The fact that a fault has been declared, however, does not necessarily mean that immediate maintenance action is needed. That is where prognostics come in. Prognostic software will use inputs from multiple sensors, operating data, and failure histories in order to predict the life of a component, and to determine when and what type of maintenance is required.

A blade slightly damaged by some foreign object entering the engine may be deformed, but if it is not affecting performance to any great degree and if a crack is not growing, replacement might be safely postponed to a regularly scheduled maintenance shutdown. Many existing health monitoring systems use fault detection and diagnostic techniques, but are not focused on automating prediction of future machine conditions. To prevent dangerous situations from occurring, and to help lower the operating and maintenance costs, designers and planners have

begun to look into key enabling technologies that provide not only early warning of potential disasters, but are also substantive indicators of the real-time health of engine components and the overall system. Blade tip sensors embedded in the engine case have been used for decades to measure blade tip clearance and blade vibration. Many sensing technologies have been used: capacitive, inductive, optical, microwave, infrared, eddy-current, pressure, and acoustic.

The prognostic approach is based on the current state of the component or machine, and on the available operating and failure history data. The ability to monitor and predict failures, detect and classify anomalous events, and assess remaining useful life [13] in electronic systems can provide significant cost benefits, enhanced mission readiness and condition based maintenance. These approaches have been very much in use for mechanical equipment, propulsion engines, turbines, and other rotating machines, pressure vessels, *etc*., but have not been popular with electronic equipment.

Prognostics and health monitoring (PHM) techniques make use of sensing, recording, and interpretation of environmental, operational, and performance-related parameters indicative of a system's health. Product health monitoring can be implemented through the use of various techniques to sense and interpret parameters that are indicative of:

- performance degradation, by knowing the deviation of operating parameters from their expected values;
- physical or electrical degradation, by observing material cracking, corrosion, inter-facial delamination, or increases in electrical resistance or threshold voltage;
- changes in a life-cycle environment, by noticing the usage duration and frequency, ambient temperature and humidity, vibration, and shock.

By observing the equipment's health, based on its monitored life-cycle conditions, maintenance procedures can be developed. The objective is to predict the advent of failure in terms of a distribution of remaining life, level of degradation, or probability of mission survival. PHM has become a requirement for any system sold to the DoD.

Chapter 67 of this handbook is from CALCE, which has been doing a poineering work in this area and it is amply made clear by this chapter that if we can assess the extent of deviation or degradation from an expected normal operating condition for electronics, information can be derived on advanced warning of failures, minimizing unscheduled maintenance, extending maintenance cycles, and improving availability by timely repairs, reducing the life-cycle cost of equipment by decreasing inspection costs, downtime, and inventory; and for improving qualification and assisting in the design and logistical support of fielded and future systems.

In other words, prognostics and health monitoring should help improve electronic system performance and reduce its life cycle costs, just as it does in mechanical equipment. The application to electronic equipment is a recent occurrence.

60.2.7 Maintenance of Infrastructures

Maintenance of infrastructure is vital in the economic well-being of a country. There are several aspects that can be discussed under this title, but we will discuss here only two important infrastructures of public interest, *viz*, rail and civil structures that include machanical structures as well.

60.2.7.1 Railway Tracks

Maintenance [14, 15] is a critical function for ensuring performance of a system. More so if it concerns railways. It is of great concern for those nations where rail transportation constitutes a major infrastructure like highways. In countries like India with a total track length of about 64,000 kilometres, and 13 million passengers and 1.3 million tonnes of freight carried by 14300 trains every day, it constitutes an important infrastructure and the lifeline of economy, resulting in an annual revenue of about US$ 18 billion. To maintain such a large length of track (which is fifth largest after USA, Russia, Canada, and China) under single

management is by no means is an easy task. Moreover, as railways are associated with passengers and freight, it always has the risk of loss of lives and loss of assets. New technologies and better safety standards are constantly introduced but still accidents occur all over the world. Of course risk of train collisions and derailments can be reduced by better safety measures and elimination of root causes. These causes will require an effective maintenance strategy to govern optimization of inspection frequency and/or improvement in skill and efficiency. A detailed and careful study of the defects that emerge both on the rolling stock and rail infrastructure is essential to frame out the correct maintenance strategy.

Detection and rectification of rail defects are major issues for all rail players around the world. Some of the defects include worn out rails, welding problems, internal defects, corrugations, and rolling contact fatigue (RCF) initiated problems such as surface cracks, head checks, squats, spilling, and shelling. If undetected and/or untreated these defects can lead to rail breaks and derailments. There is also a need for better prediction of rail defects over a period of time based on operating conditions and maintenance strategies. Trains subject the track structure to repeated loading and unloading as they pass. Each loading–unloading cycle causes deformation of the track, part of which is elastic and recovers; while other parts suffer permanent deformation. Track settlement is an integrated process in which the settlement of one component affects that of another. As soon as the track geometry starts to deteriorate, the variations of the train/track interaction forces increase, and this speeds up the track deterioration process. Measurement of track geometry irregularities is the most used automated condition monitoring technique in railway infrastructure maintenance.

Rail degradation is basically due to wear and fatigue. Track curvature has a major influence on degradation. A narrow curve implies wear, whereas tangent track implies fatigue. Fatigue is a major future concern as business demands for higher speed, higher axle loads, higher traffic density, and higher tractive forces increase. The presence of manufacturing defects in the rail subsurface and the direction of the crack mouth on the rail surface are both responsible for guiding crack development direction The presence of water or snow on the rails may also increase the crack propagation rate.

We have included Chapter 68 in this handbook, which looks into all these aspect in more detail, including the maintenance optimization of rail tracks. The basic idea is to reduce the operation and maintenance costs while still maintaining high safety standards and minimizing accidents [16–21].

60.2.7.2 Civil Structures

The performance of civil engineering systems over time is subject to a number of uncertainties [22, 23]. These include operational conditions, material characteristics, and environmental exposure. Usually, civil engineering structures age due to wear, corrosion, fatigue, and other phenomena. At some point of time they must be inspected and either repaired or replaced just as any deteriorating equipment. For concrete structures the most important aging phenomena in temperate climates are corrosion due to carbonation and/or chloride attack, for steel structures it is rust and fatigue. In general, aging phenomena are uncertain. A failure is defined when a more or less complicated function of those variables reaches a limiting state for the first time. Failure time distributions are determined numerically. This makes analyses rather complex and rather different from analyses where analytical failure time models based on rich data can be used.

60.2.8 Restructured Power Systems

This is a new development that originated towards the end of the last century and will become relevant in the 21st century. Restructuring started in 1980 in Chile and the UK and spread to Latin America (Argentina) and in diverse form to USA, Australia, and number of Asian Countries in the 1990s. Since then the US electric industry, a $220 billion industry, is undergoing a tough change in the way it delivers electricity to millions of households and industries through out the country. It was the last great government-sanctioned

monopoly and is now being deregulated slowly and opened to competition, giving consumers the power to choose their electricity provider in much the same way as they choose telephone companies today.

Restructuring or deregulating the power supply industry is a very complex exercise and depends on national strategies and policies, macroeconomic developments and existing conditions, and its application is therefore likely to be different in different countries. Liberalization, deregulation, and privatization all are part of market reforms. It was believed that privatization in the power industry would eliminate power thefts, subsidy, and bring in a higher operating efficiency, and reduce labor and workplace inefficiencies.

It is true that several factors such as technological advances, changes in political and ideological conditions, regulatory failures, high tariffs, managerial inadequacies, global financial drives, environmental activism, and shortage of public resources for development in developing countries have been accelerating the worldwide advent of restructuring of the energy supply industry although the main drive for restructuring, particularly in the UK, came from the government's belief that competition among energy suppliers would offer a wide choice for electricity consumers giving them a say in who supplies the power to them while lowering prices and expanding services. It was thought that reducing government control of the industry would benefit consumers, which would outweigh the benefits of long-established practices followed earlier.

However, the success story is different in California, which in 1996 became one of the first states to enact an electricity restructuring plan. Not long after the plan was introduced, price increases began to erode the public support for deregulation and just two years after the deregulation was enacted, California consumer groups succeeded in putting on the ballot an initiative that would have thrown out the state's deregulation plan.

In fact, the situation during the 1980s was quite conducive to the deregulation regime and provided stimulus for implementation. The advances in gas turbine technology led to more efficient small turbines and generation, which matched the efficiency of large units, particularly when run on natural gas. The price of natural gas also declined, and the restrictions on the use of natural gas were eased in that period.

Restructuring and deregulation has brought in the notions of competition and marketing strategies in addition to introducing new technical considerations in the operation of these independently owned but operationally interconnected parts of the system under the control of another independent authority with the generic name of independent system operator (ISO). ISO holds the unique position of having the responsibility and authority for secure operation of the system without owning it. The traditional vertically integrated utility is now split into several companies such as generation companies (gencos), transmission companies (transcos) and distribution companies (discos), and retail companies. Also due to different market structures in the existing restructured power systems, the reliability and price problems for various market models are different. Generally speaking, the market models can be classified into PoolCo, bilateral contracts and hybrid models.

We have included Chapter 70 to discuss all these new developments and present the new regime that will govern the restructuring of the energy system in the 21st century.

60.2.9 PRA for Nuclear Power Plants

Generally, a nuclear power plant is significantly more expensive to build than the equivalent coal-fueled or gas-fueled plant. However, coal is significantly more expensive than nuclear fuel, and natural gas is significantly more expensive than coal. Thus, capital cost aside, natural gas-generated power is the most expensive. Most forms of electricity generation produce some form of negative externality, costs imposed on third parties that are not directly paid by the producer, such as pollution which negatively affects the health of those near and downwind of the power plant, and generation costs often do not reflect these external costs. A UK Royal Academy of Engineering report in 2004 was conducted with the aim to develop "a

robust approach to compare directly the costs of intermittent generation with more dependable sources of generation". Wind power was found to be more than twice as expensive as nuclear power. Also an OECD/IEA study from 2005 estimated nuclear power total-lifetime costs *per* kWh electric *versus* coal and natural gas for 12 nations and nuclear power generally superseded coal (even without a carbon tax), even though the study unrealistically assumed 40-year plant lifetimes (new plants are designed to operate for 60 or more years). The World Nuclear Association states that "Sun, wind, tides and waves cannot be controlled to provide directly either continuous base-load power or peak-load power when it is needed. In practical terms they are therefore limited to some 10–20% of the capacity of an electricity grid, and cannot directly be applied as economic substitutes for coal or nuclear power, however important they may become in particular areas with favourable conditions."

Thus nuclear power will continue to be produced since:

- it costs about the same as coal, so it is not expensive to make;
- it does not produce smoke or carbon dioxide, so it does not contribute to the greenhouse effect or global warming;
- it produces huge amounts of energy from small amounts of fuel;
- it produces small amounts of waste; and
- it is reliable.

However it has disadvantages as well:

- Although the amount of waste produced is not much, it is highly dangerous and must be disposed of by sealing up and buried for many years to allow the radioactivity to die away.
- A substantial amount of money has to be spent on safety, since a nuclear accident can be a major disaster.

People are increasingly becoming concerned about the safety of nuclear plants and it is reflected from the fact that in the 1990s nuclear power was the fastest-growing source of power in much of the world. In 2005 it was the second slowest-growing. Notwithstanding the foregoing statement, the safety record of nuclear plants has been quite exemplary. Yet the people must be convinced by objective assessment of risk [24–30] associated with any technology they use.

The World Nuclear Association (WNA accredited to the United Nations, is an independent, non-profit organization, funded primarily by membership subscriptions) provides a comparison of deaths due to accidents among different forms of energy production. In their comparison, deaths *per* TWy of electricity produced are 885 for hydropower, 342 for coal, 85 for natural gas, and 8 for nuclear power. Moreover, there have been only two major reactor accidents in the history of civil nuclear power, *viz.,* Three Mile Island and Chernobyl. The first was contained without harm to anyone and the other involved an intense fire without the provision for containment (serious design defect). These are the only major accidents to have occurred in more than 12,700 cumulative reactor-years of commercial operation in 32 countries. The risks from western nuclear power plants, in terms of the consequences of an accident or terrorist attack, are minimal compared with other commonly accepted risks.

However, to address the safety concern the goal is to protect man and his environment by limiting the release, under any circumstances, from the radioactive materials that the facility contains; in other words, ensuring the containment of radio-active materials. This is achieved by providing three-layer barriers between the radioactive source and the public, *viz.,* the fuel cladding, the primary reactor coolant system, and the containment building. It is further ensured in the event of an accident, that its consequences must be limited to a level that is acceptable for both the public and the environment.

Probabilistic risk assessment (PRA) or *probabilistic safety analysis* (PSA) can be conducted to calculate the probability of damage to the core as a result of sequences of accidents identified by the study. PSA [31–38] can now help assess the size of radioactive releases from the reactor building in the event of an accident, as well as the impact of such releases on the public and the environment. These studies are referred to as levels

1, 2, and 3 PSAs respectively. Level 1 study is corresponding to the assessment of the risk of a core melt accident. Level 2 analyses are performed, or are planned, in most NEA countries in view of their importance in determining accident management strategies and identifying potential design weaknesses in reactor containment building. Level 3 analyses are used for emergency planning, since it assesses the amount of release of radioactivity in the environment if containment fails to contain the accident.

The results of these analyses can, therefore, identify not only the weaknesses but also the strengths with regard to the plant's safety, and thus assist in setting priorities and focusing efforts on the points identified as the most sensitive in terms of the contribution they can make to improve the safety of facilities.

We have included Chapter 71 on probabilistic risk assessment for nuclear power plants from an experienced author who has spent a great deal of time in a German nuclear reactor establishment.

60.2.10 Problems in Software Engineering

The last four chapters, *viz.*, Chapters 72, 73, 74, and 75 are related to software reliability or quality problems. Software reliability is a growing field and much research is being done in this area to develop models for prediction and growth. In fact, computers and intelligent parts are quickly pushing their mechanical counterparts out of the market. Appliances such as washing machines, telephones, TVs, and watches, are having their analog and mechanical parts replaced by CPUs and software. It is the predominance of software driven devices and equipment that has brought software to forefront of current revolution. Software can make decisions, but can be just as unreliable as human beings. Software can also have small unnoticeable errors or drifts that can culminate into a disaster. Fixing problems may not necessarily make the software more reliable. On the contrary, new serious problems may arise. In 1991, after changing three lines of code in a signaling program containing millions of lines of code, the local telephone systems in California and along the Eastern seaboard came to a stop. Software reliability [39] is an important attribute together with functionality, usability, performance, serviceability, capability, installability, maintainability, and documentation. Sometimes, software reliability may be hard to achieve, because the complexity of software tends to be high. While the complexity of software is inversely related to software reliability, it is directly related to other important factors in software quality, especially functionality, capability, *etc*. Emphasizing these features will tend to add more complexity to software.

There are two major differences between hardware and software failure rate curves [40]. One difference is that in the last phase, software does not have an increasing failure rate but hardware does. In this phase, software approaches obsolescence; there is no motivation for any upgrades or changes to the software. Therefore, the failure rate will not change. The second difference is that in the useful-life phase, software will experience a drastic increase in failure rate each time an upgrade is made. The failure rate levels off gradually, partly because of the defects found and fixed after the upgrades.

Too much proliferation of software reliability models [3] has taken place as people try to understand the characteristics of how and why software fails, and try to quantify software reliability. Over 200 models have been developed since the early 1970s, but how to quantify software reliability still remains largely unresolved.

Software modeling techniques [39] can be divided into two subcategories: prediction modeling and estimation modeling. Using prediction models, software reliability can be predicted early in the development phase and enhancements can be initiated to improve the reliability. Prediction models include Musa's execution time model [41], Putnam's model, and Rome Laboratory models, whereas estimation models include exponential distribution models, the Weibull distribution model, and the Thompson and Chelson model, *etc*. Current interest in software quality and reliability are indicated from the papers published recently [42–50].

Measuring software reliability is a difficult problem even today, because we do not have a

good understanding of the nature of software. There is no clear definition to what aspects are related to software reliability. Even the most obvious product metrics such as software size do not have a uniform definition. It is better to measure something related to reliability to reflect the characteristics, if we cannot measure reliability directly. The current practices of software reliability measurement can be divided into four categories, *viz.*, product metrics, project management metrics, process metrics, and fault and failure metrics.

Chapter 72 outlines the basic software development process. Some of the existing NHPP software reliability models and their applications are presented along with a generalized software reliability model, considering environmental factors. The concepts of software fault tolerant and software cost models are briefly discussed.

Chapter 73 explores the utility of lognormal distribution in software reliability growth modeling. The authors demonstrate that several observable properties of software systems are in fact related, being grounded in the conditional nature of software execution. This leads to the emergence of a lognormal distribution of rates of events in software systems. These include failure rates of defects and execution rates of code elements. They further discuss how the lognormal growth model can be obtained from the distribution of the first occurrence times of defects and apply it to reliability growth.

Chapter 74 indicates how within the short delivery times that are now becoming very common these days, the software product quality can be improved and in fact be controlled in the early stages of software development. The author employs multivariate linear analysis by making use of process measurement data, derives effective process factors improves product quality, and obtains quantitative relationships between quality assurance/management activity and final product quality.

In Chapter 75, the authors, present software reliability growth models (SRGMs) that describe the relationship between the number of faults removed and the number of test cases used. They also discuss flexible discrete SRGM, which can depict either exponential or S-shaped growth curves, depending upon the parameter values estimated from the past failure data.

Sustainability

Application of sustainability concept can be seen from a few representative examples like [51–53].

60.2.11 Concluding Comments

We have attempted to present very few applications that are of current interest and have relevance in the present context. It was neither our intention, nor it was physically possible to discuss all areas of applications but to present a set of 15 chapters presented here that provides an indication of a set of representative problems in the vast area of applications of performability engineering. Also since there can be thousands of references on applications and it is not possible to include all of them here, we have included mainly those representative references which have been published in the International Journal of Performability Engineering and it is hoped that with the publication of this handbook, further interest will be generated through the cross fertilization of ideas and many more new areas for applications will be opened up.

References

[1] Liu Y, Trivedi KS. Survivability quantification: The analytical modeling approach. International Journal of Performability Engineering. January 2006; 2(1): 29–44.

[2] Dhillon BS, Zhijian L. Stochastic analysis of a system containing N-redundant robots and M-redundant built-in safety units. International Journal of Performability Engineering. Oct. 2005; 1(2): 179–189

[3] Shah A, Dhillon BS. Reliability and availability Analysis of three state device redundant systems with human errors and common cause failure. International Journal of Performability Engineering. Oct. 2007; 3(4): 411–418.

[4] Wang Z, Xie L, Li B. Time dependent reliability models of systems with common cause failure.

International Journal of Performability Engineering. Oct. 2007; 3(4): 419–432.
[5] Gokhale SS, Crigler JR, Farr WH. System availability analysis considering failure severities. International Journal of Performability Engineering. Oct. 2007; 3(4): 467–480.
[6] Xing L. Reliability importance analysis of generalized phased-mission systems. International Journal of Performability Engineering. July 2007; 3(3): 303–318.
[7] Zhang M, He Zhen, Dong Y-F. A study on tool wear process control and tool quality life. International Journal of Performability Engineering. April 2006; 2(2): 163–173.
[8] Rao KD, Kushwaha HS, Verma AK, Srividya A. Epistemic uncertainty propagation in reliability assessment of complex systems. International Journal of Performability Engineering. January 2008; 4(1): 71–84.
[9] Kang HG, Jang SC, Ha J. Fault tree modeling for redundant multifunctional digital systems. International Journal of Performability Engineering. July 2007; 3(3): 329–336.
[10] Soh S, Lim KY, Rai S. Evaluating communication-network reliability with heterogeneous link capacity using subset enumeration. International Journal of Performability Engineering. Jan. 2006; 2(1): 3–17.
[11] Shrestha A, Xing L. Quantifying application communication reliability of wireless sensor networks. International Journal of Performability Engineering. January 2008; 4(1): 43–56.
[12] Levitin G, Amari SV. Reliability analysis of fault tolerant systems with multi-fault coverage. International Journal of Performability Engineering. Oct. 2007; 3(4): 441–452
[13] Mathew S, Rodgers P, Eveloy V, Vichare N, Pecht M. A methodology for assessing the remaining life of electronic hardware. International Journal of Performability Engineering. Oct. 2006; 2(4): 383–395.
[14] Hurtado JL, Joglar F, Modarres M. Generalized renewal process: Models, parameters estimation and application to maintenance problems. International Journal of Performability Engineering. July 2005; 1(1): 37–50.
[15] Gabbar HA, Yamashita H, Suzuki K. Integrated plant maintenance management using enhanced RCM mechanism. International Journal of Performability Engineering. Oct. 2006; 2(4): 369–381.
[16] Kohda T. Accident occurrence conditions in railways. International Journal of Performability Engineering. January 2007; Part II; 3(1): 105–116.
[17] Rao AL. Risk management of public transportation systems in North America. International Journal of Performability Engineering. Jan. 2007; Part I; 3(1): 5–18.
[18] Cho Y-O, Kwak S-L, Wang J-B, Park C-W. An integrated R&D program for the railway safety improvement in Korea. International Journal of Performability Engineering. Jan. 2007; Part I; 3(1): 19–24.
[19] Dumolo RN. Application of system engineering to railway projects. International Journal of Performability Engineering. January 2007; Part I; 3(1): 25–34.
[20] Kang KS. Safety certification for rapid transit systems in Singapore. International Journal of Performability Engineering. Jan. 2007; Part I; 3(1): 35–46.
[21] Poon L, Lau R. Fire risk in metro tunnels and stations. International Journal of Performability Engineering. July 2007; 3(3): 355–368.
[22] Mathada VS, Venkatachalam G, Srividya A. Slope stability assessment-a comparison of probabilistic, possibilistic and hybrid approaches. International Journal of Performability Engineering. April 2007; 3(2): 231–242.
[23] Liu K-P, Luk B-M, Yeung T-W, Tso SK, Tong F. Wall inspection system for safety maintenance of high rise buildings. International Journal of Performability Engineering. January 2007; Part II; 3(1): 187–197.
[24] Suddle SI. The weighted risk analysis applied for Bos and Lommer. International Journal of Performability Engineering. Oct. 2007; 3(4): 481–497.
[25] Smith D. Moving people from process to preference. International Journal of Performability Engineering. January 2007; Part I; 3(1): 91–99.
[26] Tohara K. Lessons learned and risk management. International Journal of Performability Engineering. January 2007; Part I; 3(1): 61–74
[27] Feng H-Q, Gabbar HA, Suzuki K, Rizal D. Use of Grey relation analysis in causative analysis of chemical plant accidents. International Journal of Performability Engineering. Oct. 2006; 2(4): 341–350.
[28] Johnsen SO, Hansen CW, Line MB, Nordby Y, Rich E, Qian Y. CheckIT: A Program to measure and improve information security and safety culture. International Journal of Performability Engineering. January 2007; Part II; 3(1): 171–186.
[29] Aven T, Abrahamsen E. On the use of cot-benefit analysis in ALARP processes. International Journal of Performability Engineering. July 2007; 3(3): 345–353.

[30] Kohda T, Nakagawa M. Dynamic risk evaluation of systems with multiple protective systems. International Journal of Performability Engineering. Oct. 2007; 3(4): 453–466.
[31] Chou Y-C, Wu C-H. Accident sequence precursor analyses of Taiwan nuclear power plant. International Journal of Performability Engineering. January 2007; Part II; 3(1): 117–126.
[32] Kang KM, Jae M, Suh KY. A Bayesian inference algorithm to identify types of accidents in nuclear power plants. International Journal of Performability Engineering. January 2007; Part II; 3(1): 127–136.
[33] Chao C-C, Huang C-T, Chen M-C, Chen WC. ABWR initiating event analysis for risk informed applications. International Journal of Perform-ability Engineering. January 2007; Part II; 3(1): 159–170.
[34] Wu W-F, You J-S, Kuo H-T, Wu C-H. Degradation analysis and risk-informed management of feedwater system in nuclear power plants. International Journal of Performability Engineering. January 2007; Part II; 3(1): 149–158.
[35] Wu C-H, Lin T-J, Kao T-M. The impact from the fire PSA hazard factor for the PWR Plant. International Journal of Performability Engineering. July 2007; 3(3): 337–344.
[36] Yau M, Motamed M, Guarro S. Assessment and integration of software risk within PRA. International Journal of Performability Engineering. July 2007; 3(3): 369–378.
[37] Srividya A, Suresh HN, Verma AK, Vinod G. Reliability of PHT Piping in PHWR against erosion corrosion. International Journal of Performability Engineering. Jan. 2008; 4(1): 85–94.
[38] Kurnianto K, Downs T. Sensor validation in nuclear power plant using the method of boosting. International Journal of Performability Engineering. Oct. 2005; 1(2): 157–165.
[39] Lyu Michael R. Handbook of software reliability engineering. McGraw-Hill, New York, 1995.
[40] Keene SJ. Comparing hardware and software reliability. Reliability Review; 1994:14(4): 5–7, 21.
[41] Musa John D. Introduction to software reliability engineering and testing. Proc. of 8th International Symposium on Software Reliability Engineering (Case Studies);1997: Nov. 2–5. Albuquerque, NM.
[42] Shigeru Y. A human factor analysis for software reliability in design-review process. International Journal of Performability Engineering. July 2006; 2(3): 223–232.
[43] Dohi T, Suzuki H, Osaki S. Transient Cost Analysis of Non-Markovian Software Systems with Rejuvenation. International Journal of Performability Engineering. July 2006; 2(3): 233–243.
[44] Mehta P, Verma AK, Srividya A. Integrated product and process attribute-quantitative model for software quality. International Journal of Performability Engineering. July 2006; 2(3): 265–276.
[45] Kanoun K , Crouzet Y. Dependability benchmarks for operating systems. International Journal of Performability Engineering. July 2006; 2(3): 277–289.
[46] Ramasamy S, Govindasamy G. Generalized exponential Poisson model for software reliability growth. International Journal of Performability Engineering. July 2006; 2(3): 291–301.
[47] Vesley WE. Use of Bayesian network in software reliability assurance. International Journal of Performability Engineering. Oct. 2006; 2(4): 305–314.
[48] Seliya N, Khoshgoftaar TM. Software quality modeling and estimation with missing data. International Journal of Performability Engineering. Jan. 2008; 4(1): 5–18.
[49] Tokuno K, Fukuda M, Yamada S. Stochastic performance evaluation for software system considering NHPP task arrival. International Journal of Performability Engineering. Jan. 2008; 4(1): 57–70.
[50] Kaaniche M, Lollini P, Bondavalli A, Kanoun K. Modeling the resilience of large and evolving systems. International Journal of Performability Engineering. April 2008; 4(2): 153–168.
[51] Baas L. Dissemination models for cleaner production and industrial ecology. International Journal of Performability Engineering. July 2005; 1(1): 89–99.
[52] Veeraraghavan T, Salari-Namin D. Sustainable development and environment assessment: A case study of a fertilizer project. International Journal of Performability Engineering. Jan. 2006; 2(1): 75–87.
[53] Barbiroli G. Enduring Quality: A key factor to increase resource productivity. International Journal of Performability Engineering. Jan. 2006; 2(1): 89–97.

61

Reliability in the Medical Device Industry

Vaishali Hegde

Respironics Inc. Sleep and Home Respiratory Central Facility
Monroeville, Pennsylvania, 15146, USA

Abstract: The medical industry is one of the fastest growing segments of the US economy. Increasingly, medical equipment is being used outside a controlled hospital environment. The complexity and increased use of medical equipment in non-hospital environments has made the need for safe, reliable products imperative. Although reliability engineering tools are well established, their application to the medical industry is fairly new. This chapter discusses the reliability tools and standards applicable to the medical equipment industry.

61.1 Introduction

The medical industry is one of the fastest growing segments of the US economy. In 2004, healthcare spending in the US reached $1.9 trillion, and was projected to reach $2.9 trillion in 2009 [1]. In 2004, the US spent 16% of its gross domestic product (GDP) on healthcare. It is projected to rise to 20% in the next decade. The United States is not the only country in the world spending large sums of money on healthcare. Countries all over the world are spending more and more on healthcare every year. According to the Organization for Economic Cooperation and Development, healthcare spending accounted for 10.9% of the GDP in Switzerland, 10.7% in Germany, 9.7% in Canada, and 9.5% in France [2].

Healthcare spending is increasing all over the world due to increased life expectancy and consequently the increased aging population. Reduction in mortality during the 20th century led to large increases in life expectancy. By 2000, life expectancy in the US was approximately 76.9 years. According to the US Census Bureau's projections, by 2030, the older population in the US is projected to be double that of 2000, growing from 35 million to 72 million. By 2050, they project the older population to be around 86.7 million. In other words, nearly one in five Americans will be age 65 and over in 2030 [3].

In 2000, about 92% of people aged 65 and over had made at least one healthcare visit to a doctor's office, an emergency room, or a hospital during the past year (NCHS, 2003a). Among people 65 and older, the number of healthcare visits increased with age.

Chronic diseases have caused most elderly deaths throughout the last 50 years. Diseases of the heart, malignant neoplasms (cancer), cerebro-vascular diseases (stroke), chronic obstructive pulmonary diseases/chronic lower respiratory diseases, and pneumonia and influenza were the top five causes of death for people aged 65 and

over, in year 2000 [3]. Treatment of these chronic diseases requires several different types of medical devices. All data mentioned above points to an explosive growth in the medical device and medical services market in the world.

When it comes to medical equipment, failure is not an option. From critical devices such as oxygen concentrators, lasers, ventilators, MRI scanners, insulin pumps, implantable pacemakers to instruments as straightforward as stethoscopes, injections, and thermometers, medical equipment must be reliable. The medical industry must have higher reliability standards than other fields. However, a high reliability standard is hard to maintain in today's environment of intense global competition, pressure for shorter product-cycle times, stringent cost constraints, higher customer expectations for quality and reliability, and complex global and heterogeneous markets.

Medical electronic products are increasingly being used in non-hospital environments by non-clinical personnel. This is because sophisticated medical products are becoming more compact and portable. For example, a few years ago, an oxygen concentrator weighed 75 pounds, had to be plugged into the wall for power, and had to be used in a controlled clinical environment. Today, a portable oxygen concentrator weighs only 8 pounds, can operate on batteries and can be used in a home environment. Developing and producing a medical electronic product reliable enough to continuously repeat certain key functions over and over again like clockwork and alarming appropriately in case of a fault condition, is now more important than ever before.

Today, reliability takes on even greater significance since medical devices designed for specific applications are becoming more expensive. It is not uncommon for cancer treatment or surgery equipment to cost a few million dollars. While hospitals may be relatively profitable, they cannot afford to have too many of these expensive products. If one such medical system incurs downtime due to failure, it can adversely affect the hospital's bottom line, its reputation, and the well-being of its patients [4]. In some cases, medical electronics products in use for several years require updating to increase their reliability as greater healthcare demands are placed on them.

The financial impact of having an unreliable or unsafe medical product in the market can be devastating for a medical device manufacturer. Since December 13, 1984, the FDA Medical Device Reporting (MDR) regulations have required firms who have received complaints of device malfunctions, serious injuries or deaths associated with medical devices to notify FDA of the incident. The MDR regulation provides a mechanism for FDA, manufacturers, importers and user facilities to identify and monitor significant adverse events involving medical devices. The goals of the regulation are to detect and correct problems in a timely manner. MedWatch, the FDA's safety information and adverse event reporting program is set up for health professionals and consumers to report serious adverse reactions and problems related to drugs, medical devices, cosmetics, *etc*. MedWatch plays a critical role in FDA's post marketing surveillance – the process of following the safety profile of medical products after they've begun to be used by consumers. The FDA publishes a weekly FDA Enforcement Report that contains all enforcement actions including recalls, field corrections, seizures, and injunctions. This report is published on the internet at http://www.fda.gov/opacom/Enforce.html. It also maintains MAUDE (manufacturer and user facility device experience database), which contains reports of adverse events involving medical devices.

Depending on the severity of MDR or MedWatch report filed, a defective medical device may have to be recalled. A recall is a method of removing or correcting products that are in violation of laws administered by the Food and Drug Administration (FDA). Filing an MDR or recalling a medical device takes a significant amount of time, effort, and resources on the part of the manufacturer. It can have a negative impact on a device manufacturers' reputation in the marketplace. It may lead to product liability lawsuits, particularly in the US. All this could consequently lead to an adverse impact on sales and profits.

Low reliability can have a significant impact on service, repair, and warranty costs as well. In fact, warranty cost is inversely proportional to the reliability of a medical device. Hence, more and more manufacturers are willing to invest in reliability related tasks to try and reap the benefits in terms of warranty costs. A 5% increase in reliability focused development costs will return a 10% reduction in warranty costs. A 20% increase in reliability focused development costs will typically reduce warranty costs by half and a 50% increase in reliability focused development costs will reduce warranty cost by a factor of 5 [5].

61.2 Government (FDA) Control

As the use of medical devices for critical life supporting functions increases, governments around the world are regulating their design, manufacture, quality, reliability, proper use and disposal. The Food and Drug Administration (FDA) is the US Government agency that oversees most medical products, foods and cosmetics. Within FDA, the Center for Devices and Radiological Health (CDRH) oversees the safety and effectiveness of medical devices and radiation-emitting products.

The FDA is responsible for protecting the public health by assuring the safety, efficacy, and security of human and veterinary drugs, biological products, medical devices, the nation's food supply, cosmetics, and products that emit radiation. The FDA is also responsible for advancing the public health by helping to speed innovations that make medicines and foods safer, and more affordable, and helping the public get the accurate, science based information they need to use medicines and foods to improve their health.

Products regulated by FDA include all foods except meat and poultry, prescription and non-prescription drugs, blood products, vaccines and tissue transplantation, medical devices and radiological products, including cellular phones, animal drug and feed, and cosmetics. In addition to setting product standards, FDA regulates the labeling of products under its jurisdiction. This information must be valid, well documented, and not misleading. FDA plays a major role in protecting consumers and the public health.

The Federal Food, Drug, and Cosmetic Act of 1938 authorized the FDA to take formal or informal regulatory measures against the mis-branding or adulteration of medical devices. Amendments to this act in 1976 empowered the FDA to regulate medical devices during their design and development phases. The Safe Medical Device Act passed in 1990, authorized the FDA to implement the Preproduction Quality Assurance Program. This program requires medical device manufacturers to address deficiencies that lead to failure during design. Nowadays, similar types of regulations concerning medical devices are being followed in other countries. For example, the Medical Device Directive (MDD) of the European Union (EU) outlines the requirements for medical devices in the EU countries.

61.3 Medical Device Classification

The FDA has established three regulatory classes for medical equipment based on the level of control necessary to assure the safety and effectiveness of the device. The class to which a device is assigned determines, among other things, the type of premarketing submission/application required for FDA clearance to market.

Device classification is risk based, that is, the risk the device poses to the patient and/or the user is a major factor in the class it is assigned. All classes of devices are subject to General Controls which are the baseline requirements of the Food, Drug and Cosmetic (FD&C) Act.

The three classes and the requirements that apply to them are:

- Class I: General Controls

Class I devices are subject to the least regulatory control. They present minimal potential for harm to the user and are often simpler in design than Class II or Class III devices. Class I devices are subject to "General Controls" as are Class II and Class III devices. Examples of Class I devices include elastic bandages, examination gloves, and hand-held surgical instruments.

- Class II: General Controls and Special Controls

Class II devices are those for which general controls alone are insufficient to assure safety and effectiveness, and existing methods are available to provide such assurances. In addition to complying with general controls, Class II devices are also subject to special controls. Special controls may include special labeling requirements, mandatory performance standards and postmarket surveillance. Examples of Class II devices include powered wheelchairs, infusion pumps, and surgical drapes.

- Class III: General Controls and Premarket Approval

Class III is the most stringent regulatory category for devices. Class III devices are those for which insufficient information exists to assure safety and effectiveness solely through general or special controls. Premarket approval by FDA, is required for this class of devices. Premarket approval is the required process of scientific review to ensure the safety and effectiveness of Class III devices.

Class III devices are usually those that support or sustain human life, are of substantial importance in preventing impairment of human health, or which present a potential, unreasonable risk of illness or injury.

The reliability activities that need to be performed during the life cycle of a product, depends to some degree on the classification of the product. Class III devices need maximum analyses and testing because they support or sustain human life.

61.4 Reliability Programs

Reliability engineering tools are well established, however, their application to the medical industry is fairly new. The first step in launching a safe and reliable medical product is a good reliability program. What are the hallmarks of a good reliability program? Developing realistic reliability goals early, planning an implementation strategy and then executing the strategy are all key features of a good reliability program.

The four phases of a reliability program are [6].

- The concept phase,
- the design phase,
- the prototype phase, and
- the manufacturing phase.

Several different reliability tools are available for use in the four phases of a reliability program. In the concept phase, one can use benchmarking and gap analyses to develop a reliability program and integration plan.

In the design phase, one can use reliability modeling and predictions, derating analysis/ component selection, worst case circuit analysis, thermal analysis, electromagnetic analysis, design of experiments, risk management/FMECAs, fault tree analysis, human factors analysis and software reliability analysis to increase reliability of a product.

In the prototype phase, one can perform highly accelerated life testing (HALT), design verification testing (DVT), and reliability demonstration testing (RDT).

In the manufacturing phase, the reliability tools that can be used are highly accelerated stress screening (HASS), on-going reliability testing, FRACAS/CAPA system setup, and end-of-life assessment.

61.4.1 The Concept Phase

61.4.1.1 Benchmarking

Benchmarking is the process of comparing the current project, methods, or processes with the best practices in the industry. Benchmarking is crucial to both a startup company as well as an established company that is coming out with a new product to assure the new product is competitive based on reliability and cost. For example, company A, a new entrant into the medical manufacturing market, wants to start selling a new type of dialysis pump. Company A should check the warranty information, annual service plan and recommended maintenance schedule of leading competitor products to try and benchmark their dialysis pump with respect to MTBF, failure rate, service interval, *etc*., against competitor pumps.

61.4.1.2 Gap Analysis

Gap analysis compares your current capabilities with what is expected of your product in the industry. Before performing a gap analysis you have to set a reliability goal and perform a review of your current capabilities. Gap = goals − current capabilities. For example, a ventilator manufacturer currently has a ventilator on the market that has a field reliability of 0.988. It is now planning to add an oxygen blending feature to this ventilator. They would like the new ventilator to have a reliability goal of 0.9999 to meet customer expectation. The process of determining the current capability (0.988), the goal (0.9999), and the gap (0.9999 − 0.988 = 0.0119) is called gap analysis.

The output of this phase is the reliability program. The program generally quantifies out of box failure rate, reliability within warranty period, and reliability throughout life of the product. It also defines a schedule of the different activities that will be performed to achieve your reliability goal.

61.4.2 The Design Phase

61.4.2.1 Reliability Modeling and Predictions

A reliability prediction is a method of calculating the reliability of a product by assigning a failure rate to each individual component and then summing all of the failure rates. Standards such as MIL-HDBK-217, Bellcore, PRISM, CNET, HRD5, *etc*., can be used for reliability predictions. A reliability model presents a clear picture of functional interdependencies and provides the framework for developing quantitative product level reliability estimates to guide design trade-off process. Models are helpful for identification of single points of failure, making numerical allocations, evaluating complex redundant configurations, and showing all series-parallel relationships.

61.4.2.2 Derating Analysis/Component Selection

In MIL-STD-721 derating is defined as using an item in such a way that applied stresses are below rated values. Limitation of electrical, mechanical and environmental stresses is critical to high reliability. One common rule of thumb used in electronics is that 50% derating can decrease the failure rate by 30%. The Telcordia SR332 (reliability prediction procedure for electronic equipment) standard gives derating information. Component selection must be based on the basis of derating analysis. Design engineers should select appropriate component ratings to avoid over-stressing them. In the case of implantable medical devices, biocompatibility and reliability of the material and components should be considered as well, while making component selections.

61.4.2.3 Worst Case Circuit Analysis

Worst case circuit analysis (WCCA) is an analysis technique which, by accounting for component variability, determines circuit performance under a worst case scenario, *i.e.*, under extreme environmental or operating conditions. The output of a WCCA allows an assessment of actual applied part stresses against rated part parameters, which can help ensure the application of sufficient part stress derating to meet design requirements. One of the most critical steps involved in completing a meaningful WCCA is the development of a part characteristic database. This database should contain a composite of information necessary for quantifying sources of component parameter variation. Once these sources have been identified, the database can be used to calculate worst case component drift for critical parameters.

61.4.2.4 Thermal Analysis

Temperature is one of the important variables that impacts system reliability. Therefore, the thermal design of a system must be planned and evaluated carefully. Thermal analysis techniques can be used to evaluate the circuit board, casing, and junction temperatures and check for components that exceed their temperature limits. The analysis can also be used to identify the hot spots and components on the board that designers may modify by various means to eliminate thermal problems. Typical solutions are adding heat sinks, thermal pads, and thermal vias, using thicker ground or power planes, local conduction pads, thermal screws, changing of radiation emissivity by coatings, or relocating components.

61.4.2.5 Electromagnetic Analysis

Electromagnetic compatibility, or EMC means that a device is compatible with (*i.e.*, no interference is caused by) its electromagnetic (EM) environment and it does not emit levels of EM energy that cause electromagnetic interference (EMI) in other devices in the vicinity. A medical device can be vulnerable to EMI if the levels of EM energy in its environment exceed the EM immunity (resistance) to which the device was designed and tested. The different forms of EM energy that can cause EMI are conducted, radiated, and electrostatic discharge (ESD). EMI problems with medical devices can be very complex, not only from the technical standpoint but also from the view of public health issues and solutions. The Center for Devices and Radiological Health (CDRH) encourages manufacturers of electro-medical equipment to use the IEC 60601-1-2 standard, a widely recognized standard issued by the International Electrotechnical Commission, Geneva, Switzerland. The standard provides various limits on emissions and immunity.

61.4.2.6 FMECA

Failure modes, effects and criticality analysis (FMECA) is a reliability evaluation and design review technique that examines the potential failure modes within a system or lower indenture level, in order to determine the effects of failures on equipment or system performance. FMECA uses a "bottom up" approach. This approach begins at the lowest level of the system hierarchy and traces up through the system hierarchy to determine the end effect on system performance. The criticality portion of this method allows us to place a numerical value or rating on the criticality of the failure effect on the entire system or user. After the initial analysis, one can prioritize the failure modes, provide mitigations, reanalyze, rescore and confirm that risks are at an acceptable level. There are several different types of FMEAs. For example, design FMEAs, process FMEAs, functional FMEAs, system FMEAs, *etc*. The basic approach for all the FMEAs is the same. A sample section of a FMEA worksheet is given in Figure 61.1.

61.4.2.7 Fault Tree Analysis

A fault tree analysis is a systematic, deductive methodology for defining a single specific undesirable event and determining all possible reasons or failures that could cause that undesirable event to occur. The undesired event is the top event in the fault tree and is generally a catastrophic or complete failure of the product. Fault trees use concepts of logic gates to determine the overall reliability. In medical devices, patient harm is the most common undesired top event. The results of FTA can be used as a troubleshooting tool during service calls, after the product is available in the market. A sample section of a fault tree is given in Figure 61.2.

System				Potential						FMEA Number					
Subsystem				Failure Mode and Effects Analysis						Prepared By					
Component				(Design FMEA)						FMEA Date					
Design Lead										Revision Date					
Core Team										Page					
											Action Results				
Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls	Det	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Actions Taken	New Sev	New Occ	New Det	New RPN
EEPROM / Store therapy settings	Data Bit Loss	No therapy due to loss of therapy parameter setting	10	Corruption	4	NV RAM BIST	1	40	Store therapy setting in a backup location						

Figure 61.1. Sample Section of a FMEA Worksheet

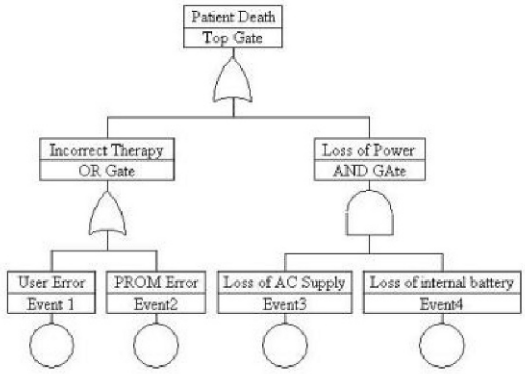


Figure 61.2. Sample section of a fault tree

61.4.2.8 Human Factors Analysis

Human factors analysis should be performed with safety, manufacturing, and maintainability in mind. Human beings are famous for not reading and following instructions. Surrounding distractions is a major concern in the hospital environment. Medical device manufacturers have to make sure that hospital staff is able to use the medical equipment correctly and efficiently in spite of all the other surrounding hospital distractions. They also have to make sure that symbols used on their medical devices meet standards approved by the FDA. AAMI (Association for the Advancement of Medical Instrumentation) has published a technical information report on graphical symbols for electrical equipment in medical practice.

61.4.2.9 Software Reliability Analysis

Software is an important component of medical devices. A software life cycle can be divided into design, coding, and testing. If good practices are followed in all stages of the software life cycle a reliable software product will be ensured. The USAF model and the Mills model are two software reliability models that are generally considered useful for medical devices. The USAF model was developed by the US Air Force Laboratory in Rome, NY. to predict software reliability during the initial phases of the software life cycle. The model begins by developing the predictions of fault density and then transforming them into other reliability measures such as failure rates [7]. The Mills model was developed by H.D. Mills [8] by reasoning that an estimation of faults remaining in software could be made through a seeding process that assumes a homogeneous distribution of a representative class of faults. Before starting the seeding process, fault analysis is performed to determine the expected types of faults in the code and their relative frequency of occurrence [7].

61.4.3 The Prototype Phase

Testing is an important part of any product development cycle. It is performed to verify performance, understand failure modes and weaknesses of the product, benchmark your product against competitor products, determine reliability and safety of the product, and study the impact of stress on performance of the product. Reliability and safety testing is crucial in medical devices.

Testing can be performed in two different modes: standard or accelerated. In standard mode, tests are performed in ambient temperature, at typical operating stress conditions. In accelerated mode, parameters such as temperature, voltage, current, and cycling, are increased well above their normal levels to reduce test times.

In the prototype phase, one can perform highly accelerated life testing (HALT), design verification testing (DVT), and reliability demonstration testing (RDT).

61.4.3.1 HALT

Highly accelerated life testing is a quick and cost effective tool used for discovering design issues and improving design margins. Thermal stress and vibration stress are the two main stresses applied during HALT. Generally a product is subjected to a cold thermal cycle, a hot thermal cycle, a fast thermal transition cycle, a vibration cycle, and a combined thermal-vibration cycle. A root cause analysis is performed at the end of the test to determine the cause of failures. Design and processing changes can be made based on HALT findings. A verification HALT can be performed to ensure that problems are fixed and new problems have not been introduced. For example, during a HALT test, a ventilator with an operating range of 5 C to 40 C, provided incorrect therapy above 35 C and shut down at 65 C. The root cause of failure

was determined to be the temperature rating of a proximal pressure flow sensor. The standard sensor was changed to an extended temperature range sensor to solve the problem. On the same ventilator, the internal battery was disconnecting at very low vibration levels. The battery connector was changed to a positive latch, mini lock type connector to prevent disengagement of the battery. Both the sensor issue and the battery connector issue would not have been discovered before product release if HALT had not been performed.

61.4.3.2 DVT

Design verification testing is performed to verify product functionality. Generally, this testing is performed under normal operating conditions; no external stresses are applied. The results of design verification testing are generally required during pre-market notification 510(k) submittal to the FDA.

61.4.3.3 RDT

Reliability demonstration testing is used to validate reliability prediction analyses and gather a measure of confidence that the released product will achieve a certain reliability target. In this test, a sample of units is tested at slightly accelerated stresses for several months. The stresses are higher than normal operating stress conditions but lower than HALT stress conditions. The stresses are held constant thus enabling you to calculate the acceleration factor for the test. MTBF (mean time between failures) can be obtained from test results. This test is generally performed once before product release.

61.4.4 The Manufacturing Phase

In the manufacturing phase, the reliability tools that can be used are highly accelerated stress screening (HASS), on-going reliability testing, FRACAS/CAPA system setup, and end-of-life assessment.

61.4.4.1 HASS

Highly accelerated stress screening is used to reduce out of box quality returns, decrease field service and warranty costs, and detect and correct process defects. Typical failures that HASS will find are soldering defects, bent IC leads, socket failures, incorrect components or component placement and programming errors. It is recommended that a HALT be performed prior to performing a HASS. HALT will help to identify the operating and destructive limits of a product. This information is essential while developing a HASS process.

61.4.4.2 ORT

On going reliability testing is performed to get an indication of the reliability of the product before it is shipped to customers. In this test, a sample of product is taken off a production line and tested for a period of time, adding the cumulative test time to ensure that the reliability target will be met. The samples are rotated on a periodic basis to get an on-going reliability. One must take care not to wear out any components because these units are shippable units and you cannot risk taking significant life out.

61.4.4.3 FRACAS/CAPA System Setup

Failure reporting and corrective action systems (FRACAS) or corrective and preventive action systems (CAPA) provide a framework for controlling corrective action processes. At its core, FRACAS is a closed loop corrective action system which enables you to collect failure data, analyze data and determine root cause, document the corrective action and implement controls to prevent the reoccurrence of the failure. An integral part of CAPA is a failure review board (FRB). The board is typically a cross-functional group representing quality, reliability, engineering, manufacturing, and regulatory and other departments depending on the nature of the business. The board is responsible for reviewing and approving recommended corrective actions and evaluating effectiveness of corrective actions after implementation. A FRACAS system is essential for medical device manufacturers because of the FDA Medical Device Reporting (MDR) regulations.

61.4.4.4 EOL Assessment

End of life assessment is performed to determine when a product is starting to wear out, whether the

preventive maintenance strategy is effective and whether the predictions performed during design phase were accurate. EOL assessment uses the Weibull plotting technique to figure out where the product is on the bathtub curve. Field failure data is used to determine the number of days before failure.

61.5 Reliability Testing

There are many different reasons for performing reliability testing. The main reasons are to induce failure modes as well as detect unanticipated failure modes so corrective actions can be implemented, to determine if items or system meet reliability requirements, to compare estimated failure rates to actual failure rates, to monitor reliability growth over time, to determine the safety margin in a design, to estimate MTBF or MTTF values, and to identify weaknesses in the design or parts [9].

O'Connor states that reliability testing is a part of an integrated test program involving statistical testing, to optimize the design of the product and the production processes; functional testing, to confirm the design; environmental testing, to ensure that the product can operate under the projected environments; reliability testing, to ensure that the product will operate for its expected life; and safety testing, to ensure safety of the product for use by humans, animals or property [10].

Developing a test plan is the first step of an integrated test program. The Reliability Toolkit provides a test plan outline which includes the following steps: define purpose and scope, list reference documents, and define test item facilities, test requirements, test schedule, test conditions, test monitoring, test participation, failure definitions, test ground rules, and test documentation [11].

Test procedures are required for the proper execution of the test plan. Test procedures must address calibration and proofing the test equipment. They must have a detailed description of the tools, parts, adjustments, hook ups, datasheets, tools, and materials required for the test. The Reliability Toolkit provides a reliability test procedure checklist that includes equipment operation, on/off cycles, operation modes, exercising methods, performance verification procedure, failure event procedure, and adjustments and preventive maintenance schedule [11].

There are several different types of reliability tests that can be performed over the life of the product cycle. Reliability development/growth tests (RD/GT), reliability qualification tests (RQT), performance tests, screening tests, and probability ratio sequential tests (PRST).

61.5.1 The Development/Growth Test

This type of test is run to determine if there is a need to change the design to achieve reliability specification, or to verify improvements occurring in design reliability after changes have been made. These tests are generally run in the prototype or development phase. Estimates of MTTF or MTBF can be obtained from these tests.

61.5.2 The Qualification Test

The objective of this type of test is to determine if a design is acceptable for the intended function. Qualification tests in many cases include aspects of vibration, shock, temperature cycling and other environmental considerations the product will see in use.

61.5.3 The Acceptance Test

Acceptance testing is statistically derived to determine if an item is to be accepted or rejected for use, either individually or on a lot basis. This method of testing does not provide MTBF, MTTF or any other quantifiable measure.

61.5.4 The Performance Test

Performance testing is conducted on completed designs and normally manufactured items to verify the reliability predictions and test results in the preproduction phase. This testing provides a benchmark for comparison of previous activities to see if they are effective in delivering a design that meets reliability requirements.

61.5.5 Screening

Screening tests are performed with the intent of eliminating the infant mortality period. By eliminating infant mortality period, the yield of finished product is improved, and a higher reliability is achieved out in the field.

61.5.6 Sequential Testing

Sequential testing for products designed to operate for some period of time is outlined in MIL-STD-781. These tests called Probability Ratio Sequential Tests (PRST) are based on the ratio of an acceptable MTBF, which should have a high probability of acceptance to an unacceptable MTBF, which should have a low probability of acceptance. Items are placed on test, and failures that occur are plotted against test time. A decision is made based on the plotted point. The decision is one of three, accept the items as meeting the required MTBF, reject the items as not meeting acceptable MTBF, or continue testing.

Sequential test plans provide the least amount of time to make a decision when product is either very good or very bad as compared to reliability requirements. When the product is borderline, testing can be continued for an indeterminate period of time, which is an unacceptable situation. To prevent the tests from continuing indefinitely there are specific truncation points designed in these tests. The test will terminate at either a given amount of failures or a predetermined test time, if a decision has not been made.

61.6 MTBF Calculation Methods in Reliability Testing

MTBF (mean time between failures) is used frequently to assess reliability of a medical product. There are five methods to estimate MTBF in reliability testing [7].

- Time terminated, failed items replaced.
- Time terminated, failed items not replaced.
- Failure terminated, failed items replaced.
- Failure terminated, failed items not replaced.
- No failures.

All the methods assume exponential distribution (constant failure rate). Each method is described below.

61.6.1 Time Terminated, Failed Items Replaced

In this method, testing is terminated at a preassigned time, and all failed items are replaced immediately after their individual failures. MTBF can be calculated using

$$MTBF = MT_d / n, \tag{61.1}$$

where T_d is the test duration time, M is the number of items placed on test and n is the total number of failures. One does not need to record the time to failure of each individual unit on test. For example, a medical device manufacturer places fifteen identical handheld oximeters on test, for 2400 hours. 6 of the 15 oximeters failed in the 2400 hour time period. All failed oximeters are replaced as soon as they fail. An estimate of the MTBF of the tested oximeters can be given by:

$$\begin{aligned} MTBF &= (15)(2400)/6 \\ &\equiv 6000 hours . \end{aligned}$$

Therefore, the MTBF of the oximeters is 6000 hours.

61.6.2 Time Terminated, Failed Items Not Replaced

In this method, testing is terminated at a preassigned time, and the failed items are not replaced. MTBF can be calculated using

$$MTBF = \left\{ \sum_{i=1}^{n} T_i + (M-n)T_d \right\} \Big/ n, \tag{61.2}$$

where T_i is the time to failure, M is the number of items placed on test; T_d is the test duration time and n is the total number of failures. One needs to

record the time to failure of each individual unit on test.

For example, a manufacturer started a test with five identical defibrillators. Two of the five defibrillators failed after 75 and 110 hours. The failed defibrillators were not replaced. The test was terminated at a predetermined time of 500 hours. What is the MTBF of the tested defibrillators?

$$MTBF = \{(75+110)+(5-2)(500)\}/2$$
$$\equiv 842.5 hours .$$

Therefore, the MTBF of the defibrillators is 842.5 hours.

61.6.3 Failure Terminated, Failed Items Replaced

In this method, testing is stopped at a predetermined number of failures, and each failed item is replaced. MTBF can be calculated using

$$MTBF = MT_d / n , \quad (61.3)$$

where T_d is the test duration time, M is the number of items placed on test, and n is the total number of failures. The equations for time terminated and failure terminated are equivalent when failed items are replaced.

61.6.4 Failure Terminated, Failed Items Not Replaced

In this method, testing is terminated at a predetermined number of failures, and the failed items are not replaced. MTBF can be calculated using

$$MTBF = \left\{ \sum_{i=1}^{n} T_i + (M-n)T_d \right\} \Big/ n , \quad (61.4)$$

where T_i is the time to failure, M is the number of items placed on test; T_d is the test duration time and n is the total number of failures.

61.6.5 No Failures Observed

In this method, MTBF cannot be calculated because no failures are observed. However, a lower one-sided confidence limit can be calculated to state the minimum limit of the MTBF for a specified confidence level.

$$LOCL = (2T_t) / \chi^2_{\alpha,m} . \quad (61.5)$$

61.7 Reliability Related Standards and Good Practices for Medical Devices

Nowadays, compliance to certain safety, quality, and usability standards is a pre-requisite to gaining approval from FDA to market a medical device in the USA. There are over 700 medical standards available on different topics for different types of devices. Some standards directly or indirectly related to medical device quality, reliability, safety, and usability are given in Table 61.1.

Table 61.1. Reliability standards

Standard Reference No.	Standard Title/Description
ANSI/AAMI/ISO 14971:2000 and 14971:2000/A1:2003	Medical devices – Application of risk management to medical devices
ANSI/AAMI ES1-1985	Safe current limits for electro medical apparatus
ASTM F1100 – 90	Standard Specification for Ventilators Intended for Use in Critical Care
ASTM F1246 – 91	Standard Specifications for Electrically Powered Home Care Ventilators, Part 1 – Positive Pressure Ventilators and Ventilator Circuits
ASTM F1463	Specification for alarm signals in medical equipment used in anesthesia and respiratory care
ASTM F0792	Guide for computer automation in the clinical laboratory
AAMI EOTP-2/85	Performance evaluation of ethylene oxide sterilizers – EO test packs, good hospital practice
AAMI TIR 12:2004	Designing, testing, and labeling reusable medical devices for reprocessing in healthcare facilities: A guide for medical device manufacturers
AAMI TIR 32:2004	Medical device software risk management
AAMI HE-1988	Human factors engineering guidelines and preferred practices for the design of medical devices
	Guidance for the content of Pre-market Submissions for Software Contained in Medical Devices Issued May 11, 2005 by CDRH
ISO 10651-6	Lung ventilators for medical use – Particular requirements for basic safety and essential performance
ISO 10993-1	Biological evaluation of medical devices – Part 1: Evaluation and testing
ISO 15001	Anesthetic and respiratory equipment – Compatibility with oxygen
ISO 8185:1997	Humidifiers for medical use – General requirements for humidification systems
ISO 9000 series	ISO 9000 series of quality standards
ISO 1348	Quality systems – medical devices – particular requirements for the application of ISO9002
IEC 60601-1-1	Medical Electrical Equipment Part 1: General requirements for safety – Collateral Standard: safety requirements for medical electrical systems
IEC 60601-1-2	Medical Electrical Equipment Part 1: General requirements for safety – Collateral Standard: electromagnetic compatibility.

Table 61.1. Continued

Standard Reference No.	Standard Title/Description
IEC 60601-1-6	General requirements for safety – Collateral Standard: Usability
IEC 60601-1-8	General requirements for safety – Collateral Standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems
IEC 68-2-64	Environmental Testing Part 2: Test methods Test Fh: Vibration, broad-band random (digital control) and guidance
IEC 1123	Reliability testing compliance test plans for success ratio
IEC 605	Equipment reliability testing
UL544	Standard for safety of medical and dental equipment
UL 2601-1	Medical Electrical Equipment, Part 1: General Requirements for Safety
MIL HDBK-338	Electronic reliability design handbook
MIL HDBK 217F	Reliability prediction of electronic equipment
MIL-STD-1629A	Procedures for performing a failure mode, effects and criticality analysis
MIL HDBK-781	Reliability test methods, plans, and environments for engineering development, qualification and production
MIL-STD-2155	Failure reporting, analysis and corrective action system (FRACAS)

References

[1] Borger C, *et al*., Health spending projections through 2015: Changes on the horizon. Health Affairs Web Exclusive W61 2006; 22 February, S.

[2] Pear R., US health care spending reaches all-time high: 15% of GDP. The New York Times 2004; January 9; 3.

[3] Wan H, Sengupta M, Velkoff V, DeBarros K. 65+ in the United States: 2005. U.S. Census Bureau. [online], 2005;1-70. Available: http://www.census.gov/prod/2006pubs/p23-209.pdf

[4] Khan Z. Medical Electronic products call for higher reliability. ECN, 3/1/2005. Available http://www.ecnmag.com/article/CA508377.html

[5] Rand Corporation. The cost and benefits of reliability in military equipment, 1988.

[6] Schenkelberg F. Reliability integration 3-day training course. Ops A La Carte LLC, Oct, 2004.

[7] Dhillon BS. Medical device reliability and associated areas, CRC Press, Boca Raton, FL, 2000.

[8] Mills HD. On the statistical validation of computer programs. IBM Federal Systems Division, Gaithersburg, MD, Report No. 72-6015, 1972.

[9] CRE Primer 1998, Quality Council of Indiana.

[10] O'Connor PDT. Practical reliability engineering. (3rd edition). Wiley, New York, 1996.

[11] Systems reliability division. Rome Laboratory Reliability Engineer's Toolkit: New York. 1993; April.

62

A Tasks-based Six Sigma Roadmap for Healthcare Services

Loon-Ching Tang, Shao-Wei Lam and Thong-Ngee Goh

Department of Industrial and Systems Engineering, National University of Singapore, 1 Engineering Drive 2, Singapore 117576, Singapore

Abstract: Due to the numerous success stories of the Six Sigma quality initiative, it has become a subject of intense study and discussion in both the industry and academia over the past fifteen years. A fundamental tenet behind the success of Six Sigma is the use of structured strategies to achieve well-defined business goals. An enhanced Six Sigma framework, which takes into account the distinctly transactional nature of processes found in an extended healthcare delivery system is proposed here. Critical differences in the key elements of a Six Sigma program between manufacturing and transactional environments are first identified to motivate the proposed framework. The new framework includes some new systems engineering tools that are deemed more effective than the traditional set of Six Sigma tools. A case study is presented to demonstrate the suitability of these tools within the proposed Six Sigma framework.

62.1 Introduction

The management of extended healthcare delivery systems[1] has always been complicated by a variety of systems complexities. These may be a result of numerous external legal-politico and socio-economic influences, and internal interactions arising from a closely knitted, interdependent web of operational activities and human interactions. Dramatic advancements in healthcare technologies in recent years have further introduced un-precedented challenges in the management of such organizations.

Given the complex nature of any extended healthcare delivery system, a recent report by the Institute of Medicine (IOM) [1] recognized that *systems engineering* tools developed for the design, analysis and control of complex systems may possibly help to achieve a high quality healthcare delivery system. The Six Sigma quality initiative appears to be a viable, organizationally effective, and sustainable platform for the introduction of these tools for the improvement of the quality of healthcare processes. Six Sigma programs are designed to adopt a comprehensive systems perspective to achieve breakthrough quality improvements in complex products and processes. Traditional Six Sigma programs already

[1] Extended healthcare delivery system in this article is defined as any medium to large scale healthcare organization, such as hospitals and polyclinics, that offers a comprehensive range of healthcare services.

encompass a compact, yet highly effective set of systems engineering tools ranging from project management and process mapping to statistical quality engineering techniques such as design of experiments (DOE) and Monte Carlo simulation. In order to address various quality issues peculiar to extended healthcare delivery systems, the current Six Sigma framework will need to evolve into one that further underscores the importance of systems modeling and optimization.

A fundamental tenet behind the success of Six Sigma is the use of s*tructured task oriented strategies* to achieve *well-defined goals* [2, 3]. The generic structure of these strategies (or frameworks) is similar in nature. One of the most well-known frameworks is the define-measure-analyze-improve-control (or DMAIC) framework with its unique set of *tasks* to be accomplished within each well-defined execution phase. The DMAIC framework was essentially developed from the manufacturing environment. Within such frameworks, statistical techniques and lean management tools have, in turn, been identified to accomplish the key tasks at each stage of a Six Sigma project.

Other well-known frameworks include the Design for Six Sigma frameworks of identify-design-optimize-validate (IDOV) and define-measure-analyze-design-validate (DMADV). These have been developed for product design and development industry. Although the generic structures of Six Sigma frameworks appear similar in nature as they broadly contain phases that deal with the problem definition, analysis, improvement, and solution implementation, the definition of key tasks within these structured strategies generally has to be translated from the characteristics of different environments. As an example, robust design and reliability engineering are typically more applicable for a product design environment than a manufacturing process. The unique requirements of different industries mandate different definition of key tasks within generic Six Sigma frameworks. The definition of key tasks naturally translates to different toolsets that are deemed most effective for different industrial environment.

The traditional Six Sigma framework was essentially developed from a manufacturing environment. As healthcare delivery systems comprise processes that are typically transactional in nature, an enhanced framework is proposed that can more effectively bridge the gap between the definition and achievement of Six Sigma goals. As a motivation for this framework, critical differences in the key elements of a Six Sigma program between manufacturing and transactional environments are first identified and discussed in the next section. A case study is then presented to demonstrate the effective integration of some new tools within the proposed Six Sigma framework.

62.2 Task Oriented Strategies of Six Sigma

Six Sigma programs are designed with an emphasis on the identification, measurement, reduction, and control of variations found in a realistic environment. The origin of Six Sigma can be attributed to the development of quality programs in Motorola in the 1980s [2]. By clearly specifying a set of proven task-oriented and well-structured strategies built upon sound systems engineering principles and statistical foundations, Six Sigma is seen to be able to effectively enhance profitability by reducing cycle time, defect rate and rework through project-by-project quality improvement efforts.

The potential of Six Sigma in healthcare has been acknowledged by many healthcare researchers and practitioners. A search in scientific healthcare literature through the PubMed database using the keyword “Six Sigma” revealed more than 79 relevant publications since 1995 (see Figure 62.1). There is a growing number of case studies that report successful Six Sigma implementations in the healthcare industry (see, for example, [4]) and consider a wide variety of customer-centric improvement activities directed at operational processes such as in the reduction of medication errors, patient waiting times in radiology department, billing errors, inventory levels, *etc*.

Given the phenomenal success behind Six Sigma, there has been some research that attempts to understand the success factors that drive it. The power behind this program has been attributed to

several critical characteristics [2]. Some theoretical underpinnings based on a goal theoretic perspective that underlie the success behind Six Sigma have also been proposed and investigated by Linderman *et al.* [5, 3]. One of the key propositions behind the goal theoretic framework [3] is the use of well-structured methods to tackle complex process improvement tasks in Six Sigma. The use of such structured methods has always been one of trademarks of Six Sigma and recognized as a key success factor [2].

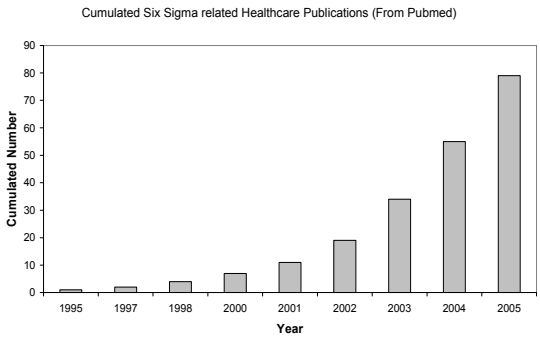


Figure 62.1. Exponential growth of Six Sigma related healthcare publications

There are differently structured Six Sigma methods that comprise generic lists of essential tasks to be fulfilled. A master task list typically found in structured Six Sigma problem solving strategies is given in Table 62.1. The most widely adopted framework is the DMAIC framework. Broadly, the DMAIC framework is a systematic project-based improvement process that essentially contains a project definition phase, process measurement and analysis phases, a process improvement phase, and a process stabilization and control phase executed in a sequential and iterative manner [2]. A classification of tasks in the master task list is given within this framework in Table 62.1.

Apart from the DMAIC framework, there are also other Six Sigma frameworks that have been developed as a result of peculiar characteristics within generic processes (examples include DMADV and IDOV frameworks for product development processes). Regardless of whatever framework Six Sigma is manifested in, a fundamental tenet behind the goal theoretic explanation underlying Six Sigma frameworks is that well-defined goals are supplemented with suitable tasks and tools within well-structured methods that enable the resolution of complex problems existing in the gulf between goal setting and goal achievement [3]. To a reasonable extent, this hypothesis has been empirically verified by Linderman *et al*. [5].

As the DMAIC framework was originally developed for a mass-manufacturing environment, a number of attempts have been made in recent years to adapt this framework to a predominantly service-oriented healthcare delivery environment. In these attempts, a myriad of practical issues

Table 62.1. Master task list in Six Sigma (task classification for DMAIC framework)

Master task list classification for: Define → Measure → Analyze → Improve → Control (DMAIC)				
Define	**Measure**	**Analyze**	**Improve**	**Control**
Understand customer needs	Translate CTQs to KPOVs	Identify KPIVs	Identify possible solutions	Establish control plan
Develop project charter and scope	Collect data on KPOVs	Quantify and analyze KPIVs	Select solution	Implement large-scale solution
Systems identification	Establish baseline		Pilot and optimize solution	Close project

ranging from cultural inertia to human resource capabilities and data generation problems have been identified and dealt with [6, 4, 7]. Such adaptations are in line with the goal theoretic perspective, which advocates the importance for an effective task oriented and structured problem solving methodology to bridge the gulf between goal setting and goal achievement. The need for more effective frameworks adapted to the peculiar needs of different industry sectors is further highlighted and dealt with for the healthcare delivery environment in this paper.

Inadequacies of the traditional DMAIC framework have motivated the authors to re-examine this Six Sigma framework for its suitability in the healthcare delivery environment. To that end, differences in several key elements of Six Sigma programs that are generic for manufacturing and transactional environments are first identified (see Table 62.2). As a consequence of these differences, a new Six Sigma roadmap, fortified with new systems engineering tools and lean concepts underscoring a team based execution strategy, is proposed for the healthcare delivery environment. A case study demonstrating the effectiveness of such a framework is then described.

62.3 Six Sigma Roadmap for Healthcare

A new Six Sigma framework for operational quality and efficiency improvements in healthcare delivery systems is proposed. It consists of five phases, namely, "define", "visualize", "analyze", "optimize" and "verify" (**DVAOV**). A comparison of the key phases and objectives of this framework with the traditional DMAIC framework [2] is shown in Table 62.3. Key systems engineering tools recommended for each of these phases together with key activities and outputs are shown in Table 62.4. In the following sections, the integration of new systems engineering tools into the proposed roadmap would be discussed in detail.

Table 62.2. Differences in key features of traditional and transactional Six Sigma

Key features	Manufacturing Six Sigma	Transactional Six Sigma
CTQs	Clearly defined within a market segment	Difficult to define (presence of substantial ambiguities even within market segments)
Systems Identification	System boundary is easier to define	System boundary difficult to establish (more significant interactions amongst processes and customers)
	Processes are easily identifiable and stable over units produced	Processes are more obscure and sensitive to customer encounters
	Clearly defined downstream customers	Involves multiple internal and external customers or stakeholders
KPIV	Little variability	Substantial variability (Customers interactions are not identical)
	Little human judgment	Usually involves significant human judgment
	Usually controllable	Difficult to control
KPOV	Measurable and quantifiable	May not always be quantifiable
	Usually obtainable from DOE	Can only be obtained from observational data
	Data can usually be modeled by normal distribution	Data is seldom normally distributed
Rework and wastes	Easily measurable	Difficult to quantify
	More obvious attributable causes	Causes are usually not obvious

Table 62.3. Comparison of manufacturing DMAIC with healthcare DVAOV

Manufacturing DMAIC		Healthcare DVAOV	
Phase	**Objective**	**Phase**	**Objective**
Define	Define the problem (including customer impact and potential benefits)	Define	Define the problem and system boundary (including customer impact and potential benefits)
Measure	Identify the CTQs of the product or service. Verify measurement system capability, assess baseline and set improvement targets	Visualize	Achieve a shared vision of the current process; identify CTQs, KPOVs; verify data collection schemes; assess baselines and identify wastes in current process; set improvement targets
Analyze	Understand root causes of defects; identify key process input variable(KPIVs)	Analyze	Understand resource constraints and root causes of defects; identify KPIVs
Improve	Quantify influences of KPIVs on the CTQs; identify acceptable limits of these variables; modify the process to stay within these limits	Optimize	Quantify influences of KPIVs on the CTQs; identify robust solutions that is expected to stay within acceptable target limits
Control	Ensure that the modified process now keeps the key process output variables (KPOVs) within acceptable limits and maintain gains in the long term	Verify	Obtain buying-in and validate recommendation via simulation and pilot run; implement solution and validate results by monitoring performance; replicate improvements to other similar processes

62.3.1 The "Define" Phase

The effective execution of the "define" phase can be considered one of the key success factors of Six Sigma projects. In many instances, the root cause of Six Sigma project failures could be traced back to this important phase. Reasons such as insufficient consultation with stakeholders, lack of commitment amongst stakeholders, vague definitions of requirements, project scope and objectives, mismanaged expectations, poor cost and budget allocations, inappropriate schedule planning, *etc.*, have often been quoted as the reason behind the failure of Six Sigma projects. The key levers for the effective resolution of these problems essentially reside in the "define" phase.

There are typically three key deliverables in the "define" phase (see Table 62.4). They are the business case, project charter, and a detailed project plan. The business case essentially sets down the "WHY's" of the project (reasons or motivations) and is derived in consideration of the key financial, marketing and strategic objectives of the enterprise. The project charter sets out the detailed scope, goals and roadmap ("HOW's") and includes a detailed breakdown of stakeholders involved, budget, schedule and plan.

One of the key complexities peculiar to transactional processes in the "define" phase is the increased difficulty of defining appropriate critical-to-quality characteristics (CTQs), especially as perceived by customers. This arose partly because of the difficulty in defining market segments due to the heterogeneity of customers' expectations of service products. Furthermore, service processes frequently do not have well-defined stakeholders. In order to clarify vague customers' requirements and maintain a system-wide perspective in quality improvement, there is a need to introduce more powerful tools such as the comprehensive service

quality function deployment (CSQFD) described by Dube [8].

The CSQFD proposed by Mazur [9] following Akao [10] and adapted by Dube [8] is more suitable for transactional processes such as healthcare delivery systems than the traditional QFD. There are more widely varying customers' requirements with multiple tangible and intangible quality attributes in transactional environments. The inclusion of the customer deployment (CD) and voice of the customer (VOC) matrices prior to the house-of-quality (HOQ) matrix in CSQFD enables a more systematic means to segment customers with differing expectations, structure customer characteristics and thereby, derive customers' requirements at the HOQ level. The CSQFD approach further emphasizes the need to take into account these customer characteristics and requirements when generating the "HOW's" for subsequent matrices. Such an approach would enable the unique co-production and interpersonal nature of service processes to be addressed more effectively in comparison to traditional QFD approaches.

Table 62.4. Proposed DVAOV framework for healthcare delivery processes

Phase	Key Tasks	Key Tools	Key Outputs
DEFINE	Understand customer's needs Estimate cost savings Selection of projects Planning and scheduling of projects	CSQFD Project management tools Cost analysis Linear Programming	Business Case Project charter Detailed project schedule and plan
VISUALIZE	Understand the current process Benchmark and identify competitive gaps Identify root causes Conduct qualitative risk analysis Design of data collection system and collection of data	Process maps Value stream analysis Gap analysis Cause and effectmMatrix FMEA Statistical sampling techniques, experimental design (DOE)	AS-IS process map VSM Maps CE Diagrams Risk charts Quantitative process data
ANALYZE	Establish and validate statistical assumptions for data collected Evaluate key statistics More detailed estimation of cost savings	Exploratory data analysis (EDA) Statistical hypothesis tests Multi-vari studies Cost analysis Linear models Queuing methodologies Linear programming	Summary of key statistics Detailed cost estimates
OPTIMIZE	Develop key input-output transfer function Evaluate options and propose most effective course of action Performing scenario/ what-if or sensitivity analysis on proposed course of action and alternatives	Response surface methodology Linear programming Queuing methodologies Simulation	Tradeoff analysis charts Preliminary action plans for alternative courses of action
VERIFY	Conduct process simulation Implement pilot process and collect data Validate improvement plans Establish SOPs and process control plans Communicate SOPs to other similar processes	Statistical process control Process capability analysis Simulation	Control plans Actual implementation plan New process SOPs Replication plans

Apart from the comprehensive CSQFD approach suitable for transactional processes, powerful mathematical programming techniques such as linear programming (LP) can be applied for tasks of project selection and management in the "define" phase. The LP modeling structure is general enough that many real-world problems of varying degrees of complexity, particularly in the domain of resource allocation problems, can be easily modeled and optimized. The use of LP for project selection with an integrated consideration of project costs and budget through an improved quality function deployment (QFD) based framework is discussed by Tang and Paoli [11].

62.3.2 The "Visualize" Phase

In view of the fact that transactional environments are characterized by processes that often involve many stakeholders participating in the service delivery process at close proximity to the customers, a new "visualize" phase is proposed. In this phase, critical elements of the original "measure" phase are retained with an additional emphasis on achieving a common vision of current processes. A shared vision is particularly important as it facilitates the inclusion of important stakeholders through a team-based approach to problem-solving. A common understanding of the current processes will help to mitigate some difficulties faced in a transactional environment, such as the identification of systems boundary and task elements. It will also facilitate consensus building and critical stakeholders' buy-in on new process standards and targets and in replicating improvements to other processes.

In order to achieve the goals of the new "visualize" phase, various visual tools such as mindmaps [12] or the current and future reality trees (CRT and FRT) from the theory of constraints advocated by Goldratt [13, 14] can be used to complement existing tools in the original "measure" phase. Here, a powerful visualizing technique that has its roots in lean thinking is proposed. This is the value stream mapping (VSM) approach. Such an approach not only serves as an effective tool to satisfy the key goals of the "visualize" phase, it also contains information essential for the downstream analyze and optimize phases. An updated VSM further allows the effective dissemination of process goals and replication of the improvements to other similar processes.

The VSM approach is well-documented in [15–17] and has been used in a variety of industries [18–21] including the healthcare industry [19]. A VSM process is usually carried out in a cross-functional team-based environment that synthesizes the perspectives and needs of relevant stakeholders representing different organizational elements [17]. One of the key strengths of VSM lies in its ability to provide a clear visual examination of an entire system, which facilitates the consideration of different stakeholders' perspectives. The characteristics of customer demands would translate to the products or service processes that should be mapped. Issues related to processes which do not contribute to the value of a final manufactured product or service process (known as "wastes" or "muda" [22, 16]) can then be identified and considered in a team-based environment. System boundaries defining the scope of each Six Sigma project and clarifying improvement objectives can also be clearly identified as VSM essentially involves an external to internal mapping process. The external value stream maps are living documents updated from feedback gained from each individual Six Sigma project. The construction of value steam maps is typically modular in nature. If the external value stream maps of an enterprise have been created and updated, it will only be necessary to focus on the detailed internal value stream maps within a particular Six Sigma project. This would enable Six Sigma project teams to maintain focus on the key processes at hand, whilst not losing sight of the big picture. VSM is a key enabler for effective root-cause and risk analysis using tools such as cause and effect diagrams and FMEA.

62.3.3 The "Analyze" and "Optimize" Phases

The objectives of the "analyze" and "optimize" phases are essentially similar to the original "analyze" and "improve" phases in traditional manufacturing Six Sigma. New systems engin-

eering tools are added to these two phases to effectuate optimization of processes unique to transactional environments. These new tools are queuing methodologies and linear programming (LP). The integration of these tools into the new DVAOV Six Sigma framework is shown in Table 62.4.

Queuing analysis directly deals with the quality of the service process in terms of servers' efficiency and effectiveness and has been effectively applied in a wide variety of service industries such as banking, healthcare, telecommunications, *etc*. Such analyses are well-suited for the analysis of various healthcare delivery processes as its very concern is in the study and improvements of systems which are subject to uncertain occurrence of demands and duration for the satisfaction of these demands. Service quality in healthcare delivery systems is often related to the length of delay before receiving the service which is directly influenced by the uncertainty in demand occurrence and duration of service performance. Queuing methodologies have been widely employed to solve a large variety of resource management problems such as those related to drug dispensing, admission management, specialist clinic scheduling (see, for example, [23, 24]). Given the stochastic considerations of queuing methodologies, it can also be effectively coupled with statistical theory in survival analysis for longer term management of clinical resources.

Linear programming (LP) was introduced in the preceding discussion of the "define" phase for the selection of projects and allocation of resources for project execution. In practical applications, LP is commonly related to the optimal allocation of limited resources or optimal asset management. Given such general applicability, LP can thus be deployed in various phases of the Six Sigma process. It can also be deployed in the "improve" phase for selecting the best options for quality or productivity improvements. Sensitivity analysis associated with LP further allows the evaluation of different improvement alternatives.

In typical real-world scenarios, Six Sigma project teams usually have to deal with the optimization of multiple conflicting objectives, such as in minimizing costs or resource usage and maximizing quality (or minimizing the number of defects or delays), the ability to meet a target response whilst maintaining an acceptable level of process variations, *etc*. Such multiple objectives optimization problems under the RSM framework has been effectively dealt with using various different multiple objective programming techniques, such as goal programming techniques [25]. Under a linear programming formulation, multiple objective linear programming frameworks (MOLP) provides a particularly favorable alternative for the generation of multiple Pareto optimal choices for deliberations by Six Sigma teams [26].

62.3.4 The "Verify" Phase

The "control" phase is replaced by a "verify" phase. Essentially, the elements of the design and implementation of control measures are retained. The *validation* and *replication* of new improved processes are highlighted in this framework. Due to the strong interpersonal nature of service processes and close interactions between producers and consumers of services, there is an added emphasis on a comprehensive validation scheme, which typically requires some form of process simulation prior to pilot implementation. The VSM output from the "visualize" phase coupled with properly validated results are expected to ease this process. The replication of validated improvements to other similar processes within the healthcare organization has also been instituted. Usually processes of similar nature can be found within an extended healthcare organization (*e.g*., multiple pharmacies (central and satellite pharmacies) existing within a single hospital). The effective deployment of improved processes will allow maximal benefits to be harvested from a single Six Sigma project.

One of the key success factors in this phase for the new framework is still a successful application of *statistical process control* (SPC). The ultimate goal of SPC is for continual improvement of processes (whether transactional or manufacturing). SPC has reportedly been used in the healthcare industry since the 1950s [27] and is equally applicable to both clinical and non-clinical healthcare processes [28–31]. Many recent innovations in

SPC charting tools have been found to be useful in healthcare processes. Some prominent examples are the *g* and *h*-type control charts for monitoring the number of cases between hospital acquired infections or other adverse healthcare events [32–34]. As many additional complexities encountered in SPC data in healthcare processes (cyclic/ trending behaviors, autocorrelation, correlated processes, *etc.*) are also typical of other industries, some recent innovations in SPC chart technology for other industries (such as for high yield manufacturing processes [35, 36]) would be useful.

62.4 Case Study of the Dispensing Process in a Pharmacy

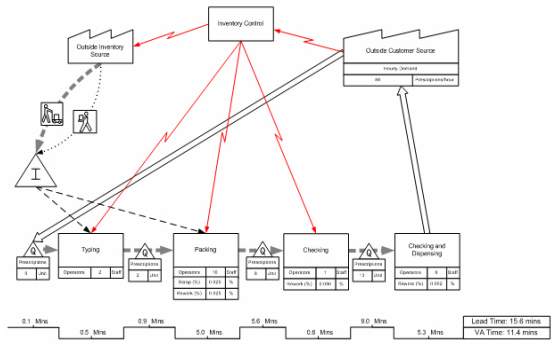
The objective of the project in this case study is to investigate the waiting times in an outpatient pharmacy of a large hospital. The investigation was prompted by complaints about the long waiting times required before drug prescriptions were dispensed. As there are multiple satellite pharmacies with similar processes to the outpatient pharmacy, the project will be able to reap benefits beyond this particular department. The success of this project would enable the Six Sigma team to garner more extensive buy-in and support from the management and other hospital staff. This is essential for sustainable implementation and successful execution of future Six Sigma projects.

A present value stream map depicting the existing situation was generated in the "visualize" phase using VSM tools. The team members provided initial estimates of the arrival rates of patients, service and rework rates. These were updated after they identified the data requirements and designed appropriate data collection strategies to obtain more accurate estimates. A simple example of such a value stream map is shown in Figure 62.2. Queuing analysis was used estimate the expected queue lengths and waiting times. The entire process can be represented by the open queuing network shown in Figure 62.3. Steady state queuing analysis is adequate here as the arrival and service rates are fast enough to ensure the system reaches its steady state in a short time. Some useful queuing results used are shown in Table 62.5. Mean waiting times of each service station can be computed from Little's theorem [37].

Table 62.5. Simple queuing results for Markovian arrival and service processes

Type of service station*	Mean queue length of service station *i*	Utilization, ρ_i	Nomenclature
M/M/1	$\frac{\rho_i^2}{1-\rho_i^2}$	$\rho_i = \frac{\lambda_i}{s_i \mu_i}$	λ_i : Mean arrival rate to the queuing system μ_i: Mean service rate by the server s_i: Number of servers
M/M/s	$\frac{(s_i\rho_i)^{s_i}\rho_i P_{i,0}}{s_i!(1-\rho_i)^2}$ where, $P_{i,0} = \left[\sum_{n=0}^{s_i-1}\frac{(s_i\rho_i)^n}{n!} + \frac{(s_i\rho_i)^{s_i}}{s_i!(1-\rho_i)}\right]$		

* *M/M/1* and *M/M/s* are standard abbreviations to characterize service stations in queuing methodologies. Both of these two types of stations experience Markovian arrival and service processes with infinite queuing capacity and FCFS service discipline. *M/M/s* system has s independently and identically distributed servers.



Rework Proportions		
	Typing	Packing
Packing	0.025	
Checking	0.025	0.025
Dispensing	0.001	0.001

Figure 62.2. Value stream map and rework proportions for a drug dispensing process

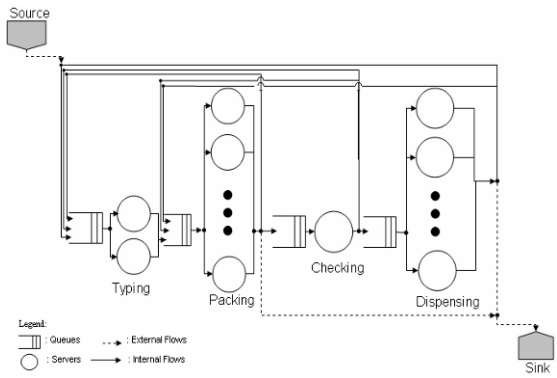


Figure 62.3. Queuing network representation of a drug dispensing process

The mean total waiting times for the entire drug dispensing process in the pharmacy can be computed by summing up the mean waiting and service times at each service station. The mean total waiting time for the entire process did not include the mean service time of the final dispensing and checking process. For the computations of mean total waiting times, the arrival rate at each queuing station, i, at statistical equilibrium can be derived from:

$$\lambda_i = \lambda_{i,0} + \sum_{j=1}^{N} \lambda_j p_{ji} , \qquad (62.1)$$

where

N : The number of queuing stations in the network.

$\lambda_{i,0}$: The arrival rate to station i from external sources.

p_{ji} : The probability a job is transferred to the jth node after service is completed at the ith node. p_{ji} hence represents the rework proportion after each process.

Due to concerns regarding the exponential assumption on service time distribution, an additional analysis was conducted with the assumption of service processes following any general distributions (*M/G/1* and *M/G/S* queuing systems). This serves to demonstrate that the assumption of exponentially distributed service times would result in more conservative system design choices. Each service station i, was assumed to experience a Poisson arrival process in the preceding analysis. Service stations with single and multiple servers were assumed to experience service processes that follow any general distributions, which are independently and identically distributed. The mean waiting queue lengths of each station can be computed using results shown in Table 62.6 [38, 39].

The mean waiting times for these stations can again be computed using Little's theorem [37]. The mean total waiting time for the entire process can be computed by summing up mean waiting and mean service times at each service station. Figure 62.4 shows the difference in mean waiting times computed with and without exponential service time assumptions across different number of packers. The mean total waiting times were observed to be higher with exponential distributional assumptions. In general, the exponential assumption usually results in more conservative system designs. Decisions based on mean waiting times and queue lengths predicted from such models would thus err on the safe side.

Table 62.6. Queuing results for *M/G/1* and *M/G/S* queuing stations

Type of service station	Mean queue length of service station *i*	Nomenclature
M/G/1	$\frac{\rho_i^2}{1-\rho_i}\cdot\frac{\left(1+\psi_i^2\right)}{2}$	ρ_i : Utilization factor ($\rho_i = \frac{\lambda_i}{s_i\mu_i}$)
M/G/s *	$\frac{1}{\lambda_i}\left(\psi_i^2\overline{W}_i^{M/M/s} + \left(1-\psi_i^2\right)\overline{W}_i^{M/D/s}\right)$	λ_i : Mean arrival rate to the queuing system
	where	μ_i: Mean service rate by the server
	$\overline{W}_i^{M/D/s} = \frac{1}{2}\cdot\frac{1}{K_i}\cdot\overline{W}_i^{M/M/s}$	s_i: Number of servers
		ψ_i^2: Squared coefficient of variation of service times, T_i.
	$K_i = \left(1+(1-\rho_i)(s_i-1)\frac{\sqrt{4+5s_i}-2}{16\rho_i s_i}\right)$	

* $\overline{W}_i^{M/M/s}$ is the mean waiting time of an *M/M/s* queuing system and $\overline{W}_i^{M/D/s}$ is the mean waiting time of an *M/D/s* queuing system with Markovian arrival and deterministic service processes.

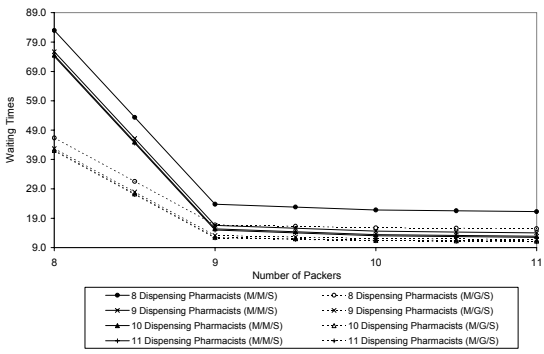


Figure 62.4. Comparisons of mean total waiting times computed with and without exponential service time assumptions

62.4.1 Sensitivity Analysis

In the "optimize" phase, the impact of different systems configurations on the overall waiting times can be assessed by varying the number of packers and dispensing pharmacists through a sensitivity analysis. It was observed that the waiting times are observed to be relatively stable with number of packers above 8. Figure 62.5 shows this result over the different numbers of dispensing pharmacists.

Root cause analysis (RCA) was also performed with the value stream maps to elicit more improvement opportunities. From the RCA (see for Ishikawa diagram in Figure 62.6), it was suggested that a new screening process be implemented at the point when the pharmacy receives prescriptions from patients as this would help to alleviate problems associated with errors in prescriptions and medicine shortages.

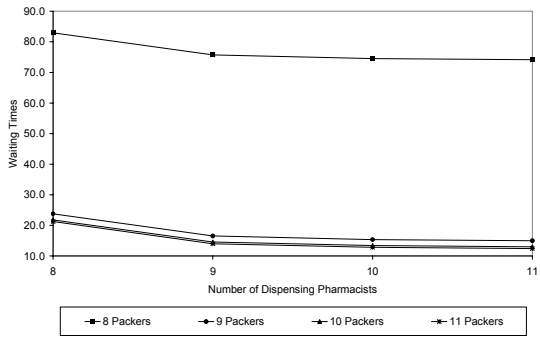


Figure 62.5. Sensitivity of total waiting times to different system configurations

Table 62.7. Comparisons of sojourn times for each process and mean total waiting times

Type of job	W/o screening	With screening
Screening	0	2.6 (1 pharmacist)
Typing	0.6 (2 typists)	0.6 (2 typists)
Packing	5.9 (10 packers)	5.6 (10 packers)
Checking	6.2 (1 pharmacist)	5.0 (1 pharmacist)
Dispensing and checking	9.0 (8 pharmacists)	2.0 (7 pharmacists)
Mean total waiting time	21.7	15.8

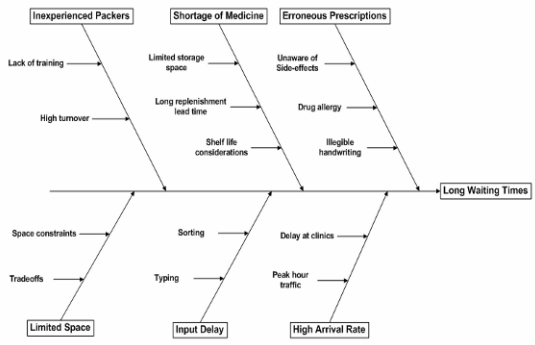


Figure 62.6. Root cause analysis of long waiting times with fish-bone diagram

A pilot run was implemented on the existing process with one dispensing pharmacist moved to the newly implemented screening process. Table 62.7 shows the improvements in the average sojourn times (sum of waiting and service times) of each process and the mean total waiting time computed. Improvements can be observed in the new process because many interruptions that occurred during the dispensing process were effectively reduced by an additional screening process upfront. As a result, the productive time of

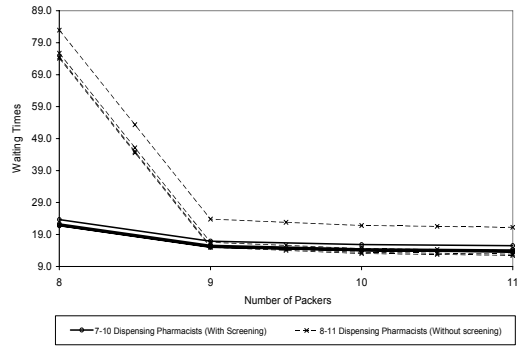


Figure 62.7. Sensitivity of total waiting times for the process with screening

pharmacists increased and the mean queue length in front of the dispensing process shortened from 13 to 3.

Various possible system configurations were experimented with a different number of packers and dispensing pharmacists with the additional screening process. From the analysis, the proposed new configuration was found to be more robust to changes in manpower deployment over the packing and dispensing sub-processes (see Figure 62.7). Eventually, this new robust design was adopted to ensure waiting time stability over possible variations in manpower deployment.

Process validations on results generated have been dealt with throughout the "analyze" and "optimize" phases in the preceding discussions. At the final "verify" phase, standard operating procedures (SOPs) were put in place in order to ensure stability of new processes. Several new control measures were proposed by the team and implemented with the understanding and inputs from the relevant stakeholders.

62.5 Conclusions

A new Six Sigma framework for extended healthcare delivery systems is proposed in this article. Several new systems engineering tools such as CSQFD, VSM, LP, and queuing analysis are proposed within this framework. A case study demonstrating the application of this roadmap for improving the waiting times in a retail pharmacy is

also presented. The proposed Six Sigma framework and its accompanying tools are expected to be more suitable for the myriad of transactional processes (*e.g.*, drug dispensing, radiological, admission, and laboratory services) found in healthcare delivery systems.

References

[1] Reid PP, Compton WD, Grossman JH, Fanjiang G. Building a better delivery system: A new engineering/ health care partnership: Committee on Engineering and the Health Care System, Institute of Medicine and National Academy of Engineering; 2005.

[2] Goh TN, Tang LC, Lam SW, Gao Y. Six Sigma: A SWOT analysis. International Journal of Six Sigma and Competitive Analysis 2006:Accepted for publication.

[3] Linderman K, Schroeder RG, Zaheer S, Choo AS. Six Sigma: A goal-theoretic perspective. Journal of Operations Management 2003; 21(2):193–203.

[4] Revere L, Black K. Integrating Six Sigma with total quality management: A case example for measuring medication errors. Journal of Healthcare Management 2003; 48(6):377–391.

[5] Linderman K, Schroeder RG, Choo AS. Six Sigma: The role of goals in improvement teams. Journal of Operations Management 2005: Accepted for publication.

[6] Benedetto AR. Adapting manufacturing-based Six Sigma methodology to the service environment of a radiology film library. Journal of Healthcare Management 2003; 48(4):263–280.

[7] Woodard TD. Addressing variation in hospital quality: Is Six Sigma the answer? Journal of Healthcare Management 2005; 50(4):226–236.

[8] Dube L, Johnson MD, Renaghan LM. Adapting the QFD approach to extended service transactions. Journal of Production and Operations Management 1999; 8:301–317.

[9] Mazur G. Comprehensive service quality function deployment. Ann Arbor, MI: Japan Business Consultant, Ltd; 1993.

[10] Akao Y. QFD: Integrating customer requirements into product design. Cambridge, MA.: Productivity Press; 1990.

[11] Tang LC, Paoli P. A spreadsheet-based multiple criteria optimization framework for quality function deployment. The International Journal of Quality and Reliability Management 2004; 21(2/3):329–347.

[12] Buzan T. The mind map book: how to use radiant thinking to maximize your brain's untapped potential. Toronto, Plume; 1996.

[13] Goldratt EM. Theory of Constraints. Great Barrington, MA: North River Press; 1999.

[14] Goldratt EM, Cox J. The goal. Great Barrington, MA: North River Press; 2004.

[15] Hines P, Taylor D. Going lean – A guide to implementation. Cardiff: Lean Enterprise Research Centre; 2000.

[16] Liker J. The Toyota way – 14 management principles from the world's greatest manufacturer: New York: McGraw-Hill; 2004.

[17] Lovelle J. Mapping the value stream. IIE Solutions 2001; 33(2):26–33.

[18] Arbulu RJ, D.Tommelein I, D.Walsh K, Hershauer JC. Value stream analysis of a re-engineered construction supply chain. Building Research and Information 2003; 31(2):161–171.

[19] Condel JL, Sharbaugh DT, Raab SS. Error-free pathology: Applying lean production methods to anatomic pathology. Clinical Laboratory Medicine 2004; 24(4):865–99.

[20] Haque B, James-Moore M. Applying lean thinking to new product introduction. Journal of Engineering Design 2004; 15(1):1–31.

[21] Melton T. The benefits of lean manufacturing – What lean thinking has to offer to process industries. Chemical Engineering Research and Design 2005; 83(A6):662–673.

[22] Hines P, Rich N. The seven value stream mapping tools. International Journal of Operations and Production Management 1997; 17(1):46–64.

[23] Joy M, Jones S. Transient probabilities for queues with applications to hospital waiting list management. Health Care Management Science 2005; 8:231–236.

[24] Marshall A, Vasilakis C, El-Darzi E. Length of stay-based patient flow models: Recent developments and future directions. Health Care Management Science 2005; 8:213–220.

[25] Tang LC, Kai X. A unified approach for dual response surface optimization. Journal of Quality Technology 2002; 34(4):437–447.

[26] Lam SW, Tang LC. Multiobjective Vendor allocation in multiechelon inventory systems. Journal of the Operational Research Society 2006; 57(5):561–578.

[27] Levey HS, Jennings ER. The use of control charts in the clinical laboratory. American Journal of Clinical Pathology 1950; 20:1059–1066.

[28] Benneyan JC, Lloyd RC, Plsek PE. Statistical process control as a tool for research and health care improvement. Journal of Quality and Safety in Health Care. Dec. 2003; 12(6): 458–464.

[29] Benneyan JC. Statistical quality control in infection control and hospital epidemiology.Part 1: Introduction and basic theory. Part 2: Chart use, statistical properties, and research issues. Infection Control and Hospital Epidemiology 1998; 19(3):194–214.

[30] Woodall W. The use of control charts in health care and public health surveillance. Journal of Quality Technology 2006; 38(2):89–134.

[31] Benneyan JC, Kaminsky FC. Another view on how to measure health care quality. Quality Progress 1995:120–124.

[32] Benneyan JC. Number-Between *g*-type Statistical Quality control charts for monitoring adverse events. Health Care Management Science 2001; 4:205–318.

[33] Benneyan JC. Performance of number-between *g*-type statistical control charts for monitoring adverse events. Health Care Management Science 2001; 4:319–336.

[34] Kaminsky FC, Benneyan JC, Davis RD, Burke RJ. Statistical control charts based on a geometric distribution. Journal of Quality Technology 1992; 24(2):63–69.

[35] Tang LC, Cheong WT. On establishing CCC charts. International Journal of Performability Engineering 2006; 1(1):5–22.

[36] Tang LC, Cheong WT. A control scheme for high-yield correlated production under group inspections. Journal of Quality Technology 2006; 38(1):45–55.

[37] Little J. A proof of the queueing formula. Operations Research 1961; 9(3):383–387.

[38] Ross SM. Introduction to Probability models. 8th ed. New York: Academic Press; 2003.

[39] Cosmetatos GP. Some approximate equilibrium results for multi-server queue (M/G/r). Operational Research Quarterly 1976; 27(3(1)):615–620.

63

Status and Recent Trends in Reliability for Civil Engineering Problems

Achintya Haldar

University of Arizona, Tucson, AZ, USA

Abstract: Civil engineering is one of the oldest engineering disciplines and has over 5000 years of glorious history. However, only recently, in the mid 1960s, have attempts been made to consider the presence of uncertainty in civil engineering problems. Structural engineering has provided leadership in developing the necessary mathematics and the related design guidelines. Several reliability evaluation methods, including the Monte Carlo simulation technique, are discussed in this chapter and elaborated with the help of examples. A stochastic finite element approach is presented to estimate reliability, particularly when the limit state or performance function is implicit. Finally, recent trends in the the use of reliability techniques in civil engineering problems are discussed. It is necessary to have readily available sophisticated computer programs for reliability analysis. Cognitive sources of uncertainty also need to be incorporated. Developments of meshless methods, robust and stochastic optimization techniques, structural health assessment, monitoring, and maintenance programs, better prediction of future extreme events like earthquake, wind, draught, tornado and tsunami, and system reliability procedures are advocated.

63.1 Introduction

Civil engineering profession has a well documented 5000 years of glorious history. It is one of the oldest engineering disciplines. Our forefathers built civil engineering systems, including shelters, water distribution systems, *etc*., based on intuition. Structures made with stone and mud or with other available materials from nature were built, say, around 3000 BC, before the construction of pyramids. The first structure where technology was used may be the pyramids. The Step Pyramid at Saqqara was built by Imhotep in 2750 BC.

Experience, intuition, and empirical rules might have played very crucial role at this early stage of development. Stone and masonry were primary materials used for construction. The Parthenon was built in 438 BC and is an outstanding example of earlier development. Then Aristotle (384–322 BC) and Archimedes (287–212 BC) helped to formulate the mathematics behind our wonderful history.

The success also demonstrated some weaknesses in our understanding. Observing hazards or failures, Hammurabi, the king of Babylonia, who died in about 1750 BC, issued building code provisions. They were carved in stones and can be seen in the Louvre in Paris. They addressed many different issues including economic provisions (prices, tariffs, trade, and commerce), family law (marriage and divorce), criminal law (assault,

theft), and civil law (slavery, debt). Penalties varied according to the status of the offenders and the circumstances of the offenses. Interpreting the laws in the context of civil engineering, it can be concluded that the responsibilities of the builders were defined depending on the consequences of failure. We cannot afford to have similar codes at present.

In the last 500 years, the mathematical aspects of civil engineering have improved significantly due to the contributions of many scholars including Leonardo da Vinci (1452–1519), Galileo (1564–1642), Andrea Palladio (1518–1580), Robert Hooke (1635–1703), Johann Bernoulli (1667-1748), Daniel Bernoulli (1700–1782), Leonard Euler (1707–1783), Charles Augustine de Coulomb (1736–1806), Louis Navier (1785–1836), Squire Whipple (1804–1888), Karl Culmann (1821–1881), J.W. Schwedler (1823–1894), Benoit-Paul-Emile Clapeyron (1799–1864), James Clerk Maxwell (1831–1879), Otto Mohr (1835–1918), Alberto Castigliano (1847–1884), Charles E. Greene (1842–1903), H. Muller-Breslau (1851–1925), August Foppl (1854–1924), G. Maney (1888–1947), Hardy Cross (1885–1959), R. Southwell (1888–1970), and others. Haldar [1] and West [2] discussed the subject in more detail elsewhere. There is no doubt that civil engineering has a long, proud history. Where do we go from here?

63.2 The Need for Reliability-based Design in Civil Engineering

In spite of our best efforts; we cannot build a failure-proof structure. Our inability to predict the future loading conditions and structural strength are some of the major reasons. Freudenthal [3] is considered to be one of first scholars who advocated for the incorporation of the reliability-based design concept in civil engineering practices. The area has expanded tremendously since then. Benjamin and Cornell [4], and Ang and Tang [5, 6] discussed the chronological developments in the related areas. An extensive list of related publications is given by Haldar and Mahadevan [7, 8].

In civil engineering, the structures group provided leadership in the recent past in developing the risk-based design concept. In structural engineering, there are many design codes based on the material to be used (concrete, steel, wood, masonry, *etc*.), types of structures (buildings, bridges, on-shore, off-shore, *etc*.), and types of loading (earthquake, wind, flood, underground, on ground, *etc*.). Almost all of these codes were modified based on the current design philosophy, *i.e.*, risk-based design concept [9–13]. In the following sections, the development of the risk-based design concept in civil engineering in the context of structural engineering is emphasized.

63.3 Changes in Design Philosophies – Design Requirements

In all engineering designs, the basic concept is that the capacity, resistance or supply should at least satisfy the demand. The demand is defined depending on the area of application. It may be the load effect on a structure, the completion time for a construction project, the traffic on a highway, recommended air or water qualities by a regulatory agency, *etc*. However, since most of the parameters in supply and demand are full of uncertainties, they cannot be predicted with certainty, and thus satisfactory performance cannot be assured. Instead, assurance can only be given in terms of the probability of success in satisfying some performance criterion. In engineering terminology, the probabilistic assurance of performance is referred to as *reliability*.

The presence of uncertainty is always considered in civil engineering design in the form of a safety factor applied to the load, resistance, or both. Before the introduction of the load and resistance factor design (LRFD) concept by the American Institute of Steel Construction (AISC) in 1986 [14], the allowable stress design (ASD) was used by the profession [15]. In ASD, the allowable stresses were calculated using a safety factor. It considered the unfactored nominal loads or load combination, producing the nominal load effect S_n. The allowable resistance R_a was calculated by dividing the nominal resistance R_n by a safety

factor. The acceptable design required that S_n be less than R_a. Then, the profession realized that the loads are more unpredictable than the resistance. This led to the use of the ultimate strength design (USD) concept [9]. In USD, the loads are multiplied by load factors representing the uncertainty in them, producing the ultimate load effect. The safe design required that R_n is greater than the ultimate load effect. However, uncertainty is expected in both the load and resistance parameters. This led to the development of the LRFD concept. The LRFD design guidelines developed by the AISC are based on numerous fundamental assumptions and the load and resistance factors are selected in such a way that would satisfy an underlying risk, although unknown to most design engineers [7, 14, 16, 17]. The basic drawback of the LRFD approach is that it fails to give options to engineers to design for other underlying risks that are not considered in the development of the design guidelines. For example, the underlying risk for a nuclear power plant, a multi-story building, or a temporary structure, does need to be the same, and the corresponding load and resistance factors should be adjusted to reflect this. However, it cannot be done at present.

A more advanced form of risk-consistent design known as the performance based design (PBD) is now being advocated. Engineering designs must satisfy numerous strength and serviceability-related performance criteria. A strength failure may lead to failure. However, serviceability failure (excessive lateral, interstory, or vertical deflection, unwanted vibration, *etc*.) may not lead to failure and thus may not need to satisfy the more demanding strength criteria. In PBD, design engineers will have options to consider numerous performance criteria satisfying the corresponding specified acceptable risks. This may produce more economical design than LRFD and other deterministic approaches. However, the PBD concept is now in the elementary stage of its development.

63.4 Available Analytical Methods – FORM/SORM, Simulation

If a design needs to satisfy specific risks, procedures must be available to estimate them and they should be acceptable to all concerned parties. The risk-based design concept has been under development since the 1960s, as briefly discussed next.

Without losing any generality, let us assume that R represents the resistance and S represents the load effect on a structural element to be designed. R and S cannot be predicted with certainty and should be considered as random variables. They can be represented by their corresponding probability density functions (PDFs), denoted by $f_R(r)$ and $f_S(s)$, respectively. They are shown in Figure 63.1. A PDF is completely defined in terms of its underlying distribution and the parameters of the distribution. In most cases, the parameters of the distribution can be evaluated from the information on the mean, standard deviation, and coefficient of variation (COV) of the underlying random variable. Since absolute safety cannot be assured, a safe design requires that R is greater than S with some pre-selected safety level. This concept can be mathematically expressed as [7]:

$$\begin{aligned} P(\text{failure}) &= P(R < S) \\ &= \int_0^\infty \left[\int_0^s f_R(r)\, dr \right] f_S(s)\, ds \\ &= \int_0^\infty F_R(s)\, f_S(s)\, ds \end{aligned} \tag{63.1}$$

where $F_R(s)$ is the cumulative distribution function (CDF) of R evaluated at s. This is considered to be the fundamental equation of the reliability-based design concept. The shaded area in Figure 63.1 qualitatively represents the probability of failure and gives the physical interpretation of (63.1). Haldar and Mahadevan [7] discussed in detail that by shifting the locations of the two PDFs (locations of the mean values of R and S, *i.e.*, μ_R and μ_S, considering the dispersions of the two PDFs (in terms of standard deviation of R and S, *i.e.*, σ_R and σ_S), and the PDFs themselves [$f_R(r)$ and $f_S(s)$], the shaded

area can be manipulated and the corresponding risk can be estimated. Obviously, a smaller area will represent safer design, and the area cannot be zero, at least conceptually.

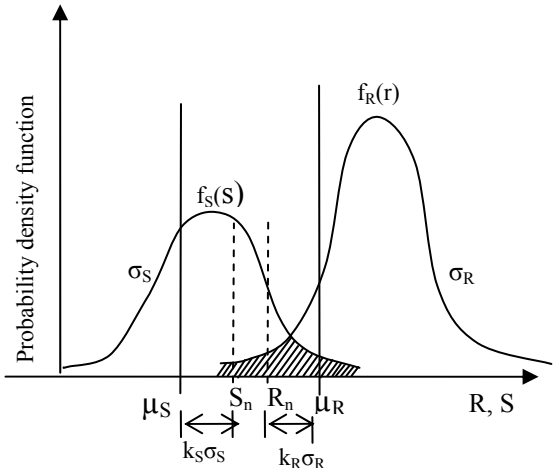


Figure 63.1. Reliability based design concept (from [7])

In general, (63.1) cannot be evaluated in close form for multiple random variables, except for some special cases [7]. Several methods of various degrees of sophistication were developed to address this fundamental problem. To make the discussion more general, *R* and *S* need to be represented by numerous basic random variables; essentially the resistance and load-related random variables present in a particular problem. Reliability or probability of failure is always estimated with respect to a performance criterion or limit state. Thus, besides the basic random variables, the demand or the performance requirement, generally given in design guidelines, should also be a component of a limit state. Generally, a limit state function is represented as:

$$Z = g(\mathbf{X}) = g(X_1, X_2, \cdots, X_n) \qquad (63.2)$$

where X_i's are the *i*th random variable in the limit state. When $Z = 0$, it represents the failure surface; when $Z < 0$, it represents the unsafe region; and when $Z > 0$, it represents the safe region.

Using (63.2), the probability of failure, p_f, *i.e.*, $P(Z < 0)$ can be represented by a multi-dimensional integral as:

$$p_f = \int \cdots \int_{g(\,)\langle 0} f_X(x_1, x_2, \cdots, x_n)\, dx_1 dx_2, \cdots, dx_n \qquad (63.3)$$

where $f_X(x_1, x_2, \cdots, x_n)$ is the joint PDF of all the basic random variables and the integration is carried out in the failure region, *i.e.*, $g(\,)\langle 0$. If the basic random variables are assumed to be statistically independent, the joint PDF can be replaced by the individual PDF. Equation (63.3) is another representation of (63.1) and is known as the *full distributional approach*. Again, information on the multidimensional integral is generally not available. Even when the information is available, the integration of the joint PDF is expected to be difficult; an analytical approximation is a practical necessity. The first level of approximation can be grouped into two types; namely, the first-order reliability method (FORM) and the second-order reliability method (SORM). In FORM, the limit state equation is represented by a linear function of the basic random variables, and in SORM, the limit state is represented by a second-order approximation. Only the commonly used different versions of FORM available in the literature will be emphasized here. Further information on SORM can be found in Haldar and Mahadevan [7].

63.4.1 First-order Reliability Methods

Historically, the first-order reliability methods (FORMs) were developed using the information on the first two moments (mean, and variance or standard deviation, or COV) only. The earlier version of FORM is known as the first-order second-moment (FOSM) or the mean value first-order second-moment (MVFOSM) method. The original formulation of this approach was suggested by Cornell [18] for only two variables, *R* and *S*. The limit state function was defined as $Z = R - S$, and both *R* and *S* were assumed to be statistically independent normal variables. For this

case, the safety index or reliability index β can be shown to be:

$$\beta = \frac{\mu_Z}{\sigma_Z} = \frac{\mu_R - \mu_S}{\sqrt{\sigma_R^2 + \sigma_S^2}} \tag{63.4}$$

The corresponding probability of failure, p_f can be shown to be:

$$p_f = \Phi(-\beta) = 1 - \Phi(\beta) \tag{63.5}$$

where Φ( ) is the CDF of the standard normal distribution.

An alternative formulation was proposed by Rosenbleuth and Esteva [19] for when *R* and *S* are statistically independent lognormal random variables. However, considering realistic practical problems, it is too idealistic to assume that a limit state function can be expressed in terms of only two statistically independent either normal or lognormal random variables. The discussion needs to be extended to consider limit state functions of the general form represented by (63.2). To use (63.4), the mean and variance of the limit state function represented by (63.2) must be evaluated; in some cases even approximately.

To generate the necessary information, the limit state function can be expanded in a Taylor series about the mean values of the basic variables as:

$$Z = g(\mu_{\mathbf{X}}) + \sum_{i=1}^{n} \frac{\partial g}{\partial X_i}\left(X_i - \mu_{\mathbf{X}_i}\right) + \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} \frac{\partial^2 g}{\partial X_i \partial X_j}\left(X_i - \mu_{X_i}\right)\left(X_i - \mu_{X_i}\right) + \cdots \tag{63.6}$$

where the partial derivatives are evaluated at the mean values of the random variables and μ_{X_i} is the mean value of X_i. Considering only the linear terms, *i.e.*, the first two terms in (63.6), the first-order approximate mean and variance of *Z* can be shown to be:

$$\mu_Z' \approx g\left(\mu_{X_1}, \mu_{X_2}, \cdots, \mu_{X_n}\right) \tag{63.7}$$

and

$$\sigma_Z^2 \approx \sum_{i=1}^{n}\sum_{j=1}^{n} \frac{\partial g}{\partial X_i}\frac{\partial g}{\partial X_j} Cov\left(X_i, X_j\right) \tag{63.8}$$

where $Cov\left(X_i, X_j\right)$ is the covariance of X_i and X_j. If the variables are statistically independent, the variance (63.8) becomes:

$$\sigma_Z^2 \approx \sum_{i=1}^{n}\left(\frac{\partial g}{\partial X_i}\right)^2 \sigma_{X_i}^2 \tag{63.9}$$

The first-order approximation of the mean and variance can be improved by including the second-order term in the Taylor series expansion. If only information on the mean and variance is available of all the random variables, the second-order variance cannot be calculated since it requires information on the third and fourth moments. However, the second-order mean can be shown to be:

$$\mu_Z'' \approx \mu_Z' + \frac{1}{2}\sum_{i=1}^{2}\left(\frac{\partial^2 g}{\partial X_i^2}\right)\mathrm{Var}\left(X_i\right) \tag{63.10}$$

In the context of FOSM, the use of second-order mean and first-order variance was advocated by Ayyub and Haldar [20]. Assuming that *Z* is normal with the mean calculated by (63.7) or (63.10) and the variance calculated by (63.8) or (63.9), the reliability index and the corresponding probability of failure can be calculated by (63.4) and (63.5), respectively.

FOSM has many deficiencies. The method does not use the information on distribution even when it is available. When *g* ( ) is highly nonlinear, the Taylor series approximation may introduce a significant amount of error in the estimation of the mean and variance. More importantly, the safety index defined by (63.4) does not give the same result for different but mechanically equivalent formulations of the same limit state function. It can be shown easily that the limit state functions defined as ($R - S < 0$) and ($R/S < 1$) are mechanically equivalent; however, using FOSM the reliability index calculated using (63.4) would be different for the two cases. Ayyub and Haldar [20] also showed that if the limit state functions are formulated in terms of stress and strength (they are essentially the same), the reliability index according to FOSM will be different.

The lack of invariance in the reliability index evaluation prompted Hasofer and Lind [21] to propose the advanced first-order second moment

(AFOSM) method; essentially for only normal random variables. In this formulation, random variables are defined in the reduced coordinate as:

$$X_i' = \frac{X_i - \mu_{X_i}}{\sigma_{X_i}}; i = 1, 2, \cdots, n \qquad (63.11)$$

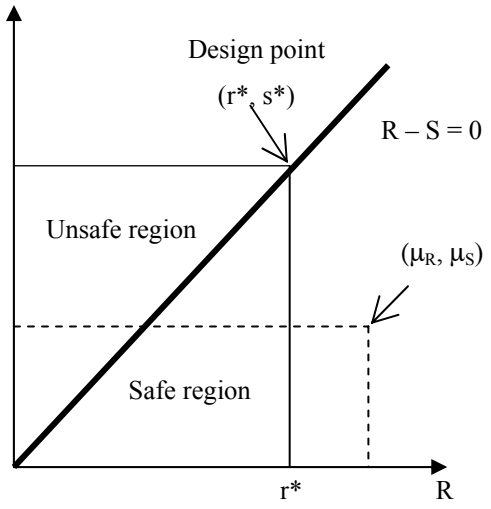
where X_i' is a random variable with zero mean and unit standard deviation. In the context of AFOSM, X_i' is a standard normal variable. With this transformation, the original limit state equation g(**X**) = 0 becomes g(**X'**) = 0 in the transformed or reduced coordinates. The Hasofer–Lind safety index, denoted as β_{HL}, is the minimum distance from the origin to the limit state surface in the reduced coordinates. It can be defined as:

$$\beta_{HL} = \sqrt{(\mathbf{x}'^*)^t (\mathbf{x}'^*)} \qquad (63.12)$$

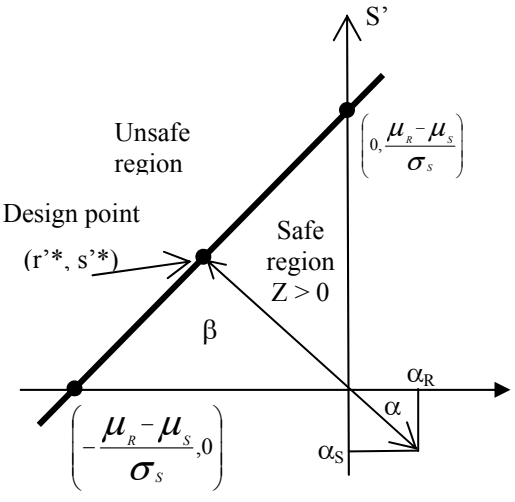
where **x**'* is the coordinates of the checking point in the reduced coordinates.

The concept is shown in Figure 63.2 for a linear limit state equation. The minimum distance point on the limit state surface is known as the design point or the most probable failure point. The reliability index according to AFOSM will give an identical reliability index to that calculated by using FOSM when the limit state equation is linear and all the variables are normal. However, the reliability indexes are calculated in completely different ways in these two approaches. The AFOSM method gives a geometric interpretation of the reliability index. As can be observed from Figure 63.2, if the reliability index is large, the safe region increases and the corresponding probability of failure becomes smaller.

When the limit state equation is nonlinear, the AFOSM method can be used, however, an iterative optimization procedure needs to be used to evaluate the reliability index, as shown in Figure 63.3. The Hasofer–Lind reliability index can be exactly related to the failure probability using (63.5) if all the variables are statistically independent and normally distributed. For any other situations, it will not give the correct reliability information. To incorporate information on distribution for linear and nonlinear limit states,



(a) Original coordinates



(b) Reduced coordinates

Figure 63.2. Reliability evaluation for linear performance function (from [7], with permission from John Wiley & Sons, Inc.)

Rackwitz and Fiessler [22] proposed improvements of the AFOSM method. At present, the more general and improved version of the Hasofer–Lind AFOSM method is known as the first-order reliability method (FORM). For the nonlinear limit state function, when it is represented by the second-order approximation at the checking point, it is known as the second-order reliability method (SORM). FORM is routinely used in many

engineering disciplines. Haldar and Mahadevan [7] suggested an alternative version of FORM that is particularly applicable when the limit states are not explicit functions of the basic random variables or when they are complicated nonlinear functions.

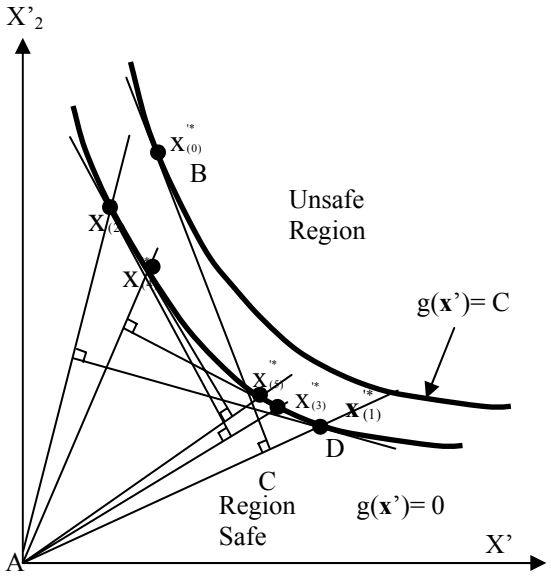


Figure 63.3. Reliability evaluation for linear performance function (from [7], with permission from John Wiley & Sons, Inc.)

63.4.2 An Iterative Procedure for FORM

The most commonly used FORM algorithm, with some improvements as suggested in [20], for nonlinear explicit limit state functions consisting of correlated nonnormal variables are briefly discussed next. In most engineering problems, the basic variables are generally assumed to be statistically independent since dependency significantly increases the difficulty in the reliability evaluation. An iterative solution strategy is required. The following brief discussions are expected to clarify the procedure for the reliability evaluation for this difficult case.

Step 1: Define the appropriate limit state function in terms of the basic random variables as in (63.2).

Step 2: Assume an initial value of the reliability index β. An initial β value of 3 is reasonable to start the iteration process.

Iteration 1

Step 3: Assume the coordinates of the initial checking point x_i^*, $i = 1, 2, \ldots, n$. The initial values are generally assumed to be the mean values of the random variables.

Step 4: Compute the equivalent normal mean and standard deviation of all the nonnormal random variables at the checking point. Denoting the equivalent normal mean and standard deviation of the ith random variable as $\mu_{X_i}^N$ and $\sigma_{X_i}^N$, respectively, It can be shown [7] that they can be estimated as:

$$\mu_{X_i}^N = x_i^* - \Phi^{-1}\left[F_{X_i}\left(x_i^*\right)\right]\sigma_{X_i}^N \tag{63.13}$$

and

$$\sigma_{X_1}^N = \frac{\phi\left\{\Phi^{-1}\left[F_{X_i}\left(x_i^*\right)\right]\right\}}{f_{X_i}\left(x_i^*\right)} \tag{63.14}$$

where $F_{X_i}\left(x_i^*\right)$ and $f_{X_i}\left(x_i^*\right)$ are the CDF and the PDF of the nonnormal random variable evaluated at the checking point, respectively, and $\Phi^{-1}(\,)$ and $\phi\,(\,)$ are the inverse of the CDF and the PDF of the standard normal distribution, respectively.

For a lognormal random variable X with parameters λ_X and ζ_X, the equivalent normal mean and standard deviation at the checking point x^* can be simplified to be [7]:

$$\sigma_X^N = \xi_X\, x^* \tag{63.15}$$

and

$$\mu_X^N = x^*\left(1 - \ln x^* + \lambda_X\right) \tag{63.16}$$

Step 5: If the variables X_i's are correlated, they need to be transformed into uncorrelated reduced normal **Y** variables. The original limit state equation needs to be expressed in terms of **Y** variables. The following steps can be followed.

The correlation matrix of the X_i variables can be expressed as:

$$\left[\mathbf{C}\right] = \begin{bmatrix} 1 & \rho_{X_1,X_2} & \cdots & \rho_{X_1,X_n} \\ \rho_{X_2,X_1} & 1 & \cdots & \rho_{X_2,X_n} \\ \vdots & \vdots & & \vdots \\ \rho_{X_n,X_1} & \rho_{X_n,X_2} & \cdots & 1 \end{bmatrix} \tag{63.17}$$

where ρ_{X_i,X_j} is the correlation coefficient of the X_i and X_j variables.

The relationship between **X** and **Y** can be shown [7] as:

$$[\mathbf{X}] = \left[\sigma_{\mathbf{X}}^{N}\right][\mathbf{T}][\mathbf{Y}] + \left\{\mu_{\mathbf{X}}^{N}\right\} \tag{63.18}$$

where $\mu_{X_i}^{N}$ and $\sigma_{X_i}^{N}$ are the equivalent normal mean and standard deviation of X_i, respectively, evaluated at the checking point using (63.13) and (63.14), and **T** is a transformation matrix. Note that the matrix containing the equivalent normal standard deviation in (63.18) is a diagonal matrix. The transformation matrix **T** can be shown to be:

$$[\mathbf{T}] = \begin{bmatrix} \theta_1^{(1)} & \theta_1^{(2)} & \cdots & \theta_1^{(n)} \\ \theta_2^{(1)} & \theta_2^{(2)} & \cdots & \theta_2^{(n)} \\ \vdots & \vdots & & \vdots \\ \theta_n^{(1)} & \theta_n^{(2)} & \cdots & \theta_n^{(n)} \end{bmatrix} \tag{63.19}$$

where $\left\{\theta^{(i)}\right\}$ is the normalized eigenvector of the ith mode of the correlation matrix $[\mathbf{C}]$ and $\theta_1^{(i)}, \theta_2^{(i)}, \cdots, \theta_n^{(i)}$ are the components of the ith eigenvector. Eigenvalues are the variance of **Y** and **Y** will have zero mean.

Using (63.18), all the basic random variables **X**'s can be transformed to statistically independent standard normal variables **Y**'s. The limit state equation defined in Step 1 now can be rewritten in terms of **Y**'s.

Step 6: Transform the initial checking point of X_i's to Y_i's, using :

$$\mathbf{Y} = \mathbf{T}^{t}\ \mathbf{X}' \tag{63.20}$$

where matrix **T** is defined by (63.19) and the vector **X**' contains all the random variables X_i's in the reduced coordinates evaluated at the checking point. For X_i, it can be expressed as:

$$X_i = \frac{x_i^{*} - \mu_{X_i}^{N}}{\sigma_{X_i}^{N}} \tag{63.21}$$

Step 7: Compute partial derivatives $\left(\frac{\partial g(\ )}{\partial Y_i}\right)^{*}$ of the transformed limit state function obtained in Step 5 evaluated at the checking point $\mathbf{y}^{*}$ defined in Step 6.

Step 8: Compute the direction cosines α_i at the checking point as:

$$\alpha_{Y_i} = \frac{\left(\frac{\partial g}{\partial Y_i}\right)^{*} \sigma_{Y_i}^{N}}{\sqrt{\sum_{i=1}^{n}\left(\frac{\partial g}{\partial Y_i}\,\sigma_{Y_i}^{N}\right)^{*2}}} \tag{63.22}$$

Iteration 2

Repeat Steps 3 to 8 until the estimate of the direction cosines converge with a predetermined tolerance. A tolerance level of 0.005 is common. Obviously, just after one iteration, no conversion decision of the direction cosines can be made. This will necessitate the execution of Steps 9 and 10.

Step 9: Compute the new checking point in the Y coordinates as:

$$y_i^{*} = -\alpha_{Y_i}\ \beta\ \sigma_{Y_i}^{N} \tag{63.23}$$

Step 10: Transform the coordinates of the new checking point in Step 9 to original coordinates using (63.20). When the coordinates of the new checking point are available, it is essentially Step 3 discussed earlier.

After repeating Steps 3 to 8 several times (three or four in most cases), the direction cosines will converge. Then, the new checking point can be evaluated using Steps 9 and 10, keeping β as the unknown parameter. This additional computation suggested by Ayyub and Haldar [20] may improve the robustness of the algorithm. The assumption of an initial value for β in Step 2 is necessary only for the sake of this additional computation.

Step 11: Compute an updated value for β satisfying the limit state equation at the new checking point.

Step 12: Repeat Steps 3 to 11 until β converges to a predetermined tolerance level. A tolerance level of 0.001 can be used, particularly if a computer is used to carry out the calculations.

63.4.3 Example

All 12 steps discussed earlier can be better explained with the following example.

A simply supported beam of span L = 9.144 m is loaded by a uniformly distributed load w in kN/m and a concentrated load P in kN applied at the midspan. The maximum deflection of the beam at the midspan can be calculated as

$$\delta_{\max} = \frac{5}{384}\frac{w L^4}{EI} + \frac{1}{48}\frac{P L^3}{EI} \tag{63.24}$$

where E is Young's modulus and I is the moment of inertia of the cross-section of the beam. A beam with EI = 182,262 kN m^2 is selected to carry the load. Suppose w and P are correlated lognormal variables with a mean of 35.03 kN/m and 111.2 kN, respectively. The corresponding standard deviations are 5.25 kN/m and 11.12 kN, respectively. The correlation between w and P is 0.7. Consider the allowable deflection at midspan as 38.1 mm. The task is to estimate the reliability index and the corresponding probability of failure of the beam using FORM.

Solution

It is not possible to show all the hand calculations here, but the results are summarized in Table 63.1. Calculations for the first and the final iterations are shown in the following sections.

Step 1: The limit state function for the problem can be shown to be

$$g(\,) = 0.0381 - \left(4.99444 \times 10^{-4}\, w + 8.73919 \times 10^{-5}\, P\right) \tag{63.25}$$

w and P are lognormal random variables. They can be expressed as $w \sim Ln(\lambda_w, \zeta_w)$ and $P \sim Ln(\lambda_P, \zeta_P)$, respectively. The parameters of w and P can be calculated as:

$$\zeta_w = \sqrt{\ln\left[1 + \left(\frac{5.25}{35.03}\right)^2\right]} = 0.149$$

and

$$\lambda_w = \ln 35.03 - \frac{1}{2} \times 0.149^2 = 3.545$$

$$\delta_P = \frac{11.12}{111.2} = 0.1 \cong \zeta_P$$

and

$$\lambda_P = \ln 111.2 - \frac{1}{2} \times 0.1^2 = 4.706$$

Since w and P are correlated, they need to be transformed in to uncorrelated $\mathbf{Y}$ variables.

However, since the equivalent normal mean and standard deviation of both of them need to be evaluated at the checking point and the coordinates of the checking point are expected to be different at each iteration, the limit state function will change for each iteration. Hand calculations are not suggested for this type of problem. However, for the sake of clarity, some of the important steps are presented below in terms of different steps discussed earlier.

Step 2: Assume β = 3 to start the iteration.

Iteration 1

Step 3:

The coordinates of the initial checking point are w^* = 35.03 and P^* = 111.20.

Step 4:

The corresponding equivalent normal mean and standard deviation of w and P are:

$$\sigma_w^N = 0.149 \times 35.03 = 5.22$$

$$\mu_w^N = 35.03 \times (1 - \ln 35.03 + 3.545) = 34.64$$

$$\sigma_P^N = 0.1 \times 111.2 = 11.12$$

$$\mu_P^N = 111.2 \times (1 - \ln 111.2 + 4.706) = 110.61$$

Step 5:

The correlation matrix [**C**] given by (63.17) for the problem is

$$[\mathbf{C}] = \begin{bmatrix} 1 & 0.7 \\ 0.7 & 1 \end{bmatrix}$$

The two eigenvalues for the correlation matrix can be shown to be 0.3 and 1.7 [23]. The corresponding normalized eigenvectors can be evaluated and the tranformation matrix [**T**] given by (63.19) can be shown to be

$$[\mathbf{T}] = \begin{bmatrix} 0.707 & 0.707 \\ -0.707 & 0.707 \end{bmatrix}$$

Using (63.18), it can be shown that

$$\begin{Bmatrix} w \\ P \end{Bmatrix} = \begin{bmatrix} 5.22 & 0 \\ 0 & 11.12 \end{bmatrix} \begin{bmatrix} 0.707 & 0.707 \\ -0.707 & 0.707 \end{bmatrix} \begin{Bmatrix} Y_1 \\ Y_2 \end{Bmatrix} + \begin{Bmatrix} 34.64 \\ 110.61 \end{Bmatrix}$$

Or,

$$w^* = 3.69 \times (Y_1 + Y_2) + 34.64$$

$$P^* = 7.86 \times (Y_2 - Y_1) + 110.61$$

Step 6:

Using (63.20), it can be shown that

$$\begin{Bmatrix} y_1^* \\ y_2^* \end{Bmatrix} = \begin{bmatrix} 0.707 & -0.707 \\ 0.707 & 0.707 \end{bmatrix} \begin{Bmatrix} 0.0747 \\ 0.0531 \end{Bmatrix} = \begin{Bmatrix} 0.0153 \\ 0.0904 \end{Bmatrix}$$

Step 7:

$$\left(\frac{\partial g}{\partial Y_1} \right)^* = -1.1560 \times 10^{-3}$$

$$\left(\frac{\partial g}{\partial Y_2} \right)^* = -2.5298 \times 10^{-3}$$

Step 8:

$$\alpha_{Y_1} = \frac{-1.156 \times 10^{-3} \times \sqrt{0.3}}{\sqrt{\left(-1.156 \times 10^{-3}\right)^2 \times 0.3 + \left(-2.5298 \times 10^{-3}\right)^2 \times 1.7}}$$

$$= \frac{-0.63317 \times 10^{-3}}{3.358675 \times 10^{-3}} = -0.1885$$

$$\alpha_{Y_2} = \frac{-2.5298 \times \times 10^{-3} \times \sqrt{1.7}}{3.358675 \times \times 10^{-3}} = -0.9821$$

As summarized in Table 63.1, it took four iterations before the direction cosines converged with an accuracy of 0.005. At this stage, the updated reliability index was estimated to be 2.789. The reliability index was assumed to be 3.0 to start the iteration. Obviously, the reliability index did not converge with an accuracy level of 0.001 and further calculations are necessary. In the next iteration, the direction cosines converged with an accuracy of 0.005. Again, the reliability index was calculated and found to be 2.778. It is an improvement but not within the accuracy level of 0.001. The final iteration was then initiated as presented next.

Final Iteration

Step 2:

From previous iteration $\beta = 2.778$

Step 3:

$$w^* = 5.486(0.3267 + 3.5377) + 30.83 = 52.03$$

$$p^* = 9.820(3.5377 - 0.3267) + 107.28 = 138.81$$

Step 4:

$$\sigma_w^N = 0.149 \times 52.03 = 7.75$$

$$\mu_w^N = 52.03 \times (1 - \ln 52.03 + 3.545) = 30.86$$

$$\sigma_P^N = 0.1 \times 138.81 = 13.89$$

$$\mu_P^N = 138.81 \times (1 - \ln 138.81 + 4.706) = 107.29$$

Step 5:

$$\begin{Bmatrix} w \\ P \end{Bmatrix} = \begin{bmatrix} 7.75 & 0 \\ 0 & 13.89 \end{bmatrix} \begin{bmatrix} 0.707 & 0.707 \\ -0.707 & 0.707 \end{bmatrix} \begin{Bmatrix} Y_1 \\ Y_2 \end{Bmatrix} + \begin{Bmatrix} 30.86 \\ 107.29 \end{Bmatrix}$$

Or,

$$w^* = 5.479 \times (Y_1 + Y_2) + 30.86$$

$$P^* = 9.82 \times (Y_2 - Y_1) + 107.29$$

$$g(\,) = 0.0381 - 4.9944 \times 10^{-4} [5.479 \times (Y_1 + Y_2) + 30.86]$$

$$- 8.73919 \times 10^{-5} [9.82 \times (Y_2 - Y_1) + 107.29]$$

$$= 0.013324 - 1.8782 \times 10^{-3} Y_1 - 3.5946 \times 10^{-3} Y_2$$

Step 6:

$$\begin{Bmatrix} y_1^* \\ y_2^* \end{Bmatrix} = \begin{bmatrix} 0.707 & -0.707 \\ 0.707 & 0.707 \end{bmatrix} \begin{Bmatrix} 2.732 \\ 2.269 \end{Bmatrix} = \begin{Bmatrix} 0.3273 \\ 3.5357 \end{Bmatrix}$$

$$\alpha_{Y_1} = \frac{-1.8782 \times 10^{-3} \times \sqrt{0.3}}{\sqrt{\left(-1.8782 \times 10^{-3}\right)^2 \times 0.3 + \left(-3.5946 \times 10^{-3}\right)^2 \times 1.7}}$$

$$= \frac{-1.02873 \times 10^{-3}}{4.79836 \times 10^{-3}} = -0.2144$$

$$\alpha_{Y_2} = \frac{-3.5946 \times 10^{-3} \times \sqrt{1.7}}{4.79836 \times 10^{-3}} = -0.9767$$

Step 8:

$$Y_1^* = 0.2144 \times \beta \times \sqrt{0.3} = 0.1174\beta$$

$$Y_2^* = 0.9767 \times \beta \times \sqrt{1.7} = 1.27346\beta$$

$$0.013324 - 1.8782 \times 10^{-3} \times 0.11743\beta - 3.5946 \times 10^{-3} \times 1.27346\beta = 0$$

Or, $\beta = 2.777$

Table 63.1. Reliability evaluation using FORM for correlated nonnormal variables

Steps 1 and 5	$g( ) = 0.0381 - (4.99444 \times 10^{-4} w + 8.73919 \times 10^{-5} P)$ (original with correlated variables) $g( ) = 0.0111 - 1.1560 \times 10^{-3} Y_1 - 2.5298 \times 10^{-3} Y_2$ (first iteration) $g( ) = 0.013324 - 1.8782 \times 10^{-3} Y_1 - 3.5946 \times 10^{-3} Y_2$ (final iteration)						
Step 2	β	3.0				2.789	2.778
Steps 3 and 10	w^*	35.03	49.96	53.59	53.85	52.10	52.03
	p^*	111.20	138.37	141.43	141.31	138.85	138.81
Step 4	μ_W^N	34.64	31.66	30.21	30.09	30.83	30.86
	σ_W^N	5.22	7.44	7.98	8.02	7.76	7.75
	μ_P^N	110.61	107.38	106.67	106.70	107.28	107.29
	σ_P^N	11.12	13.84	14.14	14.13	13.89	13.89
Step 6	y_1^*	0.0153	0.1562	0.3337	0.3634	0.3309	0.3273
	y_2^*	0.0904	3.3222	3.8093	3.8263	3.5449	3.5357
Step 7	$\left(\frac{\partial g}{\partial Y_1}\right)^*$	-1.1560×10^{-3}	-1.7724×10^{-3}	-1.9429×10^{-3}	-1.9588×10^{-3}	-1.8837×10^{-3}	-1.8782×10^{-3}
	$\left(\frac{\partial g}{\partial Y_2}\right)^*$	-2.5298×10^{-3}	-3.4818×10^{-3}	-3.6907×10^{-3}	-3.7048×10^{-3}	-3.6001×10^{-3}	-3.5946×10^{-3}
Step 8	α_{Y_1}	–0.1885	–0.2091	–0.2159	–0.2168	–0.2147	–0.2144
	α_{Y_2}	–0.9821	–0.9779	–0.9764	–0.9762	–0.9767	–0.9767
Step 11					2.789	2.778	2.777
Step 12	β						2.777

The reliability index has converged. The corresponding probability of failure of the beam in deflection is about 2.7×10^{-3}.

63.5 Probabilistic Sensitivity Indexes

In a real practical problem, the number of random variables present in the formulation can be numerous. However, not all of them have equal influence on the reliability evaluation. Their relative influence can be established by using a *sensitivity index*. The information on the gradient vector of the performance function in the standard normal variable space, already evaluated using FORM, can be used for this purpose. A sensitivity vector can be defined as [7]:

$$\gamma = \frac{\mathbf{SB}^t \alpha}{\left|\mathbf{SB}^t \alpha\right|} \tag{63.26}$$

where **S** is the diagonal matrix of standard deviations of the variables (equivalent normal standard deviations for the nonnormal random variables), **B** is a diagonal matrix required to transform the original **X** variables to equivalent uncorrelated standard normal variables **Y,** and α is the unit vector in the direction of the gradient vector.

The elements of the vector γ can be referred to as sensitivity indexes of the individual variables. Variables with low sensitivity indexes calculated at the end of the first few iterations can be treated as deterministic at their mean values in the subsequent iterations in the search for the β value. This may significantly reduce the computational effort required to obtain the underlying reliability.

63.6 Reliability Evaluation Using Simulation

With the advancement in computational power, simulation is becoming very attractive to estimate the underlying reliability [24, 25]. It does not require the sophisticated mathematical background necessary to implement FORM/SORM type reliability evaluation methods. With only a little background in probability and statistics, one can use simulation to estimate the reliability. Lewis and Orav [26] wrote "Simulation is essentially a controlled statistical sampling technique that, with a model, is used to obtain approximate answer for questions about complex, multi-factor probabilistic problems." They added "It is this interaction of experience, applied mathematics, statistics, and computing science that makes simulation such a stimulating subject, but at the same time a subject that is difficult to teach and write about." It provides a cheaper alternative to evaluate risk or the effect of uncertainty in the computer environment than the expensive physical experiments in the laboratory or in the field.

The method commonly used for this purpose is the Monte Carlo simulation technique. In the simplest form, each random variable is sampled several times satisfying the underlying probabilistic characteristics. Considering each realization of all the random variables produces a set of numbers that indicates one realization of the problem itself. Solving the problem for each realization deterministically is known as a simulation cycle, trial, or run. Using many simulation cycles gives the overall probabilistic characteristics of the problem, particularly when the number of cycles tends to infinity.

Monte Carlo simulation can be carried out with the help of following steps; (1) define the problem to be simulated in terms of all the random variables, (2) quantify the probabilistic characteristics of all the random variables in terms of their probability density or mass functions, (3) generate random numbers for these random variables satisfying their probabilistic characteristics, (4) solve the problem deterministically numerous times for each set of realizations of all the random variables, (5) extract the necessary probabilistic information from N such realization, and (6) determine the efficiency and accuracy of the simulation.

The first two steps are similar to the FORM/SORM approaches. Generating random numbers satisfying the underlying probabilistic characteristics is the essence of simulation. Most modern computers have the capability of generating uniformly distributed random numbers between 0 and 1. For an arbitrary seed value, the generator will produce the required number of uniformly distributed random numbers between 0 and 1. Depending on the size of the computer, the random numbers can be repeated. However, for engineering problems, this situation is rarely encountered. Random numbers generated this way are called *pseudo random numbers*. These uniform random numbers are then transformed into other random numbers satisfying the probabilistic characteristic of the basic random variable of interest. The *inverse transformation technique* is generally used for this purpose [7]. Some computers can directly generate random numbers for commonly used distributions.

Once the random numbers are generated for all the random variables present in the problem providing N sets of random numbers, the problem

defined in Step 1 then can be deterministically solved producing N sample points. The statistical information on these N sample points can be extracted in numerous ways. In most formulations, the function g ( ) in Step 1 will produce negative result if the system fails. Let N_f be the number of simulation cycles when g( ) is negative out of a total of N simulation cycles. Then the probability of failure can be expressed as:

$$p_f = \frac{N_f}{N} \tag{63.27}$$

The accuracy of (63.27) in predicting the probability of failure is a major concern. For a small probability of failure and/or small N, a considerable amount of error is expected in estimating p_f. For many engineering problems, the probability of failure may be smaller than 10^{-5}. Therefore, on an average, only 1 out of 100,000 trials would show a failure. For a reasonable estimate, at least 10 times this minimum, that is 1 million simulation cycles, is usually recommended to estimate the probability of failure of the order of 10^{-5}.

The previous discussions clearly indicate the basic simplicity in the simulation approach. They also point out its drawback, *i.e.*, it could be tedious or cumbersome for reliability evaluation of large systems with low probability of failure. The efficiency of simulation can be improved by using *variance reduction techniques* (VRTs). VRTs are expected to estimate the probability of failure with a reduced number of simulation cycles. The efficiency can be improved by altering the input scheme, by altering the model, or by special analysis of the output. The VRTs can also be grouped according to the purpose, *i.e.*, sampling methods, correlation methods, and special methods.

The sampling methods either constrain the sample to be representative or distort the sample to emphasize the important aspects of the function being estimated. Some of the sampling methods are systematic sampling, importance sampling, stratified sampling, Latin hypercube sampling, adaptive sampling, randomization sampling, and conditional expectation. The correlation methods employ strategies to achieve correlation between functions or different simulations to improve the efficiency. Some VRTs in correlation methods are common random numbers, antithetic variates, and control variates. Other special VTRs include partition of the region, random quadratic method, biased estimator, and indirect estimator. VRTs can also be combined to further increase the efficiency of the simulation [7].

It is usually impossible to know beforehand how much efficiency can be improved by using a specific technique. It should be noted that VRTs significantly increase the computational difficulty and a considerable amount of expertise may be necessary to implement them. The most desirable feature of simulation, its basic simplicity, is thus lost.

63.7 Reliability Evaluation Using FOSM, FORM, and Simulation

As mentioned earlier, any one of the methods discussed in the previous sections can be used to estimate reliability or probability of failure. An example is given here to demonstrate their advantages and disadvantages.

63.7.1 Example

Suppose a very tall chimney of height 36.58 m and diameter 2.53 m is made with steel plates of thickness 6.35 mm. The probability of failure of the chimney needs to be estimated when subjected to the wind load. Suppose the limit state function for the problem, as suggested by Haldar and Ayyub [27] is:

$$Z = \pi X_1 F_y - 0.04136 C_f X_2 V_{10}^2 \tag{63.28}$$

where X_1 is a function of thickness and outer radius of the chimney, C_f is a pressure coefficient, X_2 is a function of velocity pressure coefficient, gust factor, and the diameter of the chimney, and V_{10} is the wind velocity 10 m above the ground surface. They are all considered to be random variables and their probabilistic characteristics are summarized in Table 63.2.

Table 63.2. Probabilistic characteristics of random variables

Random variables	Mean	COV	Prob. distri-bution
X_1 (m^3)	5.6×10^{-3}	0.08666	Log normal
X_2 (m)	3.246	0.18652	Log normal
F_y (kPa)	262.0×10^3	0.10	Normal
C_f	0.672	0.10	Normal
V_{10}^2 (km/hour)	101.49	0.16	(Type II, u = 0)

The probability of failure of the chimney is calculated in several ways, including using FOSM (i) with first-order mean and first-order variance, (ii) second-order mean and first-order variance, (iii) FORM, (iv) basic Monte Carlo simulation, (v) Monte Carlo simulation with conditional expectation VRT, and (vi) Monte Carlo simulation with conditional expectation plus antithetic variates VRT. The results are summarized in Table 63.3.

Several important observations can be made from this example. As the example points out, the FOSM method with first-order mean or second-order mean may not improve the estimation of the probability of failure significantly. It will depend on the nonlinearity in the limit state function. However, these means may not give a realistic measure of safety. The limit state function represented by (63.28) is nonlinear and contains a random variable with extreme value distribution [7]. The probabilities of failure obtained by FOSM (two alternatives) and FORM are found to be 6.2×10^{-7} or 6.9×10^{-7} and $7.1 \times 10^{-4,}$ respectively. The results are about three orders of magnitude different, and FOSM gives very non-conservative result giving a false sense of reliability or safety. The results clearly indicate that FOSM should not be used in the reliability estimation.

Eliminating FOSM, it is important now to validate the FORM result. The validation can be achieved by comparing the RORM result with the simulation results. If one follows the suggestion made earlier, the appropriate number of simulation cycles will be at least $\approx \left(1 \big/ p_f \right) \times 10 = 13{,}500$. The results shown in Table 63.3 indicate that the basic Monte Carlo simulation even with 5,000 simulation cycles will not produce one failure, and 20,000 cycles will not give a result similar to FORM. At this stage, one may erroneously conclude that the FORM result is not correct. The example clearly indicates that definitive conclusion about any simulation scheme may not be meaningful and should be avoided as much as possible. If one stops after 20,000 simulation cycles, the probability of failure estimation will be somewhat inaccurate and the simulation will not validate the FORM result.

To demonstrate the desirable features of VRTs, the basic Monte Carlo simulation scheme is then integrated with VRTs. In one scheme (option v) only one VRT (conditional expectation VRT) is used, and in the other scheme (option vi); two VRTs are combined (conditional expectation and antithetic variates). The first scheme with one VRT gives a result similar to FORM only after 5,000 cycles. However, the second scheme with two VRTs, confirms the FORM result even with 500 cycles. The accuracy of prediction of both schemes improves as the total number of simulation cycles increases. This is generally described in terms of COV of the prediction. The results in Table 63.3 indicate that the COV of the mean probability of failure went down as N increases. In any case, both simulation schemes confirm the FORM result. One major conclusion of this exercise is to suggest that FORM should be used for reliability estimation whenever possible. A considerable amount of research is now being carried out on various aspects of simulation with VRTs. However, it is difficult to predict which VRT scheme will be appropriate for a particular problem.

Table 63.3. Reliability evaluation using different techniques

FOSM				FORM		Monte Carlo simulation					
First-order mean, first-order variance		First-order mean, first-order variance				Simulation cycles	Direct	Conditional expectation VRT		Conditional expectation plus antithetic variates VRT	
β	p_f	β	p_f	β	p_f	N	$p_f = N_f/N$	Mean	COV	Mean	COV
4.85	6.173×10^{-7}	4.83	6.877×10^{-7}	3.19	7.11×10^{-4}	500	0.000	8.44×10^{-4}	0.0642	7.427×10^{-4}	0.0370
						1,000	0.000	8.029×10^{-4}	0.0508	7.472×10^{-4}	0.0288
						5,000	0.000	7.415×10^{-4}	0.0208	7.362×10^{-4}	0.0118
						20,000	4.5×10^{-4}	7.451×10^{-4}	0.0107	7.389×10^{-4}	0.0063

63.8 FORM for Implicit Limit State Functions – The Stochastic Finite Element Method

The discussions so far assume that the limit state functions are available in explicit forms, *i.e.*, they are available in terms of random variables present in the formulation. They can be differentiated with respect to the random variables to estimate the direction cosines and the gradient vector to locate the most probable failure point. However, for most problems of practical interest, limit state functions are not available in the explicit form. This is particularly true for nonlinear problems. The probability of failure implies that it should be estimated just before failure considering all major sources of nonlinearity and uncertainty. However, commonly used FORM/SORM-based evaluation methods cannot be used to predict realistic failure probability.

Several computational schemes can be pursued for the reliability analysis for implicit limit state functions. These can be broadly divided into three categories, based on their essential philosophy, as (1) Monte Carlo simulation with VRTs, (2) response surface approach, and (3) sensitivity-based analysis. As mentioned earlier, the efficiency and accuracy of Monte Carlo simulation with or without VRTs are always open to questions. The response surface approach approximately constructs a polynomial approximation of the implicit limit state function. Its efficiency depends on the form of the polynomial and it needs to be generated in the failure region which will be unknown in most cases. The sensitivity-based approaches can be defined in three ways: (1) the finite difference approach, (2) classical perturbation, and (3) iterative perturbation. The author and his team used the iterative perturbation technique to evaluate the reliability of systems considering all major sources of nonlinearity and uncertainty. They called it the stochastic finite element method (SFEM) [8].

With the advances in computational power, it is quite appropriate to develop a finite element method- (FEM) based reliability analysis technique parallel to the deterministic analysis procedure. In this way, complicated structural arrangements and different sources of nonlinearity can be modeled in efficient ways. However, the basic drawback of the FEM is that it cannot incorporate information on uncertainties in the variables even when it is available. As mentioned earlier, in the available FORM/SORM approaches, the structural behavior needs to be considerably idealized to estimate the

reliability. The desirable features of the two approaches can be combined leading to the SFEM approach.

The SFEM-based approach is very difficult, however, the concept is briefly discussed below for the sake of completeness. Without losing any generality, the limit state function can be expressed in terms of the set of basic random variables **x**, the set of displacements **u** and the set of load effects **s** (except the displacements, such as internal forces). The displacement vector can be expressed as **u** = **QD**, where **D** is the global displacement vector and **Q** is a transformation matrix. The limit state function can be expressed as $g(\mathbf{x},\mathbf{u},\mathbf{s})=0$. In general, **x**, **u**, and **s** are related in an algorithmic sense, for example, a finite element code. For reliability computation, it is convenient to transform **x** into the standard normal space **y** = y**(x)** such that the elements of **y** are statistically independent and have a standard normal distribution. An iteration algorithm can be used to locate the design point on the limit state function using the first-order approximation. During each iteration, the structural response and the response gradient vectors are calculated using finite element models. The following iteration scheme can be used for finding the coordinates of the design point:

$$\mathbf{y}_{i+1}=\left[\mathbf{y}_i^t\alpha_i+\frac{g(\mathbf{y}_i)}{\left|\nabla g(\mathbf{y}_i)\right|}\right]\alpha_i \tag{63.29}$$

where

$$\nabla g(\mathbf{y})=\left[\frac{\partial g(\mathbf{y})}{\partial y_1},\ldots,\frac{\partial g(\mathbf{y})}{\partial y_n}\right]^t \tag{63.30}$$

and

$$\alpha_i=-\frac{\nabla g(\mathbf{y}_i)}{\left|\nabla g(\mathbf{y}_i)\right|} \tag{63.31}$$

To implement the algorithm, the gradient $\nabla g(\mathbf{y})$ of the limit state function in the standard normal space can be derived as [8]:

$$\nabla g(\mathbf{y})=\left[\frac{\partial g(\mathbf{y})}{\partial \mathbf{s}}\mathbf{J}_{s,x}+\left(\mathbf{Q}\frac{\partial g(\mathbf{y})}{\partial \mathbf{u}}+\frac{\partial g(\mathbf{y})}{\partial \mathbf{s}}\mathbf{J}_{s,D}\right)\mathbf{J}_{D,x}+\frac{\partial g(\mathbf{y})}{\partial \mathbf{x}}\right]\mathbf{J}_{y,x}^{-1} \tag{63.32}$$

where $J_{i,j}$'s are the Jacobians of transformation (*e.g.*, $J_{s,x}=\partial s/\partial x$) and y_i's are statistically independent random variables in the standard normal space. The evaluation of the quantities in (63.32) will depend on the problem under consideration (linear or nonlinear, two-dimensional or three-dimensional, *etc*.) and the performance functions used. The essential numerical aspect of SFEM is the evaluation of three partial derivatives, $\partial g/\partial s$, $\partial g/\partial u$, and $\partial g/\partial x$, and four Jacobians, $J_{s,x}$, $J_{s,D}$, $J_{D,x}$, and $J_{y,x}$. They can be evaluated by the procedures provided in [8]. Once the coordinates of the design point y* are evaluated with a preselected convergence criterion, the reliability index β can be evaluated as:

$$\beta=\sqrt{(\mathbf{y}^*)^t(\mathbf{y}^*)} \tag{63.33}$$

The corresponding probability of failure can be estimated using (63.5). A more recent discussion on SFEM can be found in Huh and Haldar [28, 29].

63.9 Recent Trends in Reliability for Civil Engineering Problems

One of the interesting questions at this stage would be where to go from here in the use of reliability for civil engineering problems. The question can be answered in terms of analytical developments and potential application areas. It is believed that the analytical development in the relaibility evaluation area is now mature enough to address all major issues. However, there is considerable room for improvement in the simulation area. Furthermore, in spite of its maturity, the reliability area is not popular among practising engineers and with the deterministic community. In the past, the reliability community overlooked the education component in developing the area. Moreover, the lack of user-friendly computer programs is another obstacle in spreading the word. The challenge can be addressed on two fronts. Reliability-based computer programs can be developed for direct applications or should be made a part of the commercially available deterministic software. There are some movements on both fronts. Several commercially available reliability-based computer programs are now available. NESSUS [30, 31],

PROBAN [32], CALREL [33], and OPENSEES [34] are examples of such software. Proppe *et al*. [35] discussed in detail the necessity of adding probabilistic features in existing deterministic finite element programs. For proper interface with the deterministic software, they advocated a graphical user interface. The COSSAN [36] software attempted to implement the concept.

Applications of the reliability methods in civil engineering problems are fertile areas, and the interest is expected to remain high in the near future. All major design guidelines have either already been revised or are in the process of being revised in reflecting the risk-based design guidelines. However, at present, some problems that cannot be addressed using codified approaches need our attention. Some future analytical and application-oriented topics are briefly discussed below.

Cognitive Sources of Uncertainty

Most of the work on reliability-based engineering incorporates noncognitive (quantitative) sources of uncertainty using crisp set theory. Cognitive or qualitative sources of uncertainty are also important. They come from the vagueness of the problem arising from the intellectual abstractions of reality. According to Ayyub and Klir [37], Albert Einstein stated, "*The mere formulation of a problem is often far more essential than its solution*." They also stated that according to Werner Karl Heisenberg "*What we observe is not nature itself, but nature exposed to our method of questioning*." To incorporate cognitive sources of uncertainty, fuzzy set theory is being developed. This area is expected to grow in the near future.

The crisp set and fuzzy set theories follow different axioms. Most problems with practical significance contain both random and fuzzy variables. Combining different types of uncertainties is a major challenge. This author attempted to initiate related work in the past with limited success [38]. Incorporation of cognitive sources of uncertainty has made significant progress in economics, *e.g.*, in buying and selling stocks. Economists have received the Nobel Prize for this type of activity in the recent past. However, a considerable amount of work still needs to be conducted for engineering applications by combining different sources on uncertainty.

For the sake of completeness, it is important to point out that the applications of artificial neural networks (ANN), the more generic term used by the research community being soft computing, in civil engineering have been noteworthy in the recent past [39]. In addition to ANN, other soft computing techniques include genetic algorithms, evolutionary computation, machine learning, organic computing, probabilistic reasoning, *etc*. The applicability of these techniques may be problem specific, some of them can be combined, or one technique can be used when another has failed to meet the objectives of the study. Soft computing differs from conventional hard computing. Unlike hard computing, soft computing is tolerant of imprecision, uncertainty, partial truth, and approximation. To some extent, it essentially plays a role similar to human mind.

Meshless or Meshfree Methods

As mentioned earlier, the introduction of the FEM-based analysis concept significantly helped the growth of structural engineering. The SFEM method developed by the author is the stochastic part of it. However, it is an approximate technique. The generation of a finite element mesh may be tedious and the solution will depend on the expertise of the analyst. This brings in a nonunique solution to a specific problem. The solution of a problem without using a structured grid is expected to be very appealing. This is known as meshless or meshfree methods. This area is expected to grow in the near future [40, 41].

Robust and Stochastic Optimization

Available optimization techniques enable us to design efficient and economical structures, in most cases. However, a major limitation of deterministic optimization techniques is that they are unable to incorporate uncertainties in the design variables even when the information is available. It is now well-established in the profession that engineering analysis and design cannot be completed without considering the presence of uncertainty. Conceptually, the development of optimum design procedures for structures under uncertainty can be

broadly divided in to three categories: (i) performance-based optimization where the objective is to minimize the expected value of the performance function, (ii) robust optimization where the design is the least sensitive to the changes in input uncertain parameters, and (iii) reliability-based optimization by incorporating statistical information of all the decision variables in the objective function and by minimizing the probability of failure. Robust optimization, as a measure of the performance, can be considered as a design procedure that is insensitive (or less sensitive) to the changes in the input decision variables within a range of interest while satisfying the safety requirements [42]. Moreover, when statistical information on the decision variables is not sufficient or complete, robust optimization is also an attractive alternative. The progress in the area of robust design optimization method has been taken place in various forms through nonlinear programming-based optimization procedures. These are primarily based on probabilistic and sensitivity-based approaches.

Reliability-based optimization of the cost function brings specified reliability for a particular limit state. But it may be sensitive to variations of specific design variables. Comprehensive reliability-based optimization techniques, including genetic algorithms, are being developed by incorporating statistical information of all the decision variables in the objective function and by minimizing the probability of failure [43]. Two most commonly used measures in probabilistic approaches are the mean and variance of the performance function. Generally, the variance is minimized with respect to the original performance requirements. A more balanced approach consisting of cost minimization and satisfying the performance requirements at the same time is expected to be very desirable. The various approaches that utilize probabilistic information reported in the literature are the weighted-sum method [44, 45], the compromise programming approach [46], and the physical programming method [47]. If cost is a decision variable, the optimization problem may not be unique world-wide. Cost depends on many factors including the locations and the standard of living of the people being affected. Rackwitz [48] introduced the life quality index factor to address the problem.

Health Assessment and Monitoring

In-service structural health assessment is also an upcoming research item. Developments of sophisticated new sensors, wireless data transmission, and the power of computers have contributed to progress in this area [49]. The structural behavior or the signature of the structure are expected to change as defects developed in them. Not all defects affect the structural behavior in a similar way. They can be tracked without compromising the underlying reliability of the structure. The structural elements need to be repaired or replaced when they become a cause for concern. After the necessary repair or replacement, it is also necessary to determine if all the defects are identified and repaired properly.

In-service health assessment requires that necessary information be generated with a minimum amount of uncertainty-filled information and without causing major disruption to the normal operation of the structure. The author and his associates are in the process of developing such a method. They are using the system identification (SI)-based defect assessment technique at the local element level. The classical SI approaches have three essential components: input excitation, the system to be identified generally represented in an algorithmic form such as finite elements, and the output response information. Knowing the input and output response time histories, the third component, *i.e.*, the system can be identified. For a finite element representation, it is equivalent to identifying the stiffness parameters of all the elements. However, in most cases of practical importance, input excitation information is not available. Also, for a large structural system, measuring responses at all dynamic degrees of freedom may not be practical or economical. Furthermore, all measured responses are expected to contain numerous sources of error, noise, or uncertainty. These observations require a system to be identified using only noise-contaminated limited response information and without using any input excitation information. However, the task is extremely complicated and mathematically challenging [50–54].

The research team at the University of Arizona is in the process of developing such a method. They have called it the generalized iterative least square extended Kalman filter with unknown input (GILS-EKF-UI) method [55]. Students from many different engineering disciplines, including aerospace, mechanical, and structural engineering, have been involved in developing the method. It is also a good example of advantages of multi-disciplinary collaboration. In the context of the use of reliability methods for civil engineering problems, methods developed in other disciplines need to be utilized and integrated in intelligent ways.

Structural Maintenance

Historically, building new structures has been a source of pride to all structural engineers. Unfortunately, all structures age with time. Several thousand bridges in the US are over their design life. Ideally, they should be replaced when they have out-lived their design life. The situation clearly indicates that structural engineers are doing their job properly, as expected. However, the resources required to build new structures are decreasing.Extension of the life of existing structures has become a necessity and is now a new research topic. The life of a structure can be extended by inspection and with proper maintenance. Inspection outcomes are full of errors or uncertainty-filled, and the maintenance strategies may be numerous. New inspection methods and tests need to be developed or available techniques need to be improved. Inspectors capable of carrying out the inspections need to be trained. Appropriate retrofitting strategies or options need to be developed. Ultimately, incorporating all available information including the cost of repair or replacement, a decision analysis framework needs to be developed for use by practising engineers. A considerable amount of work has yet to be completed. Zhao *et al.* [56] proposed such an approach for further consideration.

Methods are now also available for structural maintenance considering the degradation of the structures as they age, the cost of inspections, and cost of repairs or replacements as they become necessary [57] by incorporating information on uncertainty in the problem. The design and construction of structures considering their long-term behavior (aging, corrosion, fatigue, *etc*.) in the presence of uncertainty are expected to grow in the near future. A structural performance/health assessment method denoted as GILS-EKF-UI is being developed at University of Arizona [58]. The unique feature of this algorithm is that it can identify members' properties and in the process access the performance/health of a structural system using only noise-contaminated dynamic response information measured at few locations, completely ignoring the excitation information.

Prediction of Future Events Like Earthquake, Wind, Draught, Tornado, and Tsunami

As mentioned earlier, we have significant limitations in predicting natural phenomena like earthquake, wind, drought, tornado, tsunami, *etc*. Obviously, the success of civil engineering will depend on how accurately we predict these events. We currently have the mathematical sophistication to design structures if we can predict future events in the presence of uncertainty. A considerable amount of work, both theoretical and experimental, is needed to improve our understanding in predicting these events.

System Reliability

In general, engineering systems need to satisfy more than one limit state function. The limit state functions are generally of two types: (i) strength and (ii) serviceability. The strength limit state function is generally related to the behavior of a member (beam, column, *etc*.) at the element level. However, more than one member needs to fail to cause structural failure for statically indeterminate structures. The serviceability limits states (defection, interstory drift, lateral drift, *etc*.) are generally applicable at the structural or system level. The concept used to consider multiple failure modes and/or multiple component failures is known as system reliability evaluation.

In general, system reliability evaluation is complicated and depends on many factors including (1) the contribution of the component failure events to the system's failure, (2) the redundancy in the system, (3) the post-failure behavior of a component and the rest of the

system, (4) the statistical correlation between failure events, and (5) the progressive failure of components.

The application of the system reliability concept in various engineering disciplines can be described, at best, as non-uniform. In the context of civil/structural engineering, two basic approaches are (1) the cut-set or failure mode approach (FMA) or performance mode approach (PMA) and (2) the tie-set or stable configuration approach (SCA). In FMA, all possible ways in which a structure can fail are identified. A fault tree diagram, which decomposes the main failure event into unions and intersections, can be used for this purpose. FMA is very effective for systems with ductile components (components continue to carry loads after reaching their capacity), particularly when the dominant failure mechanisms of the system can be easily identified. SCA considers how a system or its damaged state can carry loads without failure. SCA is effective for highly redundant systems with brittle components (components that fail to carry loads after reaching their capacity) or with ductile and brittle components.

Once the failure modes or stable configurations of a system are identified, system reliability evaluation involves evaluating the probability of union and intersection of events considering their statistical correlation. In many cases, the statistical correlation may be difficult to estimate. Also, it is difficult to estimate the joint probabilities of more than two failure events. These difficulties result in estimations of upper and lower bounds for the system reliability evaluation. A more complete discussion on the topic can be found in Haldar and Mahadevan [7] and Chowdhury and Haldar [59].

63.10 Concluding Remarks

Civil engineering is the oldest engineering profession and has had over 5000 years of glorious history. The profession has accepted all challenges and provided services at the highest level to society worldwide. It is a profession whose main purpose is to improve the quality of life. However, due to the presence of a considerable amount of uncertainty, it is not possible to design totally safe structures. Based on the available information, the design philosophies have changed over the years. In the last three decades, risk-based design has become an integral part. Several methods with various degrees of sophistication are now available. They are presented in this chapter. Some of the future trends in the reliability-based design in civil engineering are also presented. Considering some emerging areas, multidisciplinary efforts are encouraged.

References

[1] Haldar A. Structural engineering in the new millennium: Opportunities and challenges. Plenary Lecture, International Conference on Civil Engineering in the New Millennium: Opportunities and Challenges (Cenem-2007), Bengal Engineering and Science University, India, January, 2007; 44–56.

[2] West HH. Analysis of structures – An integration of classical and modern methods. 2nd Edition. Wiley, New York, 1989.

[3] Freudenthal AM. Safety and the probability of structural failure. ASCE Transactions 1956; 121:1337–1397.

[4] Benjamin JR. Cornell CA. Probability, Statistics, and decision for civil engineers. McGraw-Hill, New York, 1970.

[5] Ang A H-S, Tang WH. Probability concepts in engineering design, Vol. 1: Basic Principles. Wiley, New York, 1975.

[6] Ang A H-S, Tang WH. Probability concepts in engineering design, Vol. II: Decision, risk and reliability.Wiley, New York, 1984.

[7] Haldar A, Mahadevan S. Probability, reliability, and statistical methods in engineering design. Wiley, New York, 2000

[8] Haldar A, Mahadevan S. Reliability assessment using stochastic finite element analysis. Wiley, New York, 2000.

[9] American Concrete Institute (ACI). Building code requirements for structural concrete. Farmington Hills, MI, 1999; ACI: 318–399.

[10] American Concrete Institute (ACI), Building code requirements for structural concrete, Farmington Hills, MI., 2002; ACI: 318–302.

[11] American Concrete Institute (ACI). Building code requirements for masonry structures and specification for masonry structures – 2002, ACI 530-02/ASCE 5-02/TMS 402-02, reported by the Masonry Standards Joint Committee, 2002.

[12] American Society of Civil Engineers (ASCE). Standard for load and resistance factor design (LRFD) for engineered wood construction, ASCE, 1995; 16–95.
[13] American Wood Council, The load and resistance factor design (LRFD) manual for engineered wood construction, Washington, D.C., 1996.
[14] American Institute of Steel Construction (AISC). AISC, manual of steel construction load and resistance factor design. 1st Edition, 2nd Edition, and 3rd Edition, Chicago, IL, 1986, 1994, 2001.
[15] American Institute of Steel Construction (AISC). Manual of steel construction allowable stress design. 9th Edition, Chicago, IL, 1989.
[16] Ellingwood B, Galambos TV, MacGregor JG, Cornell CA. Development of a probability based load criterion for American standard A58: Building code requirements for minimum design loads in buildings and other structure. Special Publication 577, National Bureau of Standards, Washington, D.C., 1980.
[17] Bjorhovde R, Galambos TV, Ravindra MK. LRFD Criteria for steel beam-columns. Journal of Structural Engineering, ASCE 1978; 104(9):1371–1388.
[18] Cornell CC. A probability-based structural code. Journal of the American Concrete Institute 1969; 66(12):974–985.
[19] Rosenbleuth E, Esteva L. Reliability bases for some mexican codes. ACI Publication, 1972; SP-31:1–41.
[20] Ayyub BM, Haldar A. Practical structural reliability techniques. Journal of Structural Engineering, ASCE 1984; 110(8):1707–1724.
[21] Hasofar AM, Lind NC. Exact and invariant second moment code format. Journal of Engineering Mechanics, ASCE 1974; 100(EM1):111–121.
[22] Rackwitz R, Fiessler B. Note on discrete safety checking when using non-nornal stochastic models for basic variables. Load Project Working Session, MIT, Cambridge, MA, 1976.
[23] Haldar A. (Ed.). Recent developments in reliability-based civil engineering. World Scientific, Singapore., 2006.
[24] Haldar, A, Marek P. Role of simulation in engineering design. Proceedings of the 9th International Conference on Applications of Statistics and Probability (ICASP9-2003) 2003; 2:945–950.
[25] Marek P, Haldar A, Guštar M, Tikalsky P. Editors, Euro-SiBRAM‘2002 Colloquium Proceedings, ITAM Academy of Sciences of the Czech Republic, 2002.
[26] Lewis PAW, Orav EJ. Simulation methodology for statisticians, operations analysts, and engineers. Wadsworth and Brooks/Cole Advanced Books and Software, Pacific Grove, CA, 1989; 1.
[27] Haldar A, Ayyub BM. Practical variance reduction techniques in simulation. Advances in Probabilistic Structural Mechanics – 1984, ASME, 1984; PVP -93:63–74.
[28] Huh J, Haldar A. Stochastic finite element-based seismic risk evaluation for nonlinear structures. Journal of the Structural Engineering, ASCE 2001; 127(3):323–329.
[29] Huh J, Haldar A. Seismic reliability of nonlinear frames with PR connections using systematic RSM. Probabilistic Engineering Mechanics 2002; 17(2):177–190.
[30] Cruse TA, Burnside OH, Wu Y-T, Polch EZ, Dias JB. Probabilistic structural analysis methods for select space propulsion system structural components (PSAM). Computers and Structures 1988; 29(5):891–901.
[31] Southwest Research Institute, NEUSS, San Antonio, Texas, 1991.
[32] Veritas Sesam Systtems, PROBAN, Houston, Texas, 1991.
[33] Liu P-L, Lin H-Z, Der Kiureghian, A., CALREL, University of California, Berkeley, California, 1989.
[34] McKenna, F., Fenves, G.L., and Scott, M.H., Open system for earthquake engineering simulation. http://opensees.berkeley.edu/, Pacific Earthquake Engineering Research Center, Berkeley, CA., 2002.
[35] Proppe C, Pradlwarter HJ, Schueller GI. Software for stochastic structural analysis – Needs and requirements. Proceedings of the 4th International Conference on Structural Safety and Reliability, Corotis, R.B., Schueller, G.I., and Shinizuka, M., Eds., 2001.
[36] COSSAN (Computational Stochastic Structural Analysis) – Stand – Alone Toolbox, User’s Manual, IfM – Nr: A, Institute of Engineering Mechanics, Leopold – Franzens University, Innsbruck, Austria, 1996.
[37] Ayyub BM, Klir GJ. Uncertainty modeling and analysis in Engineering and the sciences, Chapman and Hall/CRC, Boca Raton, FL, 2006.
[38] Haldar A, Reddy RK. A random-fuzzy analysis of existing structures. Journal of Fuzzy Sets and Systems 1992; 48(2);201–210.
[39] Kartam N, Flood I, Garrett JH. Artificial neural networks for civil engineers. American Society of Civil Engineers, 1997.

[40] Liu GR. Mesh free methods – Moving beyond the finite element method. CRC Press, Boca Raton, FL., 2002.
[41] Rahman S. Chapter 10 – Meshfree methods in computational stochastic mechanics. In: Haldar A, editor. Recent developments in reliability-based civil engineering. World Scientific, Singapore, 2006; 187–211.
[42] Chakraborty S, Haldar A. Robust optimization under uncertainty. Proceedings of the 3rd International Conference on Reliability, Safety and Hazard, (ICRESH-05), December 1–3 2005 Mumbai, India, Narosa Publishers, New Delhi.
[43] Onwubolu GC, Babu BV. New optimization techniques in engineering, Springer, Berlin, 2004.
[44] Lee K, Park G. Robust optimization considering tolerances of design variables. Computers and Structures 2001; 79:77–86.
[45] Doltsinis I, Kang Z, Cheng G. Robust design of non-linear structures using optimization methods. Journal of Computer Methods in Applied Mechanics and Engineering, 2005; 194:1779–1795.
[46] Chen W, Sahai A, Messac A, Sundararaj GJ. Exploration of the effectiveness of physical programming in robust design. ASME Journal of Mechanical Design 2000; 122:155–162.
[47] Messac A, Ismail-Yahaya A. Multi-objective robust design using physical programming. Structural and Multidisciplinary Optimization, 2002; 23(5):357–371.
[48] Rackwitz R. Chapter 2 – Socio-economic risk acceptability criteria. In: Haldar A, editor. Recent developments in reliability-based civil engineering. World Scientific, Singapore, 2006; 21–31.
[49] Ansari F. (Ed.), Sensing issues in civil structural health monitoring. Springer, Dordrecht, The Netherlands, 2005.
[50] Wang D, Haldar A. An element level SI with unknown input information. Journal of the Engineering Mechanics Division, ASCE 1994; 120(1):159–176.
[51] Wang D, Haldar A. System identification with limited observations and without input. Journal of Engineering Mechanics, ASCE 1997:123(5): 504–511.
[52] Ling X, Haldar A. Element level system identification with unknown input with rayleigh damping. Journal of Engineering Mechanics, ASCE, 2004; 130(8):877–885.
[53] Vo PH, Haldar A. Health assessment of beams – Theoretical formulation and analytical verification. Structure and Infrastructure Engineering. 2008; 4(1): 33–44
[54] Vo PH, Haldar A. Health assessment of beams – experimental verification. Structure and Infrastructure Engineering. 2008; 4(1): 45-56.
[55] Katkhuda H, Flores RM. Haldar A. Health assessment at local level with unknown input excitation. Journal of the Structural Engineering ASCE, 2005; 131(6):956–965.
[56] Zhao Z, Haldar A, Breen FL. Fatigue reliability updating through inspections for bridges. Journal of the Structural Division, ASCE 1994; 120(5):1624–1642.
[57] Das P, Frangopol DM, Nowak AS. Current and future trends in bridge design, construction and maintenance. Thomas Telford, London, 1999.
[58] Martinez-Flores R, Katkhuda H, Haldar A. Structural performance assessment with minimum uncertainty-filled information. International Journal of Performability Engineering, April 2008; 4(2): 121–140.
[59] Chowdhury M, Haldar A. Chapter 4 –Performance based reliability evaluation of structure-foundation systems. In: Haldar A, editor. Recent developments in reliability-based civil engineering. World Scientific, Singapore, 2006; 55–75.

64

Performability Issues in Wireless Communication Networks

Sieteng Soh[1], Suresh Rai[2], and Richard R. Brooks[3]

[1] Department of Computing, Curtin University of Technology, Perth, Western Australia.
[2] Department of Electrical and Computer Engineering, Louisiana State University, Baton Rouge, LA, USA.
[3] Holcombe Department of Electrical and Computer Engineering, Clemson University, SC, USA.

Abstract: This chapter discusses the performability models for WCN. The reliability issues, such as component failure models and evaluations that are relevant to WCN are described. System communication models for WCN, including the many-sources-to-terminal model widely used in WSN, are described. The performability evaluations of two typical WCN environments: static topology and the *ad hoc* network are described in detail. This chapter also discusses recent techniques to improve the end-to-end routing reliability in MANET.

64.1 Introduction

Performability analysis of a communication network (CN) is very important as it helps gauge the resiliency of the network in meeting some user quality of service requirement. Techniques to analyze and to improve the performability of the wired CN are extensively described in the literature. A wireless CN (WCN), in many ways, is different from the traditional CN and, consequently, its performability issues are also different in several ways. The proliferations of WCN, such as mobile *ad hoc* networks (MANET), and wireless sensor networks (WSN), make their performability issues equally important, if not even more important, because a WCN is more complex in nature than the wired CN, its components are less resourceful, and the components are more susceptible to failures. Limited resources (*e.g.*, battery, memory, and bandwidth) reduce the intrinsic performance and reliability of WCN, and thus methods to improve the metrics in WCN are imperative. The node mobility in WCN makes network links have higher unavailability rates and makes the performability analysis of a WCN even more difficult.

The performability issues of a *wired* or *wireless* CN, through which data are expected to traverse from one or many sources to one or many destinations, are increasingly becoming more critical with increasing user dependency on the network services. In general, the performability analysis of a CN starts with its communication performance model, which is defined by the user *quality–of–service* (QoS) requirements, and its reliability model. The performability metric of a CN, thus, indicates the reliability of the system in meeting the user QoS requirement. Refer to [1] and [2] for QoS and reliability models, respectively.

The conveniences advanced by wireless communication devices (*e.g.*, cellular phones), and

the technological advances in portable–lightweight computers (*e.g.*, laptops and PDAs), among others, have triggered the proliferations and set the *future trends* of the uses of WCN around the world [3].

A WCN comprises a set of nodes each of which is capable of transmitting to or receiving from other nodes. The nodes in the network, among others, can be a computer, concentrator, end user terminal, mobile station, repeater acting as a transmitter/receiver, or a sensor node. Two nodes in a WCN, in contrast to a *wired* CN, are connected by wireless communication links either directly (without infrastructure – the *ad hoc* mode) or through a base station (the infrastructure mode). In an *ad hoc* WCN, the wireless nodes communicate with each other without using a fixed infrastructure, and when two nodes are not within their transmission range, the intermediate nodes relay the messages between nodes. In some networking environments, such as wireless home or office with stationary workstations, the network nodes are wireless but non–mobile (*stationary*). In others, the network nodes are both wireless and *mobile* [3]. The stationary nodes form a fix topology or a random topology (*ad hoc*), if deployed randomly. An *ad hoc* network with mobile nodes is a *mobile wireless ad hoc network* (MANET). MANET is a new frontier for WCN and is different from a traditional WCN in many ways. One major difference is that a routing path in MANET uses a sequence of *mobile* nodes, a wireless link connecting each pair of the nodes. The *wireless sensor network* (WSN) is another class of WCN. Nodes in WSN, forming a certain topology, can be mobile or stationary and deployed randomly (*ad hoc*). Typically, a WSN comprises more but less resourceful nodes than those in the other types of WCN.

The WCN introduces many communication/network–related challenges that, in many ways, differ from those considered in the traditional wired CN [3]. This chapter typically views the differences from their communication system performability issues.

While there has been much effort directed towards performability analysis in wired CN [2], there has been less treatment of WCN, partially because (i) some WCN performability issues are application specific and (ii) it is relatively new. The performability issues in a non-*ad hoc* and non-mobile WCN can be solved directly using the existing techniques for wired CN because nodes in both networks are stationary. However, the *ad hoc* nature and/or nodes mobility and the node's limited resources (*e.g.*, battery lifetime), which are typical characteristics of the other WCN models, require different treatments. For example, one of the main causes to node failures in WCN is due to limited battery lifetime. Thus, techniques (*e.g.*, routing) put more emphasis on reducing battery consumption and sacrifice performances typical to wired CN. Performability evaluation of a fixed topology WCN, with operational links, emphasizes node stability. Alternatively, with node mobility, link unavailability is more critical in the performability evaluation of MANET. Further, the many-to-one-terminal communication model (Section 64.2.2.2), used for data acquisition analysis of WSN applications, should also be taken into account.

The lay out of the chapter is as follows. In Section 64.2, we present various system models, including the reliability models, assumptions, and communication and component failure models of WCN. Section 64.3 presents three examples of performability analysis and improvement methods used in WCN. It describes the performability analysis of the static topology of WCN and MANET. It also surveys recent approaches to improve the end-to-end path reliability in MANET. Finally, we conclude this chapter in Section 64.4.

64.2 System Models

64.2.1 Reliability Models and Assumptions

Due to the nature of the problem, this chapter does not describe the stochastic models based on the Markov or semi-Markov models. This, however, presents a combinatorial (non-state-space) model. Examples for this model include the reliability block diagram (RBD), fault trees (FT without or with repeated events), and probabilistic graphs (PG). The RBD shows the functional relationships among resources and indicates which system elements must operate to accomplish the intended

function successfully. An FT maps the operational dependency of a system on its components. However, unlike an RBD, the FT represents a probability of failure approach to system modeling. The phrase *without repeated events* means that inputs to all the gates are distinct, while *with repeated events* assumes non-distinct inputs. The PG models the system as a graph, wherein each node is a computing unit (or processing entity) and links denote communication lines between them. In this chapter, the PG model describes the various WCN reliability issues.

The following assumptions, made for the WCN performability analysis, are helpful in making the reliability computation tractable: (i) All elements (nodes and links) of the network are always in active mode (no standby or switched redundancy); (ii) The state of each element i of the network is either *operating* with a probability p_i or *failed* with probability q_i; $p_i + q_i = 1$. Thus, the probability is $p_i = 1 - \frac{MTTR_i}{MTBF_i}$, where $MTTR_i$ ($MTBF_i$) refers to the mean time to repair (mean time between failures) of a component i. Section 64.2.3 describes other WCN component failure models; (iii) The states of all elements are statistically independent; and (iv) Graph model of WCN is free from directed cycles and self-loops.

64.2.2 System Communication Models and Reliability Measures

64.2.2.1 Overview

Refer to [36] for a number of reliability measures. We use one or more of the following categories:

- *two-terminal* or (s,t) reliability is the probability that a source node s communicates with a terminal node t.
- *All-terminal* reliability is the probability that all operative nodes communicate.
- *K-terminal* or source-to-many terminals (SMT) reliability is the probability of a source node s communicating with some K ($K \geq 1$) operative terminal nodes.
- *Many-sources-to-terminal* (MST) reliability is the probability that some K ($K \geq 1$) nodes communicate with a terminal node t.

The network (modeled as $G(V,E)$) reliability $R_K(G)$, for a set of specified nodes $K \subseteq V$, is the probability that all elements of at least one minpath are working. Here $V(E)$ is the set of nodes (links) in G. Note, the minpath depends on the specified set K as well as the reliability measure and system QoS under consideration. For $K = 2$, $R_K(G)$ is the *two-terminal* reliability and a minpath is a simple path between an (s,t)-node pair. Reference [2] provides the definitions of a simple path, and algorithms to enumerate them. For $K=V$, $R_K(G)$ is *all-terminal* reliability, an important measure for reliable broad-casting in a CN. SMT reliability is applicable for the resiliency issue of network multi-casting. The MST reliability, on the other hand, analyzes the reliability of a WSN. Table 64.1 lists models and their applications. This chapter uses the s-t model.

Table 64.1. Various WCN communication models

Models		Example applications
1	Unicast (s,t)	Event transmission from the sensor to the user.
2	Multi-cast (s,T_i)	User tasking/query dissemination to several target sensors.
3	Broadcast (s,T)	user tasking/ query dissemination to all target sensors.
4	Many-to-one (S,t)	Sensor data aggregation to a user.
4.1	(1-of-S, t)	Bush-fire and intrusion detection in one sensor field.
4.2	(k-of-S, t)	GPS that uses k=3 satellites to determine locations.
4.3	(k_i-of-S_i, t)	Climate data acquisition (multi-modal – temperature, pressure, humidity).

From the performance aspect, *delay* guarantee, among others, is widely used QoS metric in CN. Several path routing algorithms consider that a transmitted message can reach its destination within the required delay constraint [4]. The routing problem in the most general form is NP-complete, and to make the problem tractable the routing path delay measure allows only the total number of links or nodes (hop count) that a message needs to traverse to reach its destination. Nevertheless, hop count measure arguably captures network cost and, thus, minimizing path length

(hop count) becomes one of the criteria for computing efficient routing paths [5]. This chapter uses the hop count QoS in WCN.

64.2.2.2 MST Reliability

A WSN consists of a large number of sensor nodes. Here each node has some means of communication and sensor mechanisms. The sensor nodes, deployed randomly, form some regular geometric topology over a wide area sensor field [6], and send data (event) to a sink. In a multi--hop WSN, the sensor nodes are located beyond the distance range of the communication media from the sink; thus, the data pass through intermediate nodes.

WSN has been proposed for various critical monitoring systems such as battlefield surveillance, nuclear, biological and chemical attack detection, forest fire detection, flood detection, and precision agriculture using various communication models. Data dissemination in WSN is categorized into *tasks* (sink to sensors, Models 1 to 3 in Table 64.1) and *events* (sensors to sink, Models 1 and 4 in Table 64.1). Regardless of the application, data dissemination is often event driven and reliable. Its timely event detection is critical [6] because it starts appropriate actions as quickly as possible. For applications requiring uni-modal information, the group of sensor nodes may send redundant information, and the sink requires only one or several of them to arrive (Models 1, 4.1 and 4.2) before it can start reacting to the occurring event. For example, consider a WSN with many redundant target sensors to monitor a remote bush fire, and each target sensor is expected to send an alarm signal to the sink as soon as it detects fire. Model 4.3 groups the sensors. Each group monitors a different class of phenomena. (It is a multi--modal data acquisition.] This model also applies to climate monitoring and various surveillance systems.

The widely adopted *directed diffusion* paradigm [7] for WSN includes an event acquisition mechanism that is robust to node failures, where the transmitted signals may still reach the sink through alternative paths. However, alternative paths may increase the number of hops that messages have to traverse (before reaching the sink). Thus, the overall *expected hop count* (EHC) goes up. Most WSN applications (*e.g.*, battlefield surveillance, nuclear, and biological and chemical attack detection) require end-to-end delay-constraints. In addition, given the resource-limited nature of WSN and the delay-sensitive nature of their applications, evaluating and improving the performability of WCN become critical, leading to a *new trend* in the research area.

64.2.2.3 (s,t) Reliability

The (*s*,*t*) reliability measure or its variance (like average terminal reliability, node-to-node grade of service, end-to-end blocking, functional reliability, *etc*.) is widely known in the literature.

The (*s*,*t*) reliability depends on the availability of each link and/or node in the path. Section 64.2.3 discusses the causes of link and node failures in WCN and the typical methods used to measure the link/node reliability metric. Section 64.3.1 extends the (*s*,*t*) reliability measure for a WCN with fixed topology that uses average hop count and node availability parameters, while considering perfect links. In contrast, Section 64.3.2, considers a random graph model [8] used to analyze the connectivity of mobile ad hoc WCN with link failures and perfect nodes. Topological changes in MANET make (*s*,*t*) paths frequently broken [9] that negatively affect the efficiency (since each path failure recovery is costly [10]) and the per-formability of the network. Therefore improving the end-to-end path reliability in the network is critical, and is arguably more important in MANET's path selection than other QoS metrics commonly used in the traditional wired CNs [10]. Multi-path routing improves the end-to-end performability in WCN [11, 12]. In Section 64.3.3, we present a survey on recent techniques to enhance the end-to-end performability in MANET.

64.2.3 Component Failure Models

In the wired CN, the network system components (nodes and links) fail randomly due to component wear out, natural catastrophes, software bugs, or deliberate acts (*e.g.*, terrorist attacks). On top of these sources of failure, the use of wireless links, nodes mobility, and limited battery lifetime in a

WCN provide other reasons for component unavailability. Thus, the performability issue in a WCN is more challenging than that in wired CN. This chapter uses availability (unavailability) and reliability (failures) interchangeably.

Reference [13] considers node unavailability in analyzing the reliability and EHC of a fixed topology WSN. The harsh nature of WSN deployment environment makes the sensor nodes subject to random failures. The reliability of a sensor node, $p(t)=e^{-\lambda t}$, is modeled using the Poisson distribution to capture the probability of operational within a time interval $(0,t)$, where λ is the failure rate of the node. Researchers have considered robust sensor systems using evolvable hardware [14] that emphasizes on the robustness of a system with respect to sensor failures.

Alternatively, sensor nodes are unavailable due to power failures. Brooks *et al.* [15] considered node failure only when the battery power is exhausted. They [15] used three methods: data agreement, communication range managements, and node positioning to extend the effective lifetime of the WSN. To achieve better performability, applications (*e.g.*, routing methods) are designed emphasizing on conserving node battery lifetime, and a better understanding on the power consumptions of operations (*e.g.*, communication, program computation) in sensor nodes. Section 64.2.3.1 describes the various energy consumptions in several typical node operations.

In MANET, node mobility is the main source of link failures. Some links break when nodes move out of range of each other. Interferences on the wireless medium may also cause the link failures. Section 64.2.3.2 presents a typical approach to compute the link availability in MANET.

64.2.3.1 Energy Consumption in WSN

Sensor networks rely on battery power. Reference [16] considers the use of ambient energy sources for sensor networks and concludes this is not currently feasible. Reliance on limited, non-renewable battery energy resources means that all aspects of sensor networks need to be as energy efficient as possible. Refer to [6] and [17] for a discussion on energy model for sensor networks, which must consider all aspects of node behavior.

From the empirical analysis of the sensor node, power consumption in [18] suggests the following: (i) For most commercial ARM8 processor instructions, the energy required is 4.3×10^{-9} joules per bit. Multiplication requires 31.9×10^{-9} joules per bit; (ii) The Berkeley smart dust prototypes consume ~ 0.05×10^{-9} joules per bit for most instructions (multiplication is not supported); (iii) Radio frequency ground communications require 10^{-7} joules per bit for 0–50 meters, and 50×10^{-6} joules per bit for 1–10 kilometers.

These figures are lower bounds, based on ongoing research programs. Commercial products are unlikely to reach these levels of efficiency in the near future: (i) Per bit energy consumption for multiply instructions on commercial processors is in the range 48 to 0.84×10^{-9} joules per bit [19]; (ii) Communications require from 40 to 0.1×10^{-6} joules per bit [18]; (iii) Reception energy needs are 2×10^{-6} (GSM) and 10^{-7} (Bluetooth) joules per bit for. [18].

Energy requirements for communications are proportional to $r^{-\alpha}$ where r is communication range in meters. The α exponent is between 2 and 5. A value of 3 is reasonable for many applications [20]. For commercial and prototype systems, transmitting one bit for one hop is on the order 10^2 times more expensive than computing one instruction on one bit.

References [18] and [21] claim transmission energy is the dominant drain on sensor networks when per hop communication is over 10 meters. This claim is based on three applications that have minimal on-board computation. Two examples in [18] only sample data, do an analog-to-digital conversion, execute a filter and transmit data. The other example does a least squares estimate of vehicle velocity from five data samples. This amounts to executing one very small matrix multiplication. For nodes that perform minimal to no local data processing, communications energy consumption is certain to be greater than the computation energy requirements.

Empirical tests [15] show that, for many sensor network applications, computation dominates energy consumption. Consider the two tracking approaches: beamforming and closest point of approach (CPA). Beamforming [22–25] is a form

of spatial filter that aggregates output from a group of sensor nodes placed locally. CPA [26–29] techniques involve using the output from a single sensor node, usually the node closest to the event. The beamforming approach is more accurate, while requiring $\sim 10^3$ times more energy. Beamforming is computation intensive, performing cross-correlation over multiple time series to estimate signal direction of arrival. The CPA based approach requires minimal computation. Energy need for communications uses the Bluetooth energy per bit. Communication was responsible for less than 20% of the total energy drain.

In the security domain, both [19] and [30] show that encryption, decryption, and secure hashing are computation intensive, with a large energy overhead. References [19] and [31] measure the energy drain of key initialization communications.

64.2.3.2 Computing Link Availability in MANET

In MANET nodes mobility is the main source of link unavailability, and due to high cost in recovering from a routing path failure, path reliability is of utmost important [10]. The most direct technique to compute the link availability in MANET is by taking a snapshot of the network topology, assuming the positions of the nodes are likely to be fixed for a period of time. However, such assumption may not be justifiable considering the dynamic nature of MANET.

Recently Jiang, *et al.* [10] proposed a prediction-based link availability estimation; they used a pair $(T_p, L(T_p)]$ to quantify link availability in MANET. For a link that is available at time t_0, $T_p > 0$ is the predicted maximum time period that the link will be continuously available until $t_0 + T_p$. Assuming both nodes associated with the link keep their current velocities (*i.e.*, speed and direction) between time t_0 and $t_0 + T_p$, the parameter T_p can be predicted accurately [10]. Then, relaxing the assumption (*i.e.*, allowing possible changes in the node velocities) and using T_p, they [10] show how to compute the link availability estimation $L(T_p)$, which is defined as the probability that the link will be available continuously during time period T_p. Then, the link reliability metric is computed as $r_l = T_p \times L(T_p)$, which is then used in [10] to develop a routing algorithm to maximize end-to-end path reliability. Note that T_p by itself is not sufficient to gauge the availability of a link. For example [10], the reliability metrics of links l_1 (T_p=10 s, $L(T_p)$=0.001) and l_2 (T_p=5 s, $L(T_p)$=0.1) are 0.01 and 0.5, respectively, and thus link l_2 is more reliable. Reference [32] shows an enhanced $L(T_p)$ estimation which gives a better accuracy than that obtained in [10], and reference [33] proposes a technique to predict link availability $L(T)$, for any time duration T. This later technique is more suitable for multi-media streaming application. Other link availability predictors for MANET are discussed in [10] and [33].

Brooks, *et al.* [8] used a random graph to model an *ad hoc* WCN. The *ad hoc* network is represented by its graph connectivity matrix, where each matrix element is the Bernoulli probability giving the link availability between two corresponding nodes. Section 64.3.2 describes the details of the random graph approach.

64.3 Performability Analysis and Improvement of WCN

64.3.1 Example I: Computing Reliability and Expected Hop Count of WCN

Reference [34] uses a probabilistic graph G to represent a static topology WCN, and describes two algorithms: Alg1 and Alg2, to compute the (s,t) reliability $TR(G)$ and the EHC of the network with probabilistic node failures. Alg1 is based on complete-state enumeration, while Alg2 avoids generating all network states by utilizing breadth-first-search to recursively obtain all (s,t) shortest paths and the factoring theorem [2] to make each newly generated state disjoint from the previous states. The technique is recursively expressed as

$$TR(G) = p_i\, TR(G|\text{ node } i \text{ is functional}) + (1-p_i)\, TR(G|\text{ node } i \text{ is not operational}), \quad (64.1)$$

where p_i is the probability that node i in G is functional. Note that (64.1) uses the concept of Shannon's expansion principle in Boolean logic for reliability modeling. Several researchers have developed factoring algorithms that implement the

series-parallel probability reductions and polygon reductions and use optimal link-selection strategies. It is important to note that this method can be employed using the graph representation, without knowing the connectivity information (*i.e.*, minpath, mincut, or spanning tree). Note that the factoring approach represents each disjoint term in single-variable inversion (SVI) notation [36], and the approach performs worst on a WCN whose (*s*,*t*) simple paths are disjoint paths. The SVI-based technique requires $1+\sum_{j=2}^{m}\prod_{i=1}^{j-1}|P_i|$ disjoint terms to represent *m* disjoint paths $P_1, P_2, \ldots, P_m$, where $|P_i|$ represents the number of nodes in path *i*. For this case, [34] provides a polynomial time approach (Alg3) to compute the reliability and EHC of the network. Another polynomial time algorithm (Alg4) in [34] is also proposed for computing the reliability measures of a WCN that can be represented as an interval-graph [35]. However, when the WCN has all but one or a few disjoint paths, we cannot use Alg3 to compute its reliability measure, and Alg2 performs worst for this case. Similarly, when the network forms an "almost interval-graph" Alg4 is inappropriate to use [37].

This section proposes a two-step approach to compute *TR*(*G*) and EHC that was first presented in [37]. First, all (*s*,*t*) simple paths (considering only the nodes) of the WCN are generated and sorted in increasing cardinality (hence shortest path first) order. Reference [37] describes two algorithms that enumerates the (*s*,*t*) paths of WCN: one for general networks, and the other for interval graphs (described in Section 64.3.1.2). In the second step, the approach uses a multi-variable inversion (MVI)-based sum-of-disjoint-products (SDP) [38] technique to generate the mutually disjoint terms (*mdt*) for the paths. Simulations on general networks reported in the literature [37] showed that the SDP-based technique is several orders of magnitude faster than the factoring technique. In addition, the technique solves the reliability metrics of WCN that contains all (*s*,*t*) disjoint-paths in time polynomial in the order of the number of its nodes. From the sorted paths in each of randomly generated interval graphs, an SDP technique [38] generates one *mdt* for each path, and it was conjectured in [37] that the two-step approach solves the *TR*(*G*) and EHC of an interval-graph in time polynomial in the order of simple paths. Reference [37] also presents the applications of the technique in WCN topology designs and their performability improvements.

64.3.1.1 Concepts

A. System Model and Representation

In the undirected graph model *G*(*V*,*E*) of a WCN, each node in *V* represents a site or a repeater in the network, and each link in *E* denotes a communication service. Two nodes are connected if the nodes are within the communication range of each other. A node is said to be *up* (*down*) if it is operational (failed). Links (*E*) are assumed to be always *operational*. An *up* (*down*) node is denoted by a Boolean expression v_j ($\overline{v_j}$). A Boolean expression $\overline{v_1}v_4 + \overline{v_3}v_4$, for example, represents an operational condition when nodes v_1 and/or v_3 fail, as long as node v_4 is operational. Note, it is *single-variable inversion* (SVI) representation [36]. The expression can also be represented concisely as $\overline{v_1 v_3} v_4$, where the inversion of multiple variables is allowed. This latter representation is *multi-variable inversion* (MVI) [36]. Let p_j (resp. q_j=1–p_j) be the operational (resp. failure) probability of a node v_j, and assume node failures are statistically independent. An (*s*,*t*) *simple* (node) path *i*, P_i, from a source node *s* to a terminal node *t* is formed by the set of *up* nodes such that no nodes are traversed more than once. In other words, $P_i = (v_0, v_1, \ldots, v_{k-1}, v_k)$, where v_0=*s*, v_k=*t*, and each 2 sequenced nodes in the path are connected by a link $e \in E$. An (*s*,*t*) path P_i is redundant with respect to an (*s*,*t*) *simple* path P_j if P_i contains all nodes in P_j. The WCN (Figure 64.1) has $P_{s,t}$={(*s*,*a*,*b*,*d*,*t*), (*s*,*a*,*c*,*e*,*d*,*t*), (*s*,*a*,*c*,*e*,*j*,*t*), (*s*,*f*,*c*,*e*,*d*,*t*), (*s*,*f*,*c*,*e*,*j*,*t*), (*s*,*f*,*g*,*h*,*i*,*j*,*t*)}.

B. The SDP Technique

Consider an (*s*,*t*) pathset $P_{s,t}=\{P_1, P_2, \ldots, P_{m-1}, P_m\}$ of a network *G*, and let E_i represent an event that all nodes in a simple path P_i operate. These events are not mutually disjoint. Making the events mutually disjoint is necessary to help generate an equivalent probability expression. This is a complex problem in the field of system reliability

as the reliability problem is NP-hard [2]. Reference [36] provides a survey of efficient SDP techniques.

64.3.1.2 (s,t) Simple-path Generators

A. General Networks

Path generators in the literature [2] consider an (*s*,*t*) simple path as a sequence of links that connect the node pair. We can use any existing link-based path generator [2] to obtain an (*s*,*t*) simple (link) pathset, which can be converted into its equivalent (*s*,*t*) simple (node) pathset. However, the approach incurs path redundancy tests. Consider the network in Figure 64.1 and its two non-redundant simple (link) paths ((*s*,*a*),(*a*,*b*),(*b*,*d*),(*d*,*t*)) and ((*s*,*a*),(*a*,*b*),(*b*,*d*), (*d*,*e*),(*e*,*j*),(*j*,*t*)). Converting the paths considering nodes, we obtain paths (*s*,*a*,*b*,*d*,*t*), and (*s*,*a*,*b*,*d*,*e*,*j*,*t*), respectively, where the second path is redundant. Reference [37] describes an efficient recursive function that enumerates all non-redundant simple (node) paths of an undirected graph *G*(*V*,*E*). The path generator [37] does not generate any redundant simple (node) paths, and therefore no path redundancy checks are required.

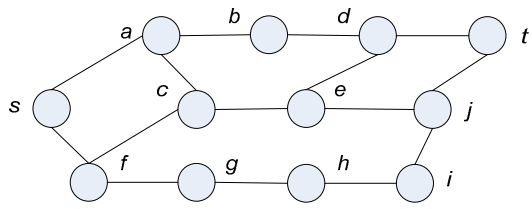
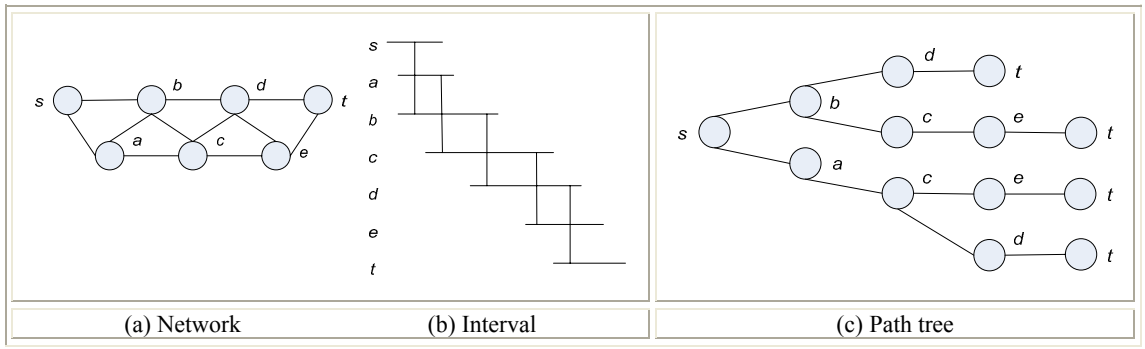


Figure 64.1. A 12-node, 15 links WCN

B. Interval Graph

An undirected graph *G* is an interval-graph if its nodes can be put into one-to-one correspondence with a set of intervals of a linearly ordered set such that two nodes are connected by a link in *G* if and only if their corresponding intervals have nonempty intersections [35]. An interval-graph has been proposed in the literature to model a WCN where the intersection of the range of transmission can be represented by its intersecting intervals [34]. Figure 64.2 shows an interval-graph and its interval representation. An interval-graph $G(V,E,C,\sigma)$ has a *perfect elimination sequence* $\sigma=(v_1,v_2, \ldots,v_n)$ of nodes in V and a sequence of maximal cliques $C=(C_1,C_2, \ldots,C_\kappa)$ of G such that maximal cliques containing one node occur consecutively [34]. For a WCN, $s= v_1$, and $t = v_n$, and the interval-graph in Figure 64.2 has σ = (*s*,*a*,*b*,*c*,*d*,*e*,*t*), and C = ({*s*,*a*,*b*}, {*a*,*b*,*c*}, {*b*,*c*,*d*}, {*c*,*d*,*e*}, {*d*,*e*,*t*}); both σ and C can be generated in linear time [35]. Notice that the cliques that contain node *c* are listed in consecutive order in C. Let us define $\tau=(\hat{v}_1, \hat{v}_2, \ldots, \hat{v}_n)$, where $\hat{v}_i \in \{1,2, \ldots,\kappa\}$ denotes the largest clique number in C for v_i such that $v_i \in C_{\hat{v}_i}$. Node *c* in Figure 64.2(a) appears in cliques C_2, C_3, and C_4, and therefore $\hat{v}_4=\hat{c}=$ max{2,3,4}=4. Similarly, the largest clique numbers for nodes *s*, *a*, *b*, *d*, *e*, and *t* are 1, 2, 3, 5, 5, and 5, and τ=(1,2,3,4,5,5,5).

Soh, *et al*. [37] proposed a function *NPG_IG*() that utilizes the preprocessed cliques in an interval graph to generate the (*s*,*t*) simple pathset.



(a) Network (b) Interval (c) Path tree

Figure 64.2. A 7-node, 11 link interval-graph

The function generates the path tree in Figure 64.2(c) for the interval graph of Figure 64.2(a). The tree represents $P_{s,t}$={(*s*,*b*,*d*,*t*), (*s*,*b*,*c*,*e*,*t*), (*s*,*a*,*c*,*e*,*t*), (*s*,*a*,*c*,*d*,*t*)}.

64.3.1.3 SDP Technique to Computing the Reliability and EHC of Static Topology WCN

Let $P(l)$ be the probability that the source node *s* is connected to the terminal node *t* with a *shortest* path of length $1 \le l \le n-1$. Without loss of generality, we assume that the source node *s* is always *up*, while the terminal node *t* may fail with certain probability. The expected hop count (EHC) between a source node *s* and a terminal node *t* in a WCN is computed as [34]:

$$EHC = \left(\sum_{l=1}^{l=k-1} lP(l) \Big/ \sum_{l=1}^{l=k-1} P(l) \right). \qquad (64.2)$$

Equation (64.2) assumes that the routing protocol in the network always finds the available (*s*,*t*) shortest path. When path is unavailable (*e.g.*, because of failure node) the router finds the next possible shortest path with the same or longer hop count. The problem of computing EHC has been shown #P-hard [34]. Figure 64.3 shows an efficient SDP approach to compute the reliability measures. The algorithm utilizes a path generator [37] to generate the (*s*,*t)* simple (node)-pathset of a WCN. Step 2 of the algorithm sorts the paths in the increasing cardinality order. This step is required to model the aforementioned routing protocol (*i.e.*, shortest path first). It is also suited well for an SDP technique because the algorithm runs more efficiently when the input paths are sorted in increasing cardinality order [39]. In Step 3, an MVI-based SDP technique computes $P(l)$ from each path in $P_{s,t}$ that has cardinality *l*, for $1 \le l \le k-1$. Finally, Step 4 uses (64.2) to compute the *EHC* of the network.

To illustrate EHC_SDP, consider the WCN in Figure 64.1. Steps 1 and 2 generate an increasing cardinality ordered simple pathset $P_{s,t}$={(*s*,*a*,*b*,*d*,*t*), (*s*,*a*,*c*,*e*,*d*,*t*), (*s*,*a*,*c*,*e*,*j*,*t*), (*s*,*f*,*c*,*e*,*d*,*t*), (*s*,*f*,*c*,*e*,*j*,*t*), (*s*,*f*,*g*,*h*,*i*,*j*,*t*)}. This, in turn, is used by an MVI-based SDP technique [10] in Step 3 to generate six *mdt*: $P(4)=sabdt$, $P(5)=sacedt\ \bar{b} + sacejt\ \bar{d} + sfcedt\ \bar{a} + sfcejt\ \bar{a}\ \bar{d}$, and $P(6)=sfghi\,jt\ \overline{abd}\ \overline{ce}$. Notice that the factoring algorithm in [7] produces 12 *mdt*. Converting the six *mdt* into its reliability expression and considering p_s=1, $P(4)=p_a\ p_b\ p_d\ p_t$, $P(5)=p_a\ p_c\ p_e\ p_d\ p_t\ q_b + p_a\ p_c\ p_e\ p_j\ p_t\ q_d + p_f\ p_c\ p_e\ p_d\ p_t\ q_a + p_f\ p_c\ p_e\ p_j\ p_t\ q_a\ q_d$, and $P(6)=p_f\ p_g\ p_h\ p_i\ p_j\ p_t\ (1-p_a\ p_b\ p_d)\ (1-p_c\ p_e)$. Assuming equal operational node reliability of 0.9, $TR(G) = P(4)+P(5)+P(6) = 0.65610+0.18305+0.02736 = 0.86651$. Using (64.2), $EHC=(4P(4)+5P(5)+6P(6))/TR(G) = 4.2744$ hops. Notice that the minimum (maximum) hop count is 4 (6), and $4 \le EHC \le 6$.

Simulations in [37] shows the SDP technique better than the factoring approach in [34], because: (i) it produces less number of *mdt*, (ii) it generates the *mdt* faster, and (iii) it computes the $TR(G)$ and EHC of WCN with all disjoint paths (WCN that forms an interval-graph) in polynomial time in the order of its nodes (simple paths). The method produces less *mdt* as it uses MVI notation [2], in contrast to the SVI in Alg2 [34].

Algorithm EHC_SDP
Step 1: Generate (*s*,*t*) simple (node)-pathset $P_{s,t} = \{P_1, P_2, \ldots, P_m\}$
Step 2: Sort paths in $P_{s,t}$ in increasing cardinality order
Step 3: Use an SDP technique to compute $P(l)$ from $P_{s,t}$ for $1 \le l \le k-1$, and

$$TR(G) = \sum_{l=1}^{l=k-1} P(l)$$

Step 4: Compute expected hop count //(64.2).

Figure 64.3. Algorithm *EHC_SDP*

64.3.1.4 Computing the reliability and EHC for special structure WCN

A. WCN with Multiple Disjoint Paths

Consider a WCN where the source node *s* is connected to the destination node *t* through multiple disjoint paths. Note that [11] proposes the use of multiple disjoint paths to provide high network resistance to link/node failures in MANET. The SDP approach computes the performability of the WCN in $O(|V|^2)$ [37].

B. Interval-graph WCN

The SDP technique in [38] generates the *mdt* from $P_{s,t}$ of the interval graph in Figure 64.2(a) as: $s\ b\ d\ t$, $s\ b\ c\ e\ t\ \bar{d}$, $s\ a\ c\ e\ t\ \bar{b}$, $s\ a\ c\ d\ t\ \bar{e}\ \bar{b}$. Notice that each of the simple paths is converted into exactly one *mdt*. In a simulation of 1000 randomly generated interval-graphs [37] (70 nodes network with node degree between 2 to 5), the SDP approach generates one equivalent *mdt* for each simple path, when the paths are sorted in increasing cardinality order. The simulation results lead to a conjecture that the performability of interval-graph $G(V,E,C,\sigma)$ is computable in polynomial time in the order of its simple paths [37].

64.3.2 Example II: Mobile Network Analysis Using Probabilistic Connectivity Matrices

An increasing number of networks are constructed without central planning or organization. Examples include the Internet, *ad hoc* wireless networks, and peer-to-peer (P2P) systems like Napster and Gnutella. Mobile computing implementations often fit this category, since user positions vary unpredictably. On the other hand, it is often quite easy to determine the aggregate statistics for the user classes.

Traditional methods of analysis are often inappropriate for these systems, since the exact topology of the system at any point in time is unknowable. For these reasons, researchers turn to statistical or probabilistic models to describe and analyze these network classes [40–42]. Random graph and percolation theories allow us to use statistical descriptions of component behaviors to determine many useful characteristics of the global system. This section presents a network analysis technique that combines random graph theory, percolation theory, and linear algebra for analyzing statistically defined networks.

Random graph theory originated with the seminal works of Erdös and Rényi in the 1950s. Until then, graph theory considered either specific graph instances or deterministically defined graph classes. Erdös and Rényi considered graph classes with a uniform probability for edges existing between any two nodes. Their results were mathematically interesting and found applications in a number of practical domains [40].

Another random network model, given in [41], is used to study *ad hoc* wireless networks like those used in many mobile networks. A set of nodes is randomly distributed in a two-dimensional region. Each node has a radio with a given range *r*. A uniform probability exists (in [41] the probability is 1) for edges being formed between nodes as long as they are within range of each other. This network model has obvious practical applications. Many of its properties resemble those of Erdös–Rényi graphs, yet it also has significant clustering like the small-world model [42].

This section presents a technique for analyzing random and pseudo-random graph models, first presented in [8]. It constructs connectivity matrices for random graph classes, where every matrix element is the probability an edge exists between two given nodes. This contains elements of discrete mathematics, linear algebra, and percolation theory. It is useful for a number of applications. Applications already documented include system reliability [43] and QoS [44] estimation.

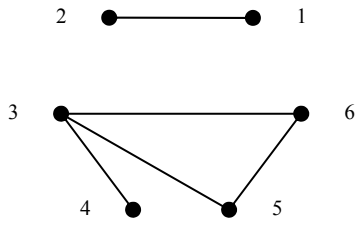
64.3.2.1 Preliminaries

A graph is defined as the tuple $[V, E]$. V is a set of vertices, and E is a set of edges. Each edge e is defined as (i,j) where i and j designate the two vertices connected by e. In this section, we consider only undirected graphs where $(i,j)=(j,i)$. An edge (i,j) is incident on vertices i and j. We do not consider multi-graphs where multiple edges can connect the same end-points.

Many data structures are used as practical representations of graphs. Refer to [45] for common representations and their usage. For example, a graph where each node has at least one incident edge can be fully represented by the list of edges. Another common representation of a graph, which we explore in more depth, is the connectivity matrix. The connectivity matrix M is a square matrix where each element $m(i,j)$ is 1 (0) if there is (not) an edge connecting vertices i and j. For undirected graphs, this matrix is symmetric.

Figure 64.4 shows a simple graph and its associated connectivity matrix.

As a matter of convention, the diagonal of the matrix can consist of either zeros or ones. Ones are frequently used, based on the simple assertion that each vertex is connected to itself. We use the convention where the diagonal is filled with zeros. A *walk* of length z is an ordered list of z edges $((i_0,j_0),(i_1,j_1),\ldots,(i_z,j_z))$, where each vertex j_a is the same as vertex i_{a+1}. A *path* of length z is a walk where all i_a are unique. If j_z is the same as i_0, the path is a *cycle.* A connected component is a set of vertices where there is a path between any two vertices in the component. (In the case of di-graphs, this is a fully connected component.) A complete graph has an edge directly connecting any two vertices in the graph. A complete subgraph is a subset of vertices in the graph with edges directly connecting any two members of the set.



(a) Graph

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

(b) Connectivity matrix

Figure 64.4. A six-node graph

A useful property of connectivity matrices is the fact that element $m^z(i,j)$ of the power z of graph G's connectivity matrix M (*i.e.*, M^z) is the number of walks of length z from vertex i to vertex j that exist on G [46]. This can be verified using the definition of matrix multiplication and the definition of the connectivity matrix. It is possible to find the connected components in a graph using iterative computation of M^z. After each exponentiation: (i) Set all non-zero elements of the M to one, giving C^1, (ii) Set C^{i+1} to C^i C^1, (iii) Set all non-zero elements of C^{i+1} to 1, (iv) Set C^{i+1} to the inclusive or of $C^{i+1}$and C^i, (v) Stop when C^{i+1} is equal to C^i.

Each row of C^i has a one in the element corresponding to each node in the same connected component. The number of distinct rows is the number of connected components.

64.3.2.2 Matrix Construction

We now show how to construct connectivity matrices for analyzing classes of random and pseudo-random graphs. The first model we discuss is the Erdös–Rényi random graph [47]; we then consider a graph model of an *ad hoc* wireless network.

The number of nodes n, and a uniform probability, p, of an edge existing between any two nodes, define Erdös–Rényi graphs. We use E for $|E|$ (*i.e.*, the number of edges in the graph). Since the degree of a node is essentially the result of multiple Bernoulli trials, the degree of an Erdös–Rényi random graph follows a Bernoulli distribution. Therefore, as n approaches infinity, the degree distribution follows a Poisson distribution.

It has been shown that the expected number of hops between nodes in these graphs grows proportionally to the log of the number of nodes [48]. Note that Erdös–Rényi graphs do not necessarily form a single connected component. When $E–n/2 << -n^{2/3}$ the graph is in a sub-critical phase and almost certainly not connected. A phase change occurs in the critical phase where $E= n/2 +O(n^{2/3})$ and in the supercritical phase where $E–n/2 >> - n^{2/3}$ a single giant component becomes almost certain. When $E= n \log n/2+ O(n)$ the graph is fully connected [49]. (Note that the expected number of edges for an Erdös–Rényi graph is $n(n–1)p/2$.)

Definition: The *probabilistic connectivity matrix M* of an n node random graph is an n-by-n matrix where each element (j,k) is the Bernoulli probability an edge exists between nodes j and k. By convention we set elements where $j=k$ to zero. The probabilistic connectivity matrix construct

translates random graph classes into an equivalent set of probabilities for the existence of edges between two given nodes. Note that, in contrast to many matrix representations of stochastic systems, the rows and columns of M do not necessarily sum to 1.

As an example, for an Erdös–Rényi graph with n set to 3 and p set to 0.25, the probabilistic connectivity matrix is:

$$\begin{bmatrix} 0 & 0.25 & 0.25 \\ 0.25 & 0 & 0.25 \\ 0.25 & 0.25 & 0 \end{bmatrix}. \quad (64.3)$$

Mobile wireless networks, in particular *ad hoc* wireless networks, with no fixed infrastructure, are suited to analysis using random graphs. A fixed radius model for random graphs is used in [41] to analyze phase change problems in *ad hoc* network design. In Section 64.3.2.3, we study phase changes in an *ad hoc* sensor network to determine whether or not a given system will produce a viable sensor network. After the phase change, a system can almost certainly self-organize into a viable network. Before the phase change, self-organization is virtually impossible. The approach presented in this section is used to predict where the phase change occurs.

The model in [41] places nodes at random in a limited two-dimensional region. Two uniform random variables provide a node's x and y coordinates. Since nodes in proximity with each other have a high probability of being able to communicate, the distance r between pairs of nodes is used as a threshold. If r is less than a given value, then an edge exists between the pair of nodes. Otherwise, no edge exists. Many similarities exist between this graph class and the graphs studied by Erdös and Rényi.

The analysis in [41] looks at finding phase transitions for constraint satisfaction problems. Range-limited graphs differ from Erdös–Rényi graphs in that they have significant clustering. We use the model from [41], except, where they create an edge with probability one when the distance between two nodes is less than the threshold; we allow the probability to be any value in the range [0,1].

The range-limited graph class differs from Erdös–Rényi and other random graph classes in that, while a random process defines it, the random process determines edge creation only indirectly. This makes it difficult, if not impossible, to undertake formal analysis. Instead of formally decomposing the graph definition into a set of Bernoulli probabilities, we are forced to derive a model that approximates system behavior. We provide results in Sections 64.3.2.3 and 64.3.2.4 showing that this model, while not perfect, is a useful tool for predicting system behavior.

We construct range-limited graphs using the following parameters:

- n – the number of nodes
- max_x (max_y) – the size of the region in the x (y) direction
- r – the maximum distance between nodes where connections are possible
- p – probability that an edge exists connecting two nodes within range of each other.

*Range-limited graph model definition***:** For range limited graphs, element (j,k) of the probabilistic connectivity matrix has value:

$$p\,(2c - c^2) \quad (64.4)$$

where c is a constant defined by:

$$c = r^2 - \left(\frac{j}{n+1} - \frac{k}{n+1}\right)^2 \quad (64.5)$$

when $r^2 \geq \left(\frac{j}{n+1} - \frac{k}{n+1}\right)^2$ and otherwise zero.

*Range-limited graph model derivation***:** Each element (j,k) of the probabilistic connectivity matrix is defined by the probability an edge exists between the pair of nodes j and k that is given by (64.4) and (64.5). Derivation of (64.4) and (64.5) proceeds in two steps. Step (i) Sort nodes by the x coordinate value (y could be used as well; the choice is arbitrary) and use order statistics to find the expected value of the x coordinate for each node; Step (ii) Determine the probabilities that an edge existing between two nodes using the expected values from Step (i).

By definition, each node is located at a point defined by two random variables: the x and y coordinates. Without loss of generality, max_x and max_y are used to normalize the values of x, y, and r to the range [0,1]. Constant scaling factors are needed to compensate for lack of symmetry when max_$x \neq$ max_y.

Rank statistics estimate the probability that two given nodes k and j are within communications range. To do this, sort each point by its x (or y) coordinate. For n samples from a uniform distribution of range [0,1], the rank statistics give expected value of the jth largest as $j/(n+1)$ with variance $\frac{1}{n+2}\left(\frac{j}{n+1}\right)\left(1-\frac{j}{n+1}\right)$. Node position j in the sorted list therefore has expected value $j/(n+1)$. Since our *ad hoc* network model uses the Euclidean distance metric, an edge exists between two nodes j and k with probability p when:

$$\left(x_j - x_k\right)^2 + \left(y_j - y_k\right)^2 \leq r^2 \ . \qquad (64.6)$$

Entering the expected values for the x ordinate of the nodes of rank j and k, it is:

$$\left(y_j - y_k\right)^2 \leq r^2 - \left(\frac{j}{n+1} - \frac{k}{n+1}\right)^2 \ . \qquad (64.7)$$

By definition, the random variables giving the x and y positions of the nodes are uniformly distributed and uncorrelated.

The probability that relation (64.7) holds is the probability that the square of the difference of two normalized uniform random variables is less than the constant value c that we define as the right hand side of (64.7). Figure 64.5 presents this as a geometry problem. The values of the two uniform random variables with range [0,1] describe a square region where every point is equally likely. The white region in the lower right hand corner of Figure 64.5 is the area that does not satisfy (64.7) because $y_j - y_k$ is greater than c. It is a right triangle, whose hypotenuse has these end points:

- When y_k is zero, y_j cannot be greater than c. The triangle base has length $1-c$.
- When y_j is one, y_k cannot be less than $1-c$. The triangle height is $1-c$.

The area of this triangle is therefore $(1-c)^2/2$.

The region that does not satisfy Equation 64.7 because $y_j - y_k$ is less than $-c$, is contained in the triangle in the upper left hand corner of Figure 64.5. The area of that region is also $(1-c)^2/2$, which can be demonstrated either by using symmetry or by repeating the logic in the previous paragraph and switching the variable names.

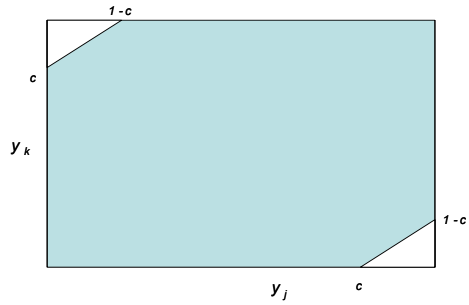


Figure 64.5. Geometric representation of (64.7)

Summing the areas of the two white triangles in Figure 64.5 gives:

$$(1-c)^2 \ . \qquad (64.8)$$

Since the area satisfying (64.7) is not contained in the two white triangles, the likelihood that nodes j and k are within communications range is:

$$1-(1-c)^2 = 1-(1-2c+c^2) = 2c-c^2 \ . \qquad (64.9)$$

Multiplying (64.9) by the probability p that two nodes within range can communicate ends the derivation of (64.4) and (64.5).

An example matrix for six nodes in a unit square with r=0.3 and p=1.0 is:

$$\begin{bmatrix} 0 & 0.134 & 0.0167 & 0 & 0 & 0 \\ 0.134 & 0 & 0.134 & 0.0167 & 0 & 0 \\ 0.0167 & 0.134 & 0 & 0.134 & 0.0167 & 0 \\ 0 & 0.0167 & 0.134 & 0 & 0.134 & 0.0167 \\ 0 & 0 & 0.0167 & 0.134 & 0 & 0.134 \\ 0 & 0 & 0 & 0.0167 & 0.134 & 0 \end{bmatrix} \qquad (64.10)$$

Figure 64.6 shows a three-dimensional plot of an example matrix. When we compare the number of edges for range-limited graphs constructed directly versus those constructed using the probabilistic connectivity matrices as a function of n and r. The approximation achieved by this model is good, but

not perfect. One reason for the deviation is the use of expected values in the derivation. For graph instances with a small number of nodes the variance of the node positions is greater. Second order effects are possible. Using expected values also assumes independence between random variables. Independence may not strictly hold throughout the range limited graph construction process. As we discuss in Sections 64.3.2.3 and 64.3.2.4, in spite of under-counting the number of edges, this model is very useful for predicting many aspects of network behavior. In particular, we have found it very useful for predicting where phase changes occur in the system.

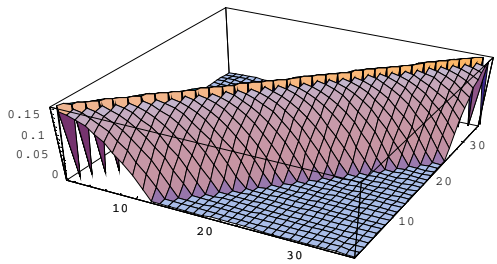


Figure 64.6. Three-dimensional plot of the connectivity matrix for a range limited graph of 35 nodes with r=0.3

64.3.2.3 Matrix Characteristics

By definition, connectivity matrices are square with the numbers of rows and columns both equal to the number of vertices in the graph (n). Each element (j,k) is the probability an edge exists between nodes j and k. Since we consider only non-directed graphs, (j,k) must equal (k,j) and therefore care needs to be taken to guarantee that algorithms for constructing matrices provide symmetric results.

An instance of a graph class can be produced by using the probabilistic connectivity matrix and performing $n(n-1)$ Bernoulli trials. One trial is made for each element (j,k) where $k>j$. If it is successful edge (j,k) exists. This produces an instance of the graph with the caveat that the range limited connectivity matrix is based on a model that approximates the statistics of the actual process. The graph constructed has slightly different statistics than actual range-limited graphs.

Theorem 1: The sum of each row (column) of the probabilistic connectivity matrix provides the expected degree of the corresponding node in G.

Proof: The expected value of a single trial of a Bernoulli distribution is the probability of success. The expected value of a sum of random variables is the sum of the expected values. Therefore the expected number of edges incident on node j is $\sum_{k=0}^{n-1}(j,k)$. QED.

A. Probability of Walks of z Hops between Nodes

Consider the usage of probabilistic connectivity matrixes. First application calculates the likelihood of connections of multiple hops between nodes. To do so, we define an analog to matrix multiplication.

Theorem 2: The probability a path of two hops exists between nodes j and k ($j \neq k$) in a random graph is:

$$1-\prod_{l\neq j,k}(1-(j,l)(l,k)) \ , \qquad (64.11)$$

where (j,l) and (l,k) are elements of the probabilistic connectivity matrix.

Proof: Each element (j,k) of the probabilistic connectivity matrix is the probability an edge exists between nodes j and k. Since self-loops are not considered, a path of length two between nodes j and k must pass through an intermediate node l that is neither j nor k. This value is the probability of the union of a set of events defined by the likelihoods of paths through all intermediate nodes.

The product of two probabilities is the likelihood of the intersection of their events when they are independent. Since the existence of each edge in the graph is determined by an independent Bernoulli trial, the likelihood edges exist simultaneously from node j to node l and node l to node k, is the product of elements (j,l) and (l,k).

The probability that either of two independent events j and k occurs is: $p_j+p_k-p_jp_k$. The probability three events j, k, and l occur can be computed recursively as $p_l + (p_j+ p_k - p_jp_k) - p_l(p_j + p_k - p_jp_k)$. This is commonly referred to as inclusion-exclusion. As the number of events increases the

number of factors involved increases, making this computation awkward for large numbers of events. An equivalent computation is:

$$1-\prod_{l\neq j,k}(1-p_{jl}p_{lk}) \quad . \tag{64.12}$$

Equation (64.12) is more efficient to compute. It computes the complement of the intersection of all the complements of the atomic events, which is equivalent to the union of the set of events. Since the matrix elements represent probabilities, (64.11) is the probability a path of two hops exists between nodes j and k. QED.

Definition: The probabilistic-matrix multiplication is defined for probabilistic connectivity matrixes using (64.11). Since all connectivity matrixes are square, probabilistic matrix multiplication is defined only for matrixes of the same dimension (n by n). The product of matrix A with matrix B is a new matrix AB where each element $ab(j,k)$ ($j\neq k$) of matrix AB is:

$$ab(j,k)=1-\prod_{l\neq j,k}(1-a(j,l)b(l,k)), \tag{64.13}$$

where $a(j,l)$ and $b(l,k)$ are elements of matrixes A and B respectively. Element $ab(j,j)$ is by convention always zero.

The similarity between this definition and standard matrix multiplication should be obvious. Equation (64.13) is needed to maintain independence when summing probabilities. As a matter of convention, we set the diagonal elements (j,j) of probabilistic connectivity matrixes to zero. Our applications typically concern the likelihood paths exist between nodes by computing the likelihoods of paths passing through any intermediate node. The value (j,j) is the probability a path connects node j with itself. The existence of loops in the graph does not increase the likelihood other nodes are connected. Constraining diagonal values to zero automatically removes loops from our calculations.

Theorem 3: For a graph class represented by a probabilistic connectivity matrix M, element (j,k) of M^z is the probability that a walk of length z exists between nodes j and k. Here, M^z is the product of M with itself z times using our conventions.

Proof: The proof is by induction. By definition, each element (j,k) is the probability an edge exists between nodes j and k. M^2 is the result of multiplying matrix M with itself. Using Theorem 2 each element (j,k) of M^2, except the diagonals, is the probability a path of length two exists between nodes j and k. Using the same logic, M^z is calculated from M^{z-1}using matrix multiplication to consider all possible intermediate nodes l between nodes j and k. Where M^{z-1} has the probabilities of a walk of length $z-1$ between j and l, and M has the values defined previously. QED

Example 1: Probabilities of walks of length three in an Erdös–Rényi graph of four nodes for p=0.65 and 0.6 are shown in (64.14) and (64.15), respectively.

B. Critical Values and Phase Changes

This section describes critical values and phase changes phenomenon in *ad hoc* networks modeled by random graphs. For Erdös–Rényi [47] and range-limited [50] graphs, first order monotone increasing graph properties follow 0-1 laws. These properties appear with probability asymptotically approaching either 0 or 1, as the parameters defining the random graph class decrease/increase.

$$M=\begin{bmatrix}0&0.65&0.65&0.65\\0.65&0&0.65&0.65\\0.65&0.65&0&0.65\\0.65&0.65&0.65&0\end{bmatrix}\ M^2=\begin{bmatrix}0&0.666&0.666&0.666\\0.666&0&0.666&0.666\\0.666&0.666&0&0.666\\0.666&0.666&0.666&0\end{bmatrix}\ M^3=\begin{bmatrix}0&0.679&0.679&0.679\\0.679&0&0.679&0.679\\0.679&0.679&0&0.679\\0.679&0.679&0.679&0\end{bmatrix}, \tag{64.14}$$

$$M=\begin{bmatrix}0&0.6&0.6&0.6\\0.6&0&0.6&0.6\\0.6&0.6&0&0.6\\0.6&0.6&0.6&0\end{bmatrix}\ M^2=\begin{bmatrix}0&0.59&0.59&0.59\\0.59&0&0.59&0.59\\0.59&0.59&0&0.59\\0.59&0.59&0.59&0\end{bmatrix}\ M^3=\begin{bmatrix}0&0.583&0.583&0.583\\0.583&0&0.583&0.583\\0.583&0.583&0&0.583\\0.583&0.583&0.583&0\end{bmatrix}. \tag{64.15}$$

A plot of property probability versus parameter value forms an S-shaped curve with an abrupt phase transition between the 0 and 1 phases [47], [41]. The parameter value where the phase transition occurs is referred to as the critical point. The connectivity matrices defined in this section can identify critical points and phase transitions in graph classes.

As an example, consider graph connectivity in Erdös–Rényi graphs. As mentioned in Section 64.3.2.2, this property has three phases determined by the number of edges in the graph: sub-critical (graph almost certainly not connected), critical, and supercritical (graph almost certainly connected). The distribution of the number of edges E in an Erdös–Rényi graph has a binomial distribution defined by taking $n(n-1)/2$ trials taken with probability p. In the sub-critical phase, the size of the largest graph component is O(log n); making the graph almost certainly disjoint. In the supercritical phase, the largest graph component size is $O(n)$. A single giant component dominates the graph. In the supercritical phase, the probability that the graph is fully connected converges to $e^{-e^{-c}}$ where $p = \{\log n + c + O(1)\}/n$ [47]

Theorem.4: For Erdös–Rényi graphs of n nodes with $0<p<1$ the probability of an edge existing between any two nodes in a probabilistic connectivity matrix M, the critical point for the property of graph connectivity occurs when $M=M^2$ [*i.e.*, $p = 1-(1-p^2)^{n-2}$]. When $M>>M^2$ [*i.e.*, $p >> 1-(1-p^2)^{n-2}$], the graph is in its sub-critical phase. When $M<<M^2$ [*i.e.*, $p << 1-(1-p^2)^{n-2}$], the graph is in its supercritical phase. (Note probability p is real valued).

Proof: By definition, all non-diagonal elements of the Erdös–Rényi graph matrix have the same value p and diagonal elements have value zero. By symmetry, all non-diagonal elements of M^n for any n will have the same value (diagonal elements are constrained to remain zero). We use the symbols <, >, <<, and >> to compare these matrices by referring to the value of the non-diagonal elements.

Non-diagonal elements of M^2 have value $1-(1-p^2)^{n-2}$ from (64.12). From Theorem 3, this is the likelihood a path of two hops exists between any two nodes in the graph. Let $p^{(2)}$ represent non-diagonal elements of M^2 [*i.e.*, $1-(1-p^2)^{n-2}$]. $p^{(2)}$ is monotone increasing with respect to p. Both p and $p^{(2)}$ are constrained to range [0,1]. The minimum (maximum) value 0 (1) of both occurs when p is 0 (1), at which point any value of n will satisfy the equation and no phase change occurs.

If $p^{(2)} > p$, the probability a path of three hops exists between any two nodes ($p^{(3)}$) is greater than the probability a path of two hops exists ($p^{(2)}$). $p^{(3)}$ has value $1-(1-p^{(2)}\ p)^{n-2}$, which is monotone increasing with respect to both p and $p^{(2)}$. By recursion, the probability any two nodes are connected increases with the path length as long as $p^{(2)} > p$. As $p^{(n-1)}$ approaches 1, a single giant component exists almost certainly. Although, there remains a finite shrinking probability that isolated nodes exist. By definition, the graph is in its supercritical phase.

By symmetry, when $p^{(2)} < p$ the likelihood a path of j hops connects any two nodes decreases monotonically with j. As $p^{(n-1)}$ approaches 0, the giant component almost certainly does not exist and the graph becomes increasingly disjoint. By definition [47], the graph is in its subcritical phase.

When $M << M^2$ the graph has been shown to be in its supercritical phase and when $M >> M^2$ the graph has been shown to be in its subcritical phase. This leaves $M \approx M^2$ as the critical phase. By definition, the critical phase is the neighborhood of the critical point so the critical point can be calculated as the point where $M = M^2$. QED

Reference [8] has empirically verified Theorem 4. Without rigor, we apply Theorem 4 to non-Erdös–Rényi graph classes to find estimate where phase changes occur. The application (Section 64.3.2.4) shows this to be a pragmatic solution.

64.3.2.4 Application of Example II

We present a security application from [51], where *ad hoc* sensor network security is enforced by a set of k keyservers chosen at random from a total of n nodes. Each keyserver serves all nodes within h hops. Keyservers can collaborate to identify and remove malicious nodes, such as clones. Here we show how to determine the number of keyservers needed. The phase change for the secure communications network occurs when:

$$k = 2 + \frac{\log(1 - p_{ij}^{(2h-1)})}{\log(1 - (p_{ij}^{(2h-2)})^2)}, \quad (64.16)$$

where k is the number of keyservers, the keyserver serves all nodes with h hops, and p_h is the probability of a walk of h or fewer hops existing between nodes with the labels $i=\left\lfloor \frac{n}{2} \right\rfloor$ and $j=\left\lfloor \frac{n}{2} \right\rfloor + 1$ from the *ad hoc* network model.

As shown in the model derivation, the phase change occurs when $p_{h+1}=p_h$. By applying (64.12) recursively, we find the likelihood of a walk of $2h-1$ hops between nodes i and j:

$$p_{ij}^{(2h-1)} = 1 - \prod_{l=1, l\neq i, l\neq j}^{n} (1 - p_{il}^{(2h-2)} * p_{lj}^{(1)}) \ . \quad (64.17)$$

Two keyservers can communicate if there is a walk of length $2h-1$ or less between them. Since keyservers are placed at random on the *ad hoc* network, we have an Erdös–Rényi graph where any two keyservers can communicate with the probability defined in (64.17). The probability that any two multi-cast regions with keyservers k_1 and k_2 can communicate using an intermediary is therefore:

$$p_{k_1k_2}^{(2)} = 1 - \prod_{i,j=1; i,j\neq k_1; i,j\neq k_2}^{k} (1 - p_{ij}^{(2h-1)} \times p_{ij}^{(2h-1)}), \quad (64.18)$$

which simplifies to:

$$p_{k_1k_2}^{(2)} = 1 - (1 - (p_{ij}^{(2h-1)})^2)^{k-2} \quad (64.19)$$

so that the phase change occurs when:

$$p_{ij}^{(2h-1)} = p_{k_1k_2}^{(2)} = 1 - (1 - (p_{ij}^{(2h-1)})^2)^{k-2} \quad (64.20)$$

Taking the log of both sides and rearranging terms yields (64.16).

Simulations of our *ad hoc* model were run using MATLAB to verify these analytical predictions. Refer to [8] for details. For Erdös–Rényi graphs, it is determined that the phase change occurs when the number of edges is $E = n/2 + O(n^{2/3})$ [49]. Note that these results are asymptotes as graph size approaches infinity and do not consider constant offsets in the O notation. Results from our approach are therefore consistent with the analysis in [47] and [49].

64.3.3 Example III: Improving End-to-end Performability in *Ad Hoc* Networks

64.3.3.1 (s,t) Routing in Ad Hoc Network

Two of the most widely used MANET routing protocols are dynamic source routing (DSR) [52] and the *ad hoc* on-demand distance vector (AODV) [53]. Both are *on-demand* or *reactive* protocols, where (*s*,*t*) paths discovery is initiated only when they are needed, in contrast to the *proactive* protocol, where each node maintains a routing table even when there is no network routing activity. The path discovery step in a reactive protocol requires route request (RREQ) message flooding to the entire network to reach the destination [52], and hence is expensive while generating only a single (*s*,*t*) path.

The node mobility in MANET makes frequent network topology changes which, in addition to nodes/links failures, may disconnect the existing (*s*,*t*) path that forces the source node to re-run the costly discovery step that also leads to a long path recovery delay. Multi-path routing protocol can be used to improve the end-to-end reliability and to reduce the frequency of using the discovery step. Most of the proposed multi-path routings are either an extension of the DSR or AODV to generate multiple (*s*,*t*) paths in one discovery step [12]. Among others, the multiple paths are used for load balancing, higher bandwidth aggregation, and performability improvement. Multi-path has also been proposed to improve the performability of WSN [54] and internetwork [55]. This section provides a survey of recent multi-path protocols for improving MANET performability.

64.3.3.2 Improving End-to-end Performability in MANET

Typically, a multi-path routing protocol attempts to find a set of node disjoint, link disjoint or non-disjoint paths [12]. Note that paths with disjoint node (*i.e.*, no node overlap) also imply disjoint links (*i.e.*, no link overlap).

Split multipath routing (SMR) [56] generates two maximally disjoint node paths: a primary path,

and a backup path. When the destination receives RREQs, it composes a primary path from the information in the first arriving RREQ (thus an (s,t) shortest delay path), and selects the backup path from the following RREQs it receives such that the path is maximally disjoint from the primary path. Then, the destination sends a route reply (RREP) for each of two paths to the source. To reduce the frequency of using route discovery, the source reinitiates the step when both the primary and backup paths are broken. When the primary path fails, the source will receive a route error (RERR) message, and it needs to resend the lost packet through the alternative path. It is shown in [56] that SMR performs better than DSR in terms of robustness to node mobility as well as end-to-end packet delay.

The back up source routing (BSR) [57] establishes and maintains a backup route that comprises a primary path having the minimal end-to-end delay and a backup path having shared nodes with the primary path, in contrast to the disjoint paths in SMR [56]. Note, the overlapping nodes in the primary and backup reduces the recovery time and overhead when the primary path fails because the packet can be resend from a shared node closest to the failure spot, and the RERR message reaches only up to the shared node, respectively. The backup route is used to prolong the lifetime of the path-pair, which obviously reduces the frequency of using the route discovery step. The reference defines the reliability of a backup route as the mean value of the lifetime of the route. Given a primary path the scheme [57] selects a backup path to maximize the reliability. With node mobility, BSR will also dynamically update backup routes to keep the routes optimal.

In MP-DSR [58], a user is allowed to set a path reliability requirement as its QoS, and the protocol uses a distributed routing algorithm to generate a set of (s,t) node-disjoint paths to meet the reliability constraint. For any time instant t_0, an end-to-end reliability is defined as the probability of successful (s,t) data transmission until time $t_0 + T_p$. The reliability is computed from the node-disjoint pathset, where each path reliability is computed from the link availabilities, which can be obtained using Jiang's prediction approach [10] discussed in Section 64.2.3.2. Given the user path reliability requirement, MP-DSR calculates the number of paths required and the lowest path reliability for each path to meet the user constraint. The two parameters are used in intermediate nodes to decide if a RREQ message be discarded or forwarded towards the destination. Upon receiving the RREQs (*i.e.*, pathset), the destination sorts the paths in the order of their reliabilities, composes a set of disjoint paths from the pathset that together meets the user requirement, and sends RREP that includes the disjoint pathset to the source.

The DPSP in [11] selects a set of disjoint paths to maximize end-to-end reliability. Essentially, DPSP solves the problem of maximizing a parallel-series system graph [11]. Note that the problem of finding the most reliable pathset has been shown to be computationally hard [11], and the maximum number of link disjoint paths equals the smallest cardinality of the minimal (s,t)-cut. DPSP assumes that the underlying routing protocol (reactive or proactive) has completed its path discovery step, and from the generated alternative paths DPSP constructs a communication graph G_p which gives a partial view of the network. Then, G_p is used to compose a directed probabilistic graph D_p that includes the link reliability information generated by each node incident to the links. Given a D_p, DPSP first finds the most reliable path, and stores it in the set of disjoint path DP. Then, iteratively it selects the next most reliable path B, which is included directly into DP if B is disjoint to all paths in DP. If B is not disjoint with any of the path in DP (the non-disjoint paths are called interlacing paths), DPSP transforms the interlacing paths into a set of disjoint paths to be added in DP. However, if the new set of disjoint paths does not produce better pathset reliability, DPSP cancels the transformation. Note, the cumulative reliability of the set of disjoint paths found by DPSP is the lower bound of the terminal reliability of the network.

Reference [59] uses M-for-N *diversity coding* and a set of disjoint paths to improve the performability of end-to-end data transmission. The scheme divides an X bits packet into N equal sized blocks, and adds M blocks of the same size (generated from X) for redundancy. Then, it

transmits an equal number of blocks (*e.g.*, one block) through each of the disjoint paths. The *M*-for-*N diversity coding* guarantees that the original packet (*i.e.*, *X*) can be reconstructed in the destination provided it receives at least *N* (out of *N*+*M*) blocks. Therefore, the problem solved in the scheme [59] reduces into allocating the *N*+*M* blocks among all disjoint paths to maximize the probability for the destination to receive at least *N* blocks.

64.4 Conclusions

We have discussed several issues related to computing and improving the performability of WCNs. In addition to the random failures that make components in a wired-non-mobile CN fail, a node in a WSN may be non-operational due to non-renewable power failures, and therefore better understanding of energy consumption in WSN is important to improve network performability. We have shown that for many classes of WSN applications, computation, in addition to the wireless communication, may dominate energy consumption. Due to mobility a wireless link between two nodes may be unavailable when the nodes are not within communication range from each other. We have discussed recent techniques to estimate the link reliability in mobile WCN. Finally three examples of performability issues of WCN have been presented. First, we discuss an efficient technique to compute the reliability and expected hop count of a static topology (non-mobile) WCN. Second, we describe a method to statistically analyse the performability of a mobile ad hoc WCN. The method utilizes random graph theory, percolation theory, and linear algebra. Finally, a survey of recent techniques to improve the end-to-end path reliability in MANET has been presented.

Acknowledgment

Dr. Rai is supported in part by the NSF grant CCR 0310916.

References

[1] Chalmers D, Sloman M. A survey of quality of service in mobile computing environments. IEEE Communications Surveys 1999; 2–10.

[2] Rai S, Agrawal DP. Distributed computing network reliability. IEEE Computer Society 1990.

[3] Kurose JF, Ross KW. Computer networking, a top-down approach featuring the internet. Third edition. Addison Wesley, Reading, MA, 2005.

[4] Goel A, *et al*, Efficient computation of delay-sensitive routes from one source to all destinations. IEEE INFOCOM 2001; 854–858.

[5] Guerin R, Orda A. Computing shortest paths for any number of hops. IEEE/ACM Transactions on Networking 2002; 10(5):613–620.

[6] Akyildiz IF, *et al.*, A survey on sensor networks. IEEE Communications 2002; 40:102–114.

[7] Intanagonwiwat C, *et al*, Directed diffusion for wireless sensor networking. IEEE/ACM Transactions on Networking 2003; 11:2–16.

[8] Brooks RR, Pillai B, Rai S, Racunas S. Mobile network analysis using probabilistic connectivity matrices. IEEE Transactions on Systems Man, and Cybernetics, July 2007; Part C, 37(4): 694–702.

[9] Royer EM, Toh C-K. A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Communications 1999; Apr.:46–55.

[10] Jiang S, He D, Rao J. A prediction-based link availability estimation for routing metrics in MANETs. IEEE/ACM Transactions on Networking 2005; 13(6):1302–1312.

[11] Papadimitratos P, Haas ZJ, Sirer EG. Path set selection in mobile *ad hoc* networks. MOBIHOC'02, June 9–11, 2002; EPFL Lausanne, Switzerland, ACM- Press:1–11.

[12] Mueller S, Tsang RP, Ghosal D. Multipath routing in mobile ad hoc networks: Issues and challenges. MASCOTS 2003, Lecture notes in computer science 2965, Calzarossa M.C., and E. Gelenbe (Eds.), 2004; 209–234.

[13] AboElFotoh HMF, Iyengar SS, Chakrabarty K. Computing reliability and message delay for cooperative wireless distributed sensor networks subject to random failures. IEEE Transactions on Reliability 2005; 54:145–155.

[14] Hereford J, Pruitt C. Robust sensor systems using evolvable hardware. Proceedings 2004 NASA/DoD Conference on Evolution Hardware 2004; 161–168.

[15] Brooks RR, Armanath S, Siddul H. On adaptation to extend the lifetime of surveillance sensor networks. Proceedings of Innovations and Commercial Applications of Distributed Sensor

Networks Symposium,Oct. 18–19, 2005; Bethesda, MD.

[16] Roundy S, Wright PK, Rabaey JM. Energy scavenging for wireless sensor networks. Kluwer, Dordrecht, 2004.

[17] Pottie GJ, Kaiser WJ. Wireless integrated network sensors. Communications of the ACM 20004; 3(5):51–58.

[18] Doherty L, Warneke BA, Boser BE, Pister KSJ. Energy and performance considerations for smart dust. International Journal of Parallel and Distributed systems and Networks 2001; 4(3):121–133.

[19] Carman DW, Kraus PS, Matt BJ. Constraints and approaches for distributed sensor network security (Final). NAI Labs Technical. Report #00-010, 2000 September 1.

[20] Zhao F, Guibas LJ. Wireless sensor networks: An information processing approach. Morgan Kaufmann, San Francisco, 2004.

[21] Rabaey JM, Ammer J, Karalar T, Li S, Otis B, Sheets M, *et al.,* PicoRadios for wireless sensor networks: The next challenge in ultra-low-power design. Proceedings of the International Solid-State Circuits Conference, San Francisco, CA, February 3–7, 2002.

[22] Slavin E, Brooks RR, Keller E. A comparison of tracking algorithms using beamforming and CPA methods with an emphasis on resource consumption *vs*. performance. PSU/ARL ESP MURI Technical Report, 2002.

[23] Chen J, Yao K. Beamforming, in [43].

[24] Phoha S, Brooks RR. Emergent surveillance plexus MURI annual report. The Pennsylvania State University Applied Research Laboratory, Report 1, Defense Advanced Research Projects Agency and Army Research Office, 2002.

[25] Phoha S, Brooks RR. Emergent surveillance plexus MURI annual report. The Pennsylvania State University Applied Research Laboratory, Report 2, Defence Advanced Research Projects Agency and Army Research Office, 2003.

[26] Brooks RR, Griffin C, Friedlander DS. Self-Organized distributed sensor network entity tracking. International Journal of High Performance Computer Applications, SpecialIissue on Sensor Networks 2002; 16(3):207–220.

[27] Brooks RR, Ramanathan P, Sayeed A. Distributed target tracking and classification in sensor networks. Proceedings IEEE, Invited Paper 2003; 91(8):1163–1171.

[28] Brooks RR, *et al.*, Distributed tracking and classification of land vehicles by acoustic sensor networks. Journal of Underwater Acoustics, Classified Journal, Invited Paper, 2003; Oct.

[29] Brooks RR, *et al*, Tracking multiple targets with self-organizing distributed ground sensors. Journal of Parallel and Distributed Computing, Issue on Sensor Networks 2004; 64(7):874–884.

[30] Potlapally NR, Ravi S. Raghunathan A, Jha NK. Analyzing the energy consumption of security protocols, Proceedings International Symposium on Low Power Electronics and Design, Seoul, South Korea, Aug. 25–27, 2003;30–35.

[31] Carman DW. Data security perspectives, in [43].

[32] Jiang S. An enhanced prediction-based link availability estimation for MANETs. IEEE Transactions on Communications 2004; 52:183–186.

[33] Qin M, Zimmermann R, Liu LS. Supporting multimedia streaming between mobile peers with link availability prediction. Proc. 13th Annual ACM International Conference on Multimedia 2005; 956.

[34] Abo El-Fotoh HMF. Algorithms for computing message delay for wireless networks. Networks 1997; 27:117–124.

[35] Golumbic MC. Algorithmic graph theory and perfect graph. Elsevier, Amsterdam, Second Edition, 2004.

[36] Rai S, Veeraraghavan M, Trivedi KS. A survey of efficient reliability computation using disjoint products approach. Networks 1995; 25:147–163.

[37] Soh S, Lau W, Rai S, Brooks RR. On computing reliability and expected hop count of wireless communication networks. International Journal of Performability Engineering, 3(2):167–179.

[38] Soh S, Rai S. CAREL: computer aided reliability evaluator for distributed computer systems. IEEE Transactions on Parallel and Distributed Systems 1991; Apr., 2:199–213.

[39] Soh S, Rai S. Experimental results on preprocessing of path/cut terms in sum of disjoint products technique. IEEE Transactions on Reliability 1993; Mar.:24–33.

[40] Barabasi A-L. Linked. Perseus, Cambridge, MA, 2002.

[41] Krishnamachari B, Wicker SB, Bejar R. Phase transition phenomena in wireless *ad-hoc* networks. Symposium on *Ad-Hoc* Wireless Networks, GlobeCom, San Antonio, Texas, 2001; Nov.

[42] Watts DJ. Small worlds. Princeton University Press, Princeton, NJ, 1999.

[43] Iyengar SS, Brooks RR (Eds.), Distributed sensor networks. Chapman and Hall, Boca Raton, FL, 2005.

[44] Kapur A, Gautam N, Brooks RR, Rai S. Design, performance and dependability of a peer-to-peer network supporting QoS for mobile code appli-

cations. Proceedings 10th International Conference on Telecom. Systems, Modelling and Analysis. Monterey, CA; Oct. 3–6, 2002:395–419.
[45] Aho AV, Hopcroft JE, Ullman JD. The design and analysis of computer algorithms. Addison-Wesley, Reading, MA, 1974.
[46] Cvetkovic DM, Doob M, Sachs H. Spectra of Graphs. Academic Press, New York, 1979.
[47] Bollobás B, Random graphs. Cambridge University Press, Cambridge, 2001.
[48] Albert R., Barabási A-L. Statistical mechanics of complex networks. arXiv:cond-mat/0106096v1, 2001; June.
[49] Jensen S, Luczak T, Rucinski A. Random graphs. Wiley, New York, 2000.
[50] Goel A, Rai S, Krishnamachari B. Sharp thresholds for monotone properties in random geometric graphs. ACM Symposiu,m on Theory of Computing 2004; June: 580–586.
[51] Pillai, B. Network embedded support for sensor network security. M.S. Thesis, Clemson University, 2006.
[52] Johnson D, Maltz D. Dynamic source routing in ad hoc wireless networks. In: Imielinski T, Korth H, editors. Mobile computing. Kluwer, Dordrecht, 1996; 153–181.
[53] Perkins CE, Royer EM. Ad-Hoc on-demand distance vector routing. Proceedings IEEE WMCSA, 1999; 90–100.
[54] Felemban E, Lee C-G, Ekici E. MMSPEED: multipath multi-speed protocol for QoS guarantee of reliability and timeliness in wireless sensor networks. IEEE Transactions on Mobile Computing 2006; 5(6):738–754
[55] Chakrabarti A., Manimaran G. Reliability constrained routing in QoS networks. IEEE/ACM Transactions on Networking, 2005; 13(3):662–675.
[56] Lee S, Gerla M. Split multipath routing with maximally disjoint paths in *ad hoc* networks. Proceedings IEEE ICC 2001; 3201–3205.
[57] Guo S, Yang O, Shu Y. Improving source routing reliability in mobile *ad hoc* networks. IEEE. Transactions on Parallel and Distributed Systems. 2005; 16(4):362–373.
[58] Leung R, Liu J, Poon E, Chan A-L C, Li B. MP-DSR: A QoS-aware multi-path dynamic source routing protocol for wireless ad-hoc networks. Proceedings 26th IEEE Annual Conference on Local Computer Networks LCN'01) Tampa, FL, Nov.14–16 2001; 132–141.
[59] Tsirigos A, Haas ZJ. Multipath routing in the presence of frequent topological changes. IEEE Communications 2001; Nov.:132–138.

65

Performability Modeling and Analysis of Grid Computing

Yuan-Shun Dai[1] and Gregory Levitin[2]

[1] Department of Computer and Information Science, Purdue University School of Science, IUPUI, Indianapolis, IN, 46202, USA
[2] Israel Electric Corporation Ltd., Amir Bld. P.O.B. 10, Haifa 31000, Israel

Abstract: Grid computing is a newly developed technology for complex systems with large-scale resource sharing, wide-area communication, and multi-institutional collaboration. Although the developmental tools and infrastructures for the grid have been widely studied, grid reliability analysis and modeling are not easy because of its largeness, complexity and stiffness. This chapter introduces the grid computing technology, analyzes different types of failures in grid system and their influence on its reliability and performance. The chapter then presents models for star-topology grid considering data dependence and tree-structure grid considering failure correlation. Evaluation tools and algorithms are developed, based on the universal generating function, graph theory, and the Bayesian approach. Illustrative numerical examples are presented to show the grid modeling and reliability/performance evaluation.

65.1 Introduction

Grid computing [1] is a newly developed technology for complex systems with large-scale resource sharing, wide-area communication, and multi-institutional collaboration [2–6]. Many experts believe that the grid technologies will offer a second chance to fulfill the promises of the Internet.

The real and specific problem that underlies the grid concept is coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations [4]. The sharing that we are concerned with is not primarily file exchange but rather direct access to computers, software, data, and other resources. This is required by a range of collaborative problem-solving and resource-brokering strategies emerging in industry, science, and engineering. This sharing is highly controlled by the resource management system [7], with resource providers and consumers defining what is shared, who is allowed to share, and the conditions under which the sharing occurs.

Recently, the open grid service architecture [5] has enabled the integration of services and resources across distributed, heterogeneous, dynamic, virtual organizations. A grid service is desired to complete a set of programs under the circumstances of grid computing. The programs may require using remote resources that are distributed. However, the programs initially do not know the site information of those remote resources in such a large-scale computing

environment, so the resource management system (the brain of the grid) plays an important role in managing the pool of shared resources, in matching the programs to their requested resources, and in controlling them to reach and use the resources through wide-area networks.

The structure and functions of the resource management system (RMS) in the grid have been introduced in details by [7–10]. Briefly stated, the programs in a grid service send their requests for resources to the RMS. The RMS adds these requests into the request queue [7]. Then, the requests are waiting in the queue for the matching service of the RMS for a period of time (called waiting time) [11]. In the matching service, the RMS matches the requests to the shared resources in the grid [12], and then builds the connection between the programs and their required resources. Thereafter, the programs can obtain access to the remote resources and exchange information with them through the channels. The grid security mechanism then operates to control the resource access through the certification, authorization, and authentication, which constitute various logical connections that causes dynamicity in the network topology.

Although the developmental tools and infrastructures for the grid have been widely studied [1], grid reliability analysis and evaluation are not easy because of its complexity, largeness, and stiffness. The gird computing contains different types of failures that can make a service unreliable, such as blocking failures, time-out failures, matching failures, network failures, program failures, and resource failures. This chapter thoroughly analyzes these failures.

Usually the grid performance measure is defined as the task execution time (service time). This index can be significantly improved by using the RMS that divides a task into a set of subtasks which can be executed in parallel by multiple online resources. Many complicated and time-consuming tasks that could not be implemented before are now working well under the grid environment.

It is observed in many grid projects that the service time experienced by the users is a random variable. Finding the distribution of this variable is important for evaluating the grid performance and improving the RMS functioning. The service time is affected by many factors. First, various available resources usually have different task processing speeds online. Thus, the task execution time can vary depending on which resource is assigned to execute the task/subtasks. Second, some resources can fail when running the subtasks, so the execution time is also affected by the resource reliability. Similarly, the communication links in grid service can be disconnected during the data transmission. Thus, the communication reliability influences the service time as well as data transmission speed through the communication channels. Moreover, the service requested by a user may be delayed due to the queue of earlier requests submitted from others. Finally, the data dependence imposes constraints on the sequence of the subtasks' execution, which has a significant influence on the service time.

This chapter first introduces the grid computing system and service, and analyzes various failures in grid system. Both reliability and performance are analyzed in accordance with the performability concept. Then the chapter presents models for star- and tree-topology grids respectively. The reliability and performance evaluation tools and algorithms are developed based on the universal generating function, graph theory, and the Bayesian approach. Both failure correlation and data dependence are considered in the models.

65.2 Grid Service Reliability and Performance

65.2.1 Description of Grid Computing

Today, the grid computing systems are large and complex, such as the IP-Grid (Indiana-Purdue Grid), which is a state wide grid (http://www.ip-grid.org/). IP-Grid is also a part of the TeraGrid that is a nationwide grid in the USA (http://www.teragrid.org/). The largeness and complexity of the grid challenge the existing models and tools to analyze, evaluate, predict, and optimize the reliability and performance of grid systems. The global grid system is depicted in the Figure 65.1. Various organizations [4], integrate/

share their resources on the global grid. Any program running on the grid can use those resources if it can be successfully connected to them and is authorized to access them. The sites that contain the resources or run the programs are linked by the global network as shown in the left part of Figure 65.1.

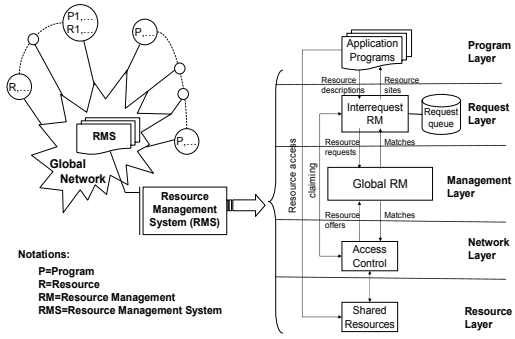


Figure 65.1. A grid computing system

The distribution of the service tasks/subtasks among the remote resources is controlled by the resource management system (RMS), which is the "brain" of grid computing [7]. RMS has five layers in general, as shown in Figure 65.1: the program layer, the request layer, the management layer, the network layer, and the resource layer.

1) *Program layer*: The program layer represents the programs of the customer's applications. The programs describe their required resources and constraint requirements (such as deadline, budget, function, *etc.*). These resource descriptions are translated to the resource requests and sent to the next request layer.
2) *Request layer*: The request layer provides the abstraction of "program requirements" as a queue of resource requests. The primary goals of this layer are to maintain this queue in a persistent and fault-tolerant manner and to interact with the next management layer by injecting resource requests for matching, claiming matched resources of the requests.
3) *Management layer*: The management layer may be thought of as the global resource allocation layer. It has the function of automatically detecting new resources, monitoring the resource pool, removing failed/unavailable resources, and most importantly matching the resource requests of a service to the registered/detected resources. If resource requests are matched with the registered resources in the grid, this layer sends the matched tags to the next network layer.
4) *Network layer*: The network layer dynamically builds connection between the programs and resources when receiving the matched tags and controls them to exchange information through communication channels in a secure way.
5) *Resource layer*: The resource layer represents the shared resources from different resource providers including the usage policies (such as service charge, reliability, serving time, *etc*.).

65.2.2 Failure Analysis of Grid Service

Even though all online nodes or resources are linked through the Internet with one another, not all resources or communication channels are actually used for a specific service. Therefore, according to this observation, we can make tractable models and analyses of grid computing *via* a virtual structure for a certain service. The grid service is defined as follows:

> *Grid service is a service offered under the grid computing environment, which can be requested by different users through the RMS, which includes a set of subtasks that are allocated to specific resources via the RMS for execution, and which returns the result to the user after the RMS integrates the outputs from different subtasks.*

The above five layers coordinate together to achieve a grid service. At the "program layer", the subtasks (programs) composing the entire grid service task initially send their requests for remote resources to the RMS. The "request layer" adds these requests in the request queue. Then, the "management layer" tries to find the sites of the resources that match the requests. After all the requests of those programs in the grid service are matched, the "network layer" builds the connections among those programs and the matched resources.

It is possible to identify various types of failures on respective layers:

- *Program layer*: Software failures can occur during the subtask (program) execution; see, *e.g.*, [13, 14].
- *Request layer*: When the programs' requests reach the request layer, two types of failures may occur: "blocking failure" and "time-out failure". Usually, the request queue has a limitation on the maximal number of waiting requests [7]. If the queue is full when a new request arrives, the request blocking failure occurs. The grid service usually has its due time set by customers or service monitors. If the waiting time for the requests in the queue exceeds the due time, the time-out failure occurs [11].
- *Management layer*: At this layer, "matching failure" may occur if the requests fail to match with the correct resources, [15, pp. 185–186]. Errors, such as incorrectly translating the requests, registering a wrong resource, ignoring resource disconnection, misunderstanding the users' requirements, can cause these matching failures.
- *Network layer*: When the subtasks (programs) are executed on remote resources, the communication channels may be disconnected either physically or logically, which causes the "network failure", especially for those long time transmissions of large dataset [16].
- *Resource layer*: The resources shared on the grid can be of software, hardware or firmware type. The corresponding software, hardware or combined faults can cause resource unavailability.

65.2.3 Grid Service Reliability and Performance

Most previous research on distributed computing studied performance and reliability separately. However, performance and reliability are closely related and affect each other, in particular under the grid computing environment. For example, while a task is fully parallelized into m subtasks executed by m resources, the performance is high but the reliability might be low because the failure of any resource prevents the entire task from completion. This causes the RMS to restart the task, which reversely increases its execution time (*i.e.*, reduces performance). Therefore, it is worth assigning some subtasks to several resources to provide execution redundancy. However, excessive redundancy, even though improving the reliability, can decrease the performance by not fully parallelizing the task. Thus, the performance and reliability affect each other and should be considered together in the grid service modeling and analysis.

In order to study performance and reliability interactions, one also has to take into account the effect of service performance (execution time) upon the reliability of the grid elements. The conventional models [17–20] are based on the assumption that the operational probabilities of nodes or links are constant, which ignores the links' bandwidth, communication time and resource processing time. Such models are not suitable for precisely modeling the grid service performance and reliability.

Another important issue that has much influence the performance and reliability is data dependence, which exists when some subtasks use the results from some other subtasks. The service performance and reliability is affected by data dependence because the subtasks cannot be executed totally in parallel. For instance, the resources that are idle in waiting for the input to run the assigned subtasks are usually hot-standby because cold-start is time consuming. As a result, these resources can fail in waiting mode.

The considerations presented above lead the following assumptions that lay in the base of grid service reliability and performance model.

Assumptions:

1) The service request reaches the RMS and is being served immediately. The RMS divides the entire service task into a set of subtasks. The data dependence may exist among the subtasks. The order is determined by precedence constraints and is controlled by the RMS.
2) Different grid resources are registered or automatically detected by the RMS. In a grid service, the structure of virtual network (consisting of the RMS and resources

involved in performing the service) can form star topology with the RMS in the center or, tree topology with the RMS in the root node.

3) The resources are specialized. Each resource can process one or multiple subtask(s) when it is available.
4) Each resource has a given constant processing speed when it is available and has a given constant failure rate. Each communication channel has constant failure rate and a constant bandwidth (data transmission speed).
5) The failure rates of the communication channels or resources are the same when they are idle or loaded (hot standby model). The failures of different resources and communication links are independent.
6) If the failure of a resource or a communication channel occurs before the end of output data transmission from the resource to the RMS, the subtask fails.
7) Different resources start performing their tasks immediately after they get the input data from the RMS through communication channels. If same subtask is processed by several resources (providing execution redundancy), it is completed when the first result is returned to the RMS. The entire task is completed when all of the subtasks are completed and their results are returned to the RMS from the resources.
8) The data transmission speed in any multi-channel link does not depend on the number of different packages (corresponding to different subtasks) sent in parallel. The data transmission time of each package depends on the amount of data in the package. If the data package is transmitted through several communication links, the link with the lowest bandwidth limits the data transmission speed.
9) The RMS is fully reliable, which can be justified to consider a relatively short interval of running a specific service. The imperfect RMS can also be easily included as a module connected in series to the whole grid service system.

65.2.4 Grid Service Time Distribution and Reliability/Performance Measures

The data dependence on task execution can be represented by $m \times m$ matrix H such that $h_{ki} = 1$ if subtask i needs for its execution output data from subtask k and $h_{ki} = 0$ otherwise (the subtasks can always be numbered such that $k<i$ for any $h_{ki} = 1$). Therefore, if $h_{ki} = 1$ execution of subtask i cannot begin before completion of subtask k. For any subtask i one can define a set ϕ_i of its immediate predecessors: $k \in \phi_i$ if $h_{ki} = 1$.

The data dependence can always be presented in such a manner that the last subtask m corresponds to final task processed by the RMS when it receives output data of all the subtasks completed by the grid resources.

The task execution time is defined as time from the beginning of input data transmission from the RMS to a resource to the end of output data transmission from the resource to the RMS.

The amount of data that should be transmitted between the RMS and resource j that executes subtask i is denoted by a_i. If data transmission between the RMS and the resource j is accomplished through links belonging to a set γ_j, the data transmission speed is

$$s_j = \min_{L_x \in \gamma_j} (b_x), \qquad (65.1)$$

where b_x is the bandwidth of the link L_x. Therefore, the random time t_{ij} of subtask i execution by resource j can take two possible values

$$t_{ij} = \hat{t}_{ij} = \tau_j + \frac{a_i}{s_j} \qquad (65.2)$$

if the resource j and the communication path γ_j do not fail until the subtask completion and $t_{ij} = \infty$ otherwise. Here, τ_j is the processing time of the *j-th* resource.

Subtask i can be successfully completed by resource j if this resource and communication path γ_j do not fail before the end of subtask execution. Given constant failure rates of resource j and links,

one can obtain the conditional probability of subtask success as

$$p_j(\hat{t}_{ij}) = e^{-(\lambda_j+\pi_j)\hat{t}_{ij}}, \quad (65.3)$$

where π_j is the failure rate of the communication path between the RMS and the resource j, which can be calculated as $\pi_j = \sum_{x\in\gamma_j}\lambda_x$, λ_x is the failure rate of the link L_x. The exponential distribution (65.3) is common in software or hardware components' reliability that had been justified in both theory and practice [15].

These give the conditional distribution of the random subtask execution time t_{ij}:

$\Pr(t_{ij} = \hat{t}_{ij}) = p_j(t_{ij})$ and

$\Pr(t_{ij} = \infty) = 1 - p_j(t_{ij})$.

Assume that each subtask i is assigned by the RMS to resources composing set ω_i. The RMS can initiate execution of any subtask j (send the data to all the resources from ω_i) only after the completion of every subtask $k \in \phi_i$. Therefore the random time of the start of subtask i execution T_i can be determined as

$$T_i = \max_{k\in\phi_i}(\tilde{T}_k), \quad (65.4)$$

where $\tilde{T}_k$ is random completion time for subtask k. If $\phi_i = \varnothing$, *i.e.* subtask i does not need data produced by any other subtask, the subtask execution starts without delay: $T_i = 0$. If $\phi_i \neq \varnothing$, T_i can have different realizations $\hat{T}_{il}$ ($1 \le l \le N_i$).

Having the time T_i when the execution of subtask i starts and the time t_{ij} of subtask i executed by resource j, one obtains the completion time for subtask i on resource j as

$$\tilde{t}_{ij} = T_i + t_{ij}. \quad (65.5)$$

In order to obtain the distribution of random time $\tilde{t}_{ij}$ one has to take into account that probability of any realization of $\tilde{t}_{ij} = \hat{T}_{il} + \hat{t}_{ij}$ is equal to the product of probabilities of three events:

- execution of subtask i starts at time $\hat{T}_{il}$: $q_{il}=\Pr(T_i = \hat{T}_{il})$;
- resource j does not fail before start of execution of subtask i: $p_j(\hat{T}_{il})$;
- resource j does not fail during the execution of subtask i: $p_j(\hat{t}_{ij})$.

Therefore, the conditional distribution of the random time $\tilde{t}_{ij}$ given execution of subtask i starting at time $\hat{T}_{il}$ ($T_i = \hat{T}_{il}$) takes the form

$$\Pr(\tilde{t}_{ij} = \hat{T}_{il} + \hat{t}_{ij}) = p_j(\hat{T}_{il})p_j(\hat{t}_{ij}) = p_j(\hat{T}_{il} + \hat{t}_{ij}) = e^{-(\lambda_j+\pi_j)(\hat{T}_{il}+\hat{t}_{ij})}, \quad (65.6)$$

$$\Pr(\tilde{t}_{ij} = \infty) = 1 - p_j(\hat{T}_{il} + \hat{t}_{ij}) = 1 - e^{-(\lambda_j+\pi_j)(\hat{T}_{il}+\hat{t}_{ij})}.$$

The random time of subtask i completion $\tilde{T}_i$ is equal to the shortest time when one of the resources from ω_i completes the subtask execution:

$$\tilde{T}_i = \min_{j\in\omega_i}(\tilde{t}_{ij}). \quad (65.7)$$

According to the definition of the last subtask m, the time of its beginning corresponds to the service completion time, because the time of the task proceeds with RMS is neglected. Thus, the random service time Θ is equal to T_m. Having the distribution (pmf) of the random value $\Theta \equiv T_m$ in the form $q_{ml} = \Pr(T_m = \hat{T}_{ml})$ for $1 \le l \le N_m$, one can evaluate the reliability and performance indices of the grid service.

In order to estimate both the service reliability and its performance, different measures can be used depending on the application. In applications where the execution time of each task (service

time) is of critical importance, the system reliability $R(\Theta^*)$ is defined (according to performability concept in [21–23] as a probability that the correct output is produced in time less than Θ^*.

This index can be obtained as

$$R(\Theta^*) = \sum_{l=1}^{N_m} q_{ml} \cdot 1(\hat{T}_{ml} < \Theta^*). \quad (65.8)$$

When no limitations are imposed on the service time, the service reliability is defined as the probability that it produces correct outputs without respect to the service time, which can be referred to as $R(\infty)$. The conditional expected service time W is considered to be a measure of its performance, which determines the expected service time given that the service does not fail, *i.e.*,

$$W = \sum_{l=1}^{N_m} \hat{T}_{ml} q_{ml} / R(\infty). \quad (65.9)$$

65.3 Star Topology Grid Architecture

A grid service is desired to execute a certain task under the control of the RMS. When the RMS receives a service request from a user, the task can be divided into a set of subtasks that are executed in parallel. The RMS assigns those subtasks to available resources for execution. After the resources complete the assigned subtasks, they return the results back to the RMS and then the RMS integrates the received results into entire task output which is requested by the user.

The above grid service process can be approximated by a structure with star topology, as depicted by Figure 65.2, where the RMS is directly connected with any resource through respective communication channels. The star topology is feasible when the resources are totally separated so that their communication channels are independent. Under this assumption the grid service reliability and performance can be derived by using the universal generating function technique.

65.3.1 Universal Generating Function

The universal generating function (u-function) technique was introduced and proved to be very effective for the reliability evaluation of different types of multi-state systems [24].

The u-function representing the pmf of a discrete random variable Y is defined as a polynomial

$$u(z) = \sum_{k=1}^{K} \alpha_k z^{y_k}, \quad (65.10)$$

where the variable Y has K possible values and α_k is the probability that Y is equal to y_k.

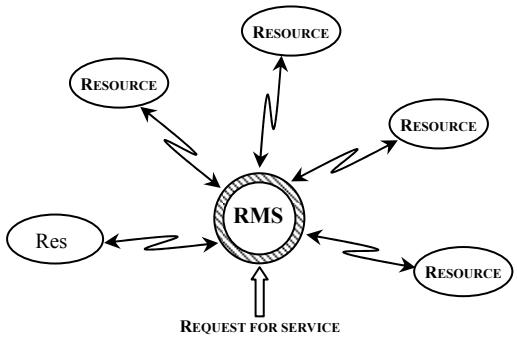


Figure 65.2. Grid system with star architecture

To obtain the u-function representing the pmf of a function of two independent random variables $\varphi(Y_i, Y_j)$, composition operators are introduced. These operators determine the u-function for $\varphi(Y_i, Y_j)$ using simple algebraic operations on the individual u-functions of the variables. All of the composition operators take the form

$$U(z) = u_i(z) \otimes_{\varphi} u_j(z) = \sum_{k=1}^{K_i} \alpha_{ik} z^{y_{ik}} \otimes_{\varphi} \sum_{h=1}^{K_j} \alpha_{jh} z^{y_{jh}} = \sum_{k=1}^{K_i} \sum_{h=1}^{K_j} \alpha_{ik} \alpha_{jh} z^{\varphi(y_{ik}, y_{jh})} \quad (65.11)$$

The u-function U(z) represents all of the possible mutually exclusive combinations of realizations of the variables by relating the probabilities of each

combination to the value of function $\varphi(Y_i, Y_j)$ for this combination.

In the case of grid system, the u-function $u_{ij}(z)$ can define pmf of execution time for subtask *i* assigned to resource *j*. This u-function takes the form

$$u_{ij}(z) = p_j(\hat{t}_{ij}) z^{\hat{t}_{ij}} + (1 - p_j(\hat{t}_{ij})) z^{\infty}, \quad (65.12)$$

where $\hat{t}_{ij}$ and $p_j(\hat{t}_{ij})$ are determined according to (65.2) and (65.3), respectively.

The pmf of the random start time T_i for subtask *i* can be represented by u-function $U_i(z)$ taking the form

$$U_i(z) = \sum_{l=1}^{L_i} q_{il} z^{\hat{T}_{il}}, \quad (65.13)$$

where

$$q_{il} = \Pr(T_i = \hat{T}_{il}). \quad (65.14)$$

For any realization $\hat{T}_{il}$ of T_i the conditional distribution of completion time $\tilde{t}_{ij}$ for subtask *i* executed by resource *j* given $T_i = \hat{T}_{il}$ according to (65.6) can be represented by the u-function

$$\tilde{u}_{ij}(z, \hat{T}_{il}) = p_j(\hat{T}_{il} + \hat{t}_{ij}) z^{\hat{T}_{il} + \hat{t}_{ij}} + (1 - p_j(\hat{T}_{il} + \hat{t}_{ij})) z^{\infty}.$$

The total completion time of subtask *i* assigned to a pair of resources *j* and *d* is equal to the minimum of completion times for these resources according to (65.7). To obtain the u-function representing the pmf of this time, given $T_i = \hat{T}_{il}$, composition operator with $\varphi(Y_j, Y_d) = \min(Y_j, Y_d)$ should be used:

$$\begin{aligned}
\tilde{u}_i(z, \hat{T}_{il}) &= \tilde{u}_{ij}(z, \hat{T}_{il}) \otimes_{\min} \tilde{u}_{id}(z, \hat{T}_{il}) \\
&= [p_j(\hat{T}_{il} + \hat{t}_{ij}) z^{\hat{T}_{il} + \hat{t}_{ij}} + (1 - p_j(\hat{T}_{il} + \hat{t}_{ij})) z^{\infty}] \\
&\otimes_{\min} [p_d(\hat{T}_{il} + \hat{t}_{id}) z^{\hat{T}_{il} + \hat{t}_{id}} + (1 - p_d(\hat{T}_{il} + \hat{t}_{id})) z^{\infty}] \\
&= p_j(\hat{T}_{il} + \hat{t}_{ij}) p_d(\hat{T}_{il} + \hat{t}_{id}) z^{\hat{T}_{il} + \min(\hat{t}_{ij}, \hat{t}_{id})} \\
&+ p_d(\hat{T}_{il} + \hat{t}_{id})(1 - p_j(\hat{T}_{il} + \hat{t}_{ij})) z^{\hat{T}_{il} + \hat{t}_{id}} \\
&+ p_j(\hat{T}_{il} + \hat{t}_{ij})(1 - p_d(\hat{T}_{il} + \hat{t}_{id})) z^{\hat{T}_{il} + \hat{t}_{ij}} \\
&+ (1 - p_j(\hat{T}_{il} + \hat{t}_{ij}))(1 - p_d(\hat{T}_{il} + \hat{t}_{id})) z^{\infty}.
\end{aligned} \quad (65.15)$$

The u-function $\tilde{u}_i(z, \hat{T}_{il})$ representing the conditional pmf of completion time $\tilde{T}_i$ for subtask *i* assigned to all of the resources from set $\omega_i = \{j_1, \ldots, j_i\}$ can be obtained as

$$\tilde{u}_i(z, \hat{T}_{il}) = \tilde{u}_{ij_1}(z, \hat{T}_{il}) \otimes_{\min} \ldots \otimes_{\min} \tilde{u}_{ij_i}(z, \hat{T}_{il}), \quad (65.16)$$

$\tilde{u}_i(z, \hat{T}_{il})$ can be obtained recursively:

$$\begin{aligned}
&\tilde{u}_i(z, \hat{T}_{il}) = \tilde{u}_{ij_1}(z, \hat{T}_{il}), \\
&\tilde{u}_i(z, \hat{T}_{il}) = \tilde{u}_i(z, \hat{T}_{il}) \otimes_{\min} \tilde{u}_{ie}(z, \hat{T}_{il})
\end{aligned}$$

for $e = j_2, \ldots, j_i$. (65.17)

Having the probabilities of the mutually exclusive realizations of start time T_i, $q_{il} = \Pr(T_i = \hat{T}_{il})$ and u-functions $\tilde{u}_i(z, \hat{T}_{il})$ representing corresponding conditional distributions of task *i* completion time, we can now obtain the u-function representing the unconditional pmf of completion time $\tilde{T}_i$ as

$$\tilde{U}_i(z) = \sum_{l=1}^{N_i} q_{il} \tilde{u}_i(z, \hat{T}_{il}). \quad (65.18)$$

Having u-functions $\widetilde{U}_k(z)$ representing pmf of the completion time $\widetilde{T}_k$ for any subtask $k \in \phi_i = \{k_1,...,k_i\}$, one can obtain the u-functions $U_i(z)$ representing pmf of subtask i start time T_i according to (65.4) as

$$U_i(z) = \widetilde{U}_{k_1}(z) \underset{\max}{\otimes} \widetilde{U}_{k_2}(z) ... \underset{\max}{\otimes} \widetilde{U}_{k_i}(z) = \sum_{l=1}^{N_i} q_{il} z^{\hat{T}_{il}}. \quad (65.19)$$

$U_i(z)$ can be obtained recursively:

$$U_i(z) = z^0,$$
$$U_i(z) = U_i(z) \underset{\max}{\otimes} \widetilde{U}_e(z)$$
for $e = k_1, \ldots, k_i$. (65.20)

It can be seen that if $\phi_i = \varnothing$ then $U_i(z) = z^0$.

The final u-function $U_m(z)$ represents the pmf of random task completion time T_m in the form

$$U_m(z) = \sum_{l=1}^{N_m} q_{ml} z^{\hat{T}_{ml}}. \quad (65.21)$$

Using the operators defined above one can obtain the service reliability and performance indices by implementing the following algorithm:

1. Determine $\hat{t}_{ij}$ for each subtask i and resource $j \in \omega_i$ using (65.2);
   Define for each subtask i ($1 \le i \le m$) $\widetilde{U}_i(z) = U_i(z) = z^0$.
2. For all i:
   If $\phi_i = 0$ or if for any $k \in \phi_i$ $\widetilde{U}_k(z) \neq z^0$ (u-functions representing the completion times of all of the predecessors of subtask i are obtained)
   2.1. Obtain $U_i(z) = \sum_{l=1}^{N_i} q_{il} z^{\hat{T}_{il}}$ using recursive procedure (65.20);
   2.2. For $l = 1, \ldots, N_i$:
   2.2.1. For each $j \in \omega_i$ obtain $\widetilde{u}_{ij}(z, \hat{T}_{il})$ using (65.14);
   2.2.2. Obtain $\widetilde{u}_i(z)$ using recursive procedure (65.17);
   2.3. Obtain $\widetilde{U}_i(z)$ using (65.18).
3. If $U_m(z) = z^0$ return to step 2.
4. Obtain reliability and performance indices $R(\Theta^*)$ and W using (65.8) and (65.9).

65.3.2 Illustrative Example

This example presents analytical derivation of the indices $R(\Theta^*)$ and W for simple grid service that uses six resources. Assume that the RMS divides the service task into three subtasks. The first subtask is assigned to resources 1 and 2, the second subtask is assigned to resources 3 and 4, the third subtask is assigned to resources 5 and 6:
$\omega_1 = \{1,2\}$, $\omega_2 = \{3,4\}$, $\omega_3 = \{5,6\}$.
The failure rates of the resources and communication channels and subtask execution times are presented in Table 65.1.

Table 65.1. Parameters of grid system for the analytical example

No. of sub i	No. of res j	$\lambda_j+\pi_j$ (sec^{-1})	$\hat{t}_{ij}$ (sec)	$p_j(\hat{t}_{ij})$
1	1	0.0025	100	0.779
	2	0.00018	180	0.968
2	3	0.0003	250	-
	4	0.0008	300	-
3	5	0.0005	300	0.861
	6	0.0002	430	0.918

Subtasks 1 and 3 get the input data directly from the RMS, subtask 2 needs the output of subtask 1, the service task is completed when the RMS gets the outputs of both subtasks 2 and 3: $\phi_1 = \phi_3 = \varnothing$, $\phi_2 = \{1\}$, $\phi_4 = \{2,3\}$. These subtask precedence constraints can be represented by the directed graph in Figure 65.3.

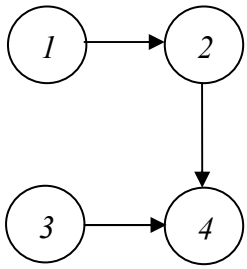


Figure 65.3. Subtask execution precedence constraints for the analytical example

Since $\phi_1 = \phi_3 = \varnothing$, the only realization of start times T_1 and T_3 is 0 and therefore, $U_1(z)=U_2(z)=z^0$. According to step 2 of the algorithm we can obtain the u-functions representing pmf of completion times $\tilde{t}_{11}$, $\tilde{t}_{12}$, $\tilde{t}_{35}$ and $\tilde{t}_{36}$. In order to determine the subtask execution time distributions for the individual resources, define the u-functions $u_{ij}(z)$ according to Table 65.1 and (65.9):

$$\tilde{u}_{11}(z,0) = \exp(-0.0025\times 100)z^{100} + [1-\exp(-0.0025\times 100)]z^{\infty} = 0.779z^{100} + 0.221z^{\infty}$$

In a similar way we obtain

$$\tilde{u}_{12}(z,0) = 0.968z^{180} + 0.032z^{\infty};$$

$$\tilde{u}_{35}(z,0) = 0.861z^{300} + 0.139z^{\infty};$$

$$\tilde{u}_{36}(z,0) = 0.918z^{430} + 0.082z^{\infty}.$$

The u-function representing the pmf of the completion time for subtask 1 executed by both resources 1 and 2 is

$$\tilde{U}_1(z) = \tilde{u}_1(z,0) = \tilde{u}_{11}(z,0) \underset{\min}{\otimes} \tilde{u}_{12}(z,0) =$$

$$(0.779z^{100} + 0.221z^{\infty}) \underset{\min}{\otimes} (0.968z^{180} + 0.032z^{\infty})$$

$$=0.779z^{100} + 0.214z^{180} + 0.007z^{\infty}.$$

The u-function representing the pmf of the completion time for subtask 3 executed by both resources 5 and 6 is

$$\tilde{U}_3(z) = \tilde{u}_3(z,0) = \tilde{u}_{35}(z) \underset{\min}{\otimes} \tilde{u}_{36}(z) =$$

$$(0.861z^{300} + 0.139z^{\infty}) \underset{\min}{\otimes} (0.918z^{430} + 0.082z^{\infty})$$

$$=0.861z^{300} + 0.128z^{430} + 0.011z^{\infty}.$$

Execution of subtask 2 begins immediately after completion of subtask 1. Therefore,

$$U_2(z) = \tilde{U}_1(z) = 0.779z^{100} + 0.214z^{180} + 0.007z^{\infty}$$

(T_2 has three realizations 100, 180 and ∞).

The u-functions representing the conditional pmf of the completion times for the subtask 2 executed by individual resources are obtained as follows.

$$\tilde{u}_{23}(z,100) = e^{-0.0003\times(100+250)}z^{100+250} + [1-e^{-0.0003\times(100+250)}]z^{\infty} = 0.9z^{350} + 0.1z^{\infty};$$

$$\tilde{u}_{23}(z,180) = e^{-0.0003\times(180+250)}z^{180+250} + [1-e^{-0.0003\times(180+250)}]z^{\infty} = 0.879z^{430} + 0.121z^{\infty};$$

$$\tilde{u}_{23}(z,\infty) = z^{\infty};$$

$$\tilde{u}_{24}(z,100) = e^{-0.0008\times(100+300)}z^{100+300} + [1-e^{-0.0008\times(100+300)}]z^{\infty} = 0.726z^{400} + 0.274z^{\infty};$$

$$\tilde{u}_{24}(z,180) = e^{-0.0008\times(180+300)}z^{180+300} + [1-e^{-0.0008\times(180+300)}]z^{\infty} = 0.681z^{480} + 0.319z^{\infty};$$

$$\tilde{u}_{24}(z,\infty) = z^{\infty}.$$

The u-functions representing the conditional pmf of subtask 2 completion time are:

$$\tilde{u}_2(z,100) = \tilde{u}_{23}(z,100) \underset{\min}{\otimes} \tilde{u}_{24}(z,100) =$$

$$(0.9z^{350} + 0.1z^{\infty}) \underset{\min}{\otimes} (0.726z^{400} + 0.274z^{\infty})$$

$$=0.9z^{350} + 0.073z^{400} + 0.027z^{\infty};$$

$$\tilde{u}_2(z,180) = \tilde{u}_{23}(z,180) \underset{\min}{\otimes} \tilde{u}_{24}(z,180) =$$

$$(0.879z^{430} + 0.121z^{\infty}) \underset{\min}{\otimes} (0.681z^{480} + 0.319z^{\infty})$$

$$=0.879z^{430} + 0.082z^{480} + 0.039z^{\infty};$$

$$\tilde{u}_2(z,\infty) = \tilde{u}_{23}(z,\infty) \underset{\min}{\otimes} \tilde{u}_{24}(z,\infty) = z^{\infty}.$$

According to (65.18) the unconditional pmf of subtask 2 completion time is represented by the following u-function

$$\tilde{U}_2(z) = 0.779\tilde{u}_2(z,100) + 0.214\tilde{u}_2(z,180) + 0.007z^{\infty}$$

$=0.779(0.9z^{350}+0.073z^{400}+0.027z^{\infty})+0.214(0.879z^{430}+0.082z^{480}+0.039z^{\infty})+0.007z^{\infty}$

$=0.701z^{350}+0.056z^{400}+0.188z^{430}+0.018z^{480}+0.037z^{\infty}$

The service task is completed when subtasks 2 and 3 return their outputs to the RMS (which corresponds to the beginning of subtask 4). Therefore, the u-function representing the pmf of the entire service time is obtained as

$$U_4(z) = \tilde{U}_2(z) \underset{\max}{\otimes} \tilde{U}_3(z)$$

$=(0.701z^{350}+0.056z^{400}+0.188z^{430}+0.018z^{480}+0.037z^{\infty}) \underset{\max}{\otimes} (0.861z^{300}+0.128z^{430}+0.011z^{\infty})=0.603z^{350}+0.049z^{400}+0.283z^{430}+0.017z^{480}+0.048z^{\infty}.$

The pmf of the service time is:

$\Pr(T_4 = 350) = 0.603$; $\Pr(T_4 = 400) = 0.049$;

$\Pr(T_4 = 430) = 0.283$; $\Pr(T_4 = 480) = 0.017$;

$\Pr(T_4 = \infty) = 0.048$.

From the obtained pmf we can calculate the service reliability using (65.8):

$R(\Theta^*) = 0.603$ for $350 < \Theta^* \le 400$;

$R(\Theta^*) = 0.652$ for $400 < \Theta^* \le 430$;

$R(\Theta^*) = 0.935$ for $430 < \Theta^* \le 480$;

$R(\infty) = 0.952$

and the conditional expected service time according to (65.9):

$W = (0.603\times350 + 0.049\times400 + 0.283\times430 + 0.017\times480) / 0.952 = 378.69$ sec.

65.4 Tree Topology Grid Architecture

In the star grid, the RMS is connected with each resource by one direct communication channel (link). However, such approximation is not accurate enough even though it simplifies the analysis and computation. For example, several resources located in a same local area network (LAN) can use the same gateway to communicate outside the network. Therefore, all these resources are not connected with the RMS through independent links. The resources are connected to the gateway, which communicates with the RMS through one common communication channel. Another example is a server that contains several resources (has several processors that can run different applications simultaneously, or contains different databases). Such a server communicates with the RMS through the same links. These situations cannot be modeled using only the star topology grid architecture.

In this section, we present a more reasonable virtual structure which has a tree topology. The root of the tree virtual structure is the RMS, and the leaves are resources, while the branches of the tree represent the communication channels linking the leaves and the root. Some channels are commonly used by multiple resources. An example of the tree topology is given in Figure 65.3 in which four resources (R1, R2, R3, R4) are available for a service.

The tree structure models the common cause failures in shared communication channels. For example, in Figure 65.4, the failure in channel L6 makes resources R1, R2, and R3 unavailable. This type of common cause failure was ignored by the conventional parallel computing models, and the above star-topology models. For small-area communication, such as a LAN or a cluster, such an assumption that ignores the common cause failures on communications is acceptable because the communication time is negligible compared to the processing time. However, for wide-area communication, such as the grid system, it is more likely to have failure on communication channels. Therefore, the communication time cannot be neglected. In many cases, the communication time may dominate the processing time due to the large amount of data transmitted. Therefore, the virtual tree structure is an adequate model representing the functioning of grid services.

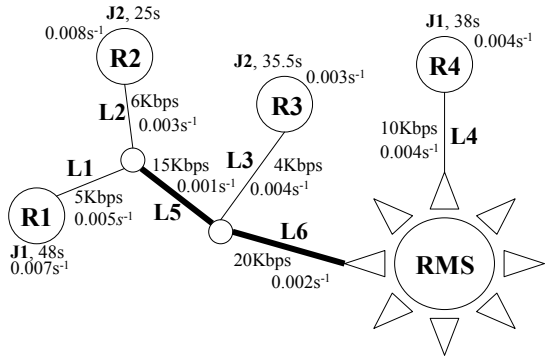


Figure 65.4. Virtual tree structure of a grid service

65.4.1 Algorithms for Determining the pmf of the Task Execution Time

With the tree structure, the simple u-function technique is not applicable because it does not consider the failure correlations. Thus, new algorithms are required. This section presents a novel algorithm to evaluate the performance and reliability for the tree-structured grid service based on graph theory and the Bayesian approach.

65.4.1.1 Minimal Task Spanning Tree (MTST)

The set of all nodes and links involved in performing a given task form a task spanning tree. This task spanning tree can be considered to be a combination of minimal task spanning trees (MTST), where each MTST represents a minimal possible combination of available elements (resources and links) that guarantees the successful completion of the entire task. The failure of any element in a MTST leads to the entire task failure.

For solving the graph traversal problem, several classical algorithms have been suggested, such as depth-first search, breadth-first search, *etc*. These algorithms can find all MTST in an arbitrary graph [16]. However, MTST in graphs with a tree topology can be found in a much simpler way because each resource has a single path to the RMS, and the tree structure is acyclic.

After the subtasks have been assigned to corresponding resources, it is easy to find all combinations of resources such that each combination contains exactly m resources executing m different subtasks that compose the entire task. Each combination determines exactly one MTST consisting of links that belong to paths from the m resources to the RMS. The total number of MTST is equal to the total number of such combinations N, where

$$N = \prod_{j=1}^{m} |\omega_j| \qquad (65.22)$$

(see Section 65.4.2.1).

Along with the procedures of searching all the MTST, one has to determine the corresponding running time and communication time for all the resources and links.

For any subtask j, and any resource k assigned to execute this subtask, one has the amount of input and output data, the bandwidths of links, belonging to the corresponding paths γ_k, and the resource processing time. With these data, one can obtain the time of subtask completion (see Section 65.4.2.2).

Some elements of the same MTST can belong to several paths if they are involved in data transmission to several resources. To track the element involvement in performing different subtasks and to record the corresponding times in which the element failure causes the failure of a subtask, we create the lists of two-field records for each subtask in each MTST. For any MTST S_i ($1 \le i \le N$), and any subtask j ($1 \le j \le m$), this list contains the names of the elements involved in performing the subtask j, and the corresponding time of subtask completion y_{ij} (see Sections 65.4.2.3 and 65.4.2.4). Note that y_{ij} is the conditional time of subtask j completion given only MTST i is available.

Note that a MTST completes the entire task if all of its elements do not fail by the maximal time needed to complete subtasks in performing which they are involved. Therefore, when calculating the element reliability in a given MTST, one has to use the corresponding record with maximal time.

65.4.1.2 pmf of the Task Execution Time

Having the MTST, and the times of their elements involvement in performing different subtasks, one can determine the pmf of the entire service time.

First, we can obtain the conditional time of the entire task completion given only MTST S_i is available as

$$Y_{\{i\}} = \max_{1\le j\le m}(y_{ij}) \text{ for any } 1\le i\le N. \quad (65.23)$$

For a set ψ of available MTST, the task completion time is equal to the minimal task completion times among the MTST.

$$Y_{\psi} = \min_{i\in\psi}(Y_{\{i\}}) = \min_{i\in\psi}\left[\max_{1\le j\le m}(y_{ij})\right]. \quad (65.24)$$

Now, we can sort the MTST in an increasing order of their conditional task completion times $Y_{\{i\}}$, and divide them into different groups containing MTST with identical conditional completion time. Suppose there are K such groups denoted by $G_1, G_2, ..., G_K$ where $1 \le K \le N$, and any group G_i contains MTST with identical conditional task completion times Θ_i ($0 \le \Theta_1 < \Theta_2 < ... < \Theta_K$). Then, it can be seen that the probability $Q_i = \Pr(\Theta = \Theta_i)$ can be obtained as

$$Q_i = \Pr(E_i, \overline{E}_{i-1}, \overline{E}_{i-2}, ..., \overline{E}_1) \quad (65.25)$$

where E_i is the event when at least one of MTST from the group G_i is available, and $\overline{E}_i$ is the event when none of MTST from the group G_i is available.

Suppose the MTST in a group G_i are arbitrarily ordered, and F_{ij} (j=1,2,…, N_i) represents an event when the j-th MTST in the group is available. Then, the event E_i can be expressed by

$$E_i = \bigcup_{j=1}^{N_i} F_{ij}, \quad (65.26)$$

and (65.25) takes the form

$$\Pr(E_i, \overline{E}_{i-1}, \overline{E}_{i-2}, ..., \overline{E}_1) = \Pr(\bigcup_{j=1}^{N_i} F_{ij}, \overline{E}_{i-1}, \overline{E}_{i-2}, ..., \overline{E}_1). \quad (65.27)$$

Using the Bayesian theorem on conditional probability, we obtain from (65.27) that

$$Q_i = \sum_{j=1}^{N_i} \Pr(F_{ij}) \cdot \Pr(\overline{F}_{i(j-1)}, \overline{F}_{i(j-2)}, ..., \overline{F}_{i1}, \overline{E}_1, \overline{E}_2, \cdots, \overline{E}_{i-1} \mid F_{ij}) \quad (65.28)$$

The probability $\Pr(F_{ij})$ can be calculated as a product of the reliabilities of all the elements belonging to the jth MTST from group G_i.

The probability $\Pr(\overline{F}_{i(j-1)}, \overline{F}_{i(j-2)}, ..., \overline{F}_{i1}, \overline{E}_1, \overline{E}_2, \cdots, \overline{E}_{i-1} \mid F_{ij})$ can be computed by the following two-step algorithm (see Example 4.2.4).

Step 1: Identify failures of all the critical elements' in a period of time (defined by the start and end time), during which they lead to the failures of any MTST from groups G_m for m=1,2,…i-1 (events $\overline{E}_m$), and any MTST S_k from group G_i for k=1,2,…, $j-1$ (events $\overline{F}_{ik}$), but do not affect the MTST S_j from group G_i.

Step 2: Generate all the possible combinations of the identified critical elements that lead to the event $\overline{F}_{i(j-1)}, \overline{F}_{i(j-2)}, ..., \overline{F}_{i1}, \overline{E}_1, \overline{E}_2, \cdots, \overline{E}_{i-1} \mid F_{ij}$ using a binary search, and compute the probabilities of those combinations. The sum of the probabilities obtained is equal to $\Pr(\overline{F}_{i(j-1)}, \overline{F}_{i(j-2)}, ..., \overline{F}_{i1}, \overline{E}_1, \overline{E}_2, \cdots, \overline{E}_{i-1} \mid F_{ij})$. When calculating the failure probabilities of MTSTs' elements, the maximal time from the corresponding records in a list for the given MTST should be used. The algorithm for obtaining the probabilities $\Pr\{\overline{E}_1, \overline{E}_2, \cdots \overline{E}_{i-1} \mid E_i\}$ can be found in Dai *et al.* [16].

Having the conditional task completion times $Y_{\{i\}}$ for different MTST, and the corresponding probabilities Q_i, one obtains the task completion time distribution (Θ_i, Q_i), $1\le i\le K$, and can easily calculate the indices (65.8) and (65.9) (see Section 65.4.2.5).

65.4.2 Illustrative Example

Consider the virtual grid presented in Figure 65.4, and assume that the service task is divided into two subtasks J1 assigned to resources R1 and R4, and J2 assigned to resources R2 and R3. J1, and J2 require 50 Kbits, and 30 Kbits of input data, respectively, to be sent from the RMS to the corresponding resource; and 100 Kbits, and 60 Kbits of output data respectively to be sent from the resource back to the RMS.

The subtask processing times for resources, bandwidth of links, and failure rates are presented in Figure 65.4 next to the corresponding elements.

65.4.2.1 The Service MTST

The entire graph constitutes the task spanning tree. There exist four possible combinations of two resources executing both subtasks: {R1, R2}, {R1, R3}, {R4, R2}, {R4, R3}. The four MTST corresponding to these combinations are: S_1: {R1, R2, L1, L2, L5, L6}; S_2: {R1, R3, L1, L3, L5, L6}; S_3: {R2, R4, L2, L5, L4, L6}; S_4: {R3, R4, L3, L4, L6}.

65.4.2.2 Parameters of MTSTs' Paths

Having the MTST, one can obtain the data transmission speed for each path between the resource, and the RMS (as minimal bandwidth of links belonging to the path); and calculate the data transmission times, and the times of subtasks' completion. These parameters are presented in Table 65.2. For example, resource R1 (belonging to two MTST S_1 & S_2) processes subtask J1 in 48 seconds. To complete the subtask, it should receive 50 Kbits, and return to the RMS 100 Kbits of data. The speed of data transmission between the RMS and R1 is limited by the bandwidth of link L1, and is equal to 5 Kbps. Therefore, the data transmission time is 150/5=30 seconds, and the total time of task completion by R1 is 30+48=78 s.

Table 65.2. Parameters of the MTSTs' paths

Elements	R1	R2	R3	R4
Subtasks	J1	J2	J2	J1
Transmission speed (Kbps)	5	6	4	10
Data transmission time (s)	30	15	22.5	15
Processing time (s)	48	25	35.5	38
Subtask complete time (s)	78	40	58	53

65.4.2.3 List of MTST Elements

Now one can obtain the lists of two-field records for components of the MTST.

S_1: path for J1:(R1,78); (L1,78); (L5,78); (L6,78); path for J2: (R2,40); (L2,40); (L5,40); (L6,40).

S_2: path for J1: (R1,78), (L1,78), (L5,78), (L6,78); path for J2: (R3,58), (L3,58), (L6,58).

S_3: path for J1: (R4,53), (L4,53); path for J2: (R2,40), (L2,40), (L5,40), (L6,40).

S_4: path for J1: (R4,53), (L4,53); path for J2: (R3,58), (L3,58), (L6,58).

65.4.2.4 pmf of Task Completion Time

The conditional times of the entire task completion by different MTST are

Y_1=78; Y_2=78; Y_3=53; Y_4=58.

Therefore, the MTST compose three groups:

$G_1 = \{S_3\}$ with $\Theta_1 = 53$; $G_2 = \{S_4\}$ with $\Theta_2 = 58$; and $G_3 = \{S_1, S_2\}$ with $\Theta_3 = 78$.

According to (65.25), we have for group G_1: $Q_1=\Pr(E_1)=\Pr(S_3)$. The probability that the MTST S_3 completes the entire task is equal to the product of the probabilities that R4, and L4 do not fail by 53 seconds; and R2, L2, L5, and L6 do not fail by 40 seconds.

$\Pr(\Theta=53)=Q_1=\exp(-0.004\times53)\exp(-0.004\times53)\exp(-0.008\times40)$
$\times\exp(-0.003\times40)\exp(-0.001\times40)\exp(-0.002\times40) = 0.3738.$

Now we can calculate Q_2 as

$$Q_2=\Pr(E_2,\overline{E}_1)=\Pr(F_{21})\Pr(\overline{E}_1|F_{21})=\Pr(F_{21})\Pr(\overline{F}_{11}|F_{21})=\Pr(S_4)\Pr(\overline{S}_3|S_4)$$

because G_2, and G_1 have only one MTST each. The probability that the MTST S_4 completes the entire task $\Pr(S_4)$ is equal to the product of probabilities that R3, L3, and L6 do not fail by 58 seconds; and R4, and L4 do not fail by 53 seconds.

$$\Pr(S_4) = \exp(-0.004\times53)\exp(-0.003\times58)\exp(-0.004\times53)\exp(-0.004\times58)\exp(-0.002\times58)$$

= 0.3883

To obtain $\Pr(\overline{S}_3|S_4)$, one first should identify the critical elements according to the algorithm presented in the Dai *et al.* [16]. These elements are R2, L2, and L5. Any failure occurring in one of these elements by 40 seconds causes failure of S_3, but does not affect S_4. The probability that at least one failure occurs in the set of critical elements is

$$\Pr(\overline{S}_3|S_4) = 1-\exp(-0.08\times4)\exp(-0.03\times4)\exp(-0.01\times4) = 0.3812.$$

Then,

$$\Pr(\Theta=58) = \Pr(E_2, \overline{E}_1) = \Pr(S_4)\Pr(\overline{S}_3|S_4) = 0.3883\times0.3812 = 0.1480.$$

Now one can calculate Q_3 for the last group $G_3 = \{S_1, S_2\}$ corresponding to $\Theta_3 = 78$ as

$$Q_3 = \Pr(E_3, \overline{E}_2, \overline{E}_1) = \Pr(F_{31})\Pr(\overline{E}_1, \overline{E}_2|F_{31}) + \Pr(F_{32})\Pr(\overline{F}_{31}, \overline{E}_1, \overline{E}_2|F_{32}) = \Pr(S_1)\Pr(\overline{S}_3, \overline{S}_4|S_1) + \Pr(S_2)\Pr(\overline{S}_1, \overline{S}_3, \overline{S}_4|S_2)$$

The probability that the MTST S_1 completes the entire task is equal to the product of the probabilities that R1, L1, L5, and L6 do not fail by 78 seconds; and R2, and L2 do not fail by 40 seconds.

$$\Pr(S_1) = \exp(-0.007\times78)\exp(-0.008\times40)\exp(-0.005\times78)\exp(-0.003\times40)\times\exp(-0.001\times78)\exp(-0.002\times78) = 0.1999.$$

The probability that the MTST S_2 completes the entire task is equal to the product of the probabilities that R1, L1, L5, and L6 do not fail by 78 seconds; and R3, and L3 do not fail by 58 seconds.

$$\Pr(S_2) = \exp(-0.007\times78)\exp(-0.003\times58)\exp(-0.005\times78)\exp(-0.004\times58)\times\exp(-0.001\times78)\exp(-0.002\times78) = 0.2068.$$

To obtain $\Pr(\overline{S}_3, \overline{S}_4|S_1)$, one first should identify the critical elements. Any failure of either R4 or L4 in the time interval from 0 to 53 seconds causes failures of both S_3, and S_4; but does not affect S_1. Therefore,

$$\Pr(\overline{S}_3, \overline{S}_4|S_1) = 1-\exp(-0.004\times53)\exp(-0.004\times53) = 0.3456.$$

The critical elements for calculating $\Pr(\overline{S}_1, \overline{S}_3, \overline{S}_4|S_2)$ are R2, and L2 in the interval from 0 to 40 seconds; and R4, and L4 in the interval from 0 to 53 seconds. The failure of both elements in any one of the following four combinations causes failures of S_3, S_4, and S_1, but does not affect S_2:

1. R2 during the first 40 seconds, and R4 during the first 53 seconds;
2. R2 during the first 40 seconds, and L4 during the first 53 seconds;
3. L2 during the first 40 seconds, and R4 during the first 53 seconds; and
4. L2 during the first 40 seconds, and L4 during the first 53 seconds.

Therefore,

$$\Pr(\overline{S}_1, \overline{S}_3, \overline{S}_4|S_2) = 1-\prod_{i=1}^{4}\left[1-\prod_{j=1}^{2}[1-\exp(\lambda_{ij}\cdot t_{ij})]\right] = 0.1230,$$

where λ_{ij} is the failure rate of the jth critical element in the ith combination (j=1,2), (i=1,2,3,4); and t_{ij} is the duration of the time interval for the corresponding critical element.

Having the values of $\Pr(S_1), \Pr(S_2), \Pr(\overline{S}_3, \overline{S}_4|S_1)$, and $\Pr(\overline{S}_1, \overline{S}_3, \overline{S}_4|S_2)$, one can calculate

$$\Pr(\Theta=78) = Q_3 = 0.1999\times0.3456+0.2068\times0.1230=0.0945.$$

After obtaining Q_1, Q_2, and Q_3, one can evaluate the total task failure probability as
$\Pr(\Theta=\infty)=1-Q_1-Q_2-Q_3$
$=1-0.3738-0.1480-0.0945=0.3837$,
and obtain the pmf of service time presented in Table 65.3.

Table 65.3. pmf of service time

Θ_i	Q_i	$\Theta_i Q_i$
53	0.3738	19.8114
58	0.1480	8.584
78	0.0945	7.371
∞	0.3837	∞

65.4.2.5 Calculating the Reliability Indices

From Table 65.3, one obtains the probability that the service does not fail as

$$R(\infty) = Q_1 + Q_2 + Q_3 = 0.6164,$$

the probability that the service time is not greater than a pre-specified value of θ^*=60 seconds as

$$R(\theta^*) = \sum_{i=1}^{3} Q_i \cdot 1(\Theta_i < \theta^*) = 0.3738 + 0.1480 = 0.5218,$$

and the expected service execution time given that the system does not fail as

$$W = \sum_{i=1}^{3} \Theta_i Q_i / R(\infty) = 35.7664 / 0.6164 = 58.025$$

seconds.

65.4.3 Parameterization and Monitoring

In order to obtain the reliability and performance indices of the grid service one has to know such model parameters as the failure rates of the virtual links and the virtual nodes, and bandwidth of the links. It is easy to estimate those parameters by implementing the monitoring technology.

A monitoring system (the *Alertmon NetworkMonitor,* http://www.abilene.iu.edu/noc.html) is being applied in the IP-grid (Indiana Purdue Grid) project (www.ip-grid.org), to detect the component failures, to record service behavior, to monitor the network traffics, and to control the system configurations.

With this monitoring system, one can easily obtain the parameters required by the grid service reliability model by adding the following functions in the monitoring system:

1) Monitoring the failures of the components (virtual links and nodes) in the grid service, and recording the total execution time s of those components. The failure rates of the components can be simply estimated by the number of failures over the total execution time.
2) Monitoring the real time network traffic of the involved channels (virtual links) in order to obtain the bandwidth of the links.

To achieve the above monitoring functions, network sensors are required. We presented a type of sensor attaching to the components, acting as neurons attaching to the skins. This means the components themselves or adjacent components play the roles of sensors at the same time when they are working. Only a little computational resource in the components is used for accumulating failures/time and for dividing operations, and only a little memory is required for saving the data (accumulated number of failures, accumulated time, and current bandwidth). The virtual nodes that have memory and computational function can play the sensing role themselves; if some links have no CPU or memory, then the adjacent processors or routers can perform this data collecting operations. Using such a self-sensing technique avoids overloading of the monitoring center even in the grid system containing numerous components. Again, it does not affect the service performance considerably since only small part of computation and storage resources is used for the monitoring. In addition, such a self-sensing technique can also be applied in monitoring other measures.

When evaluating the grid service reliability, the RMS automatically loads the required parameters from corresponding sensors and calculates the service reliability and performance according to the approaches presented in the previous sections. This strategy can also be used for implementing the autonomic computing concept.

65.5 Conclusions

Grid computing is a newly developed technology for complex systems with large-scale resource sharing, wide-area communication, and multi-institutional collaboration. Although the developmental tools and techniques for the grid have been widely studied, grid reliability analysis and modeling are not easy because of their complexity of combining various failures.

This chapter introduced the grid computing technology and analyzed the grid service reliability and performance under the context of performability. The chapter then presented models for star-topology grid with data dependence and tree-structure grid with failure correlation. Evaluation tools and algorithms were presented based on the universal generating function, graph theory, and the Bayesian approach. Numerical examples were presented to illustrate the grid modeling and reliability/performance evaluation procedures and approaches.

Future research can extend the models for grid computing to other large-scale distributed computing systems. After analyzing the details and specificity of corresponding systems (*e.g.*, NASA ANTS missions), the approaches and models can be adapted to real conditions.

The models are also applicable to the wireless network that is more failure prone. Hierarchical models can also be analyzed in which output of lower level models can be considered as the input of the higher level models. Each level can make use of the proposed models and evaluation tools.

References

[1] Foster I, Kesselman C. The grid 2: Blueprint for a new computing infrastructure. San Francisco, CA: Morgan-Kaufmann, 2003

[2] Kumar A. An efficient SuperGrid protocol for high availability and load balancing. IEEE Transactions on Computers 2000; 49(10):1126–1133.

[3] Das SK, Harvey DJ, Biswas R. Parallel processing of adaptive meshes with load balancing. IEEE Transactions on Parallel and Distributed Systems 2001; 12(12):1269–1280.

[4] Foster I, Kesselman C, Tuecke S. The anatomy of the grid: Enabling scalable virtual organizations. International Journal of High Performance Computing Applications 2001; 15:200–222.

[5] Foster I, Kesselman C, Nick JM, Tuecke S. Grid services for distributed system integration. Computer 2002; 35(6):37–46.

[6] Berman F, Wolski R, Casanova H, Cirne W, Dail H, Faerman M, *et al.,* Adaptive computing on the Grid using AppLeS. IEEE Transactions on Parallel and Distributed Systems 2003; 14(14):369–382.

[7] Livny M, Raman R. High-throughput resource management. In: The grid: Blueprint for a new computing infrastructure. San Francisco, CA: Morgan-Kaufmann, 1998; 311–338.

[8] Cao J, Jarvis SA, Saini S, Kerbyson DJ, Nudd GR. ARMS: An agent-based resource management system for grid computing. Scientific Programming, 2002; 10(2):135–148.

[9] Krauter K, Buyya R, Maheswaran M. A taxonomy and survey of grid resource management systems for distributed computing. Software – Practice and Experience 2002; 32(2):135–164.

[10] Nabrzyski J, Schopf JM, Weglarz J. Grid resource management, Kluwer, Dordrecht, 2003.

[11] Abramson D, Buyya R, Giddy J. A computational economy for grid computing and its implementation in the Nimrod-G resource broker, Future Generation Computer Systems 200218(8):1061–1074.

[12] Ding Q, Chen GL, Gu J. A unified resource mapping strategy in computational grid environments. Journal of Software 2002; 13(7): 1303–1308.

[13] Xie M. Software reliability modeling. Singapore: World Scientific, 1991

[14] Pham H. Software reliability. Singapore: Springer, 2000.

[15] Xie M, Dai YS, Poh KL. Computing systems reliability: Models and analysis. New York: Kluwer, 2004.

[16] Dai YS, Xie M Poh KL. Reliability analysis of grid computing systems. IEEE Pacific Rim International Symposium on Dependable Computing (PRDC2002), IEEE Computer Press 2002; 97–104.

[17] Kumar VKP, Hariri S, Raghavendra CS. Distributed program reliability analysis. IEEE Transactions on Software Engineering 1986; SE–12:42–50.

[18] Chen DJ, Huang TH. Reliability analysis of distributed systems based on a fast reliability algorithm. IEEE Transactions on Parallel and Distributed Systems, 1992; 3 (2):139–154.

[19] Chen DJ, Chen RS, Huang TH. A heuristic approach to generating file spanning trees for reliability analysis of distributed computing

systems. Computers and Mathematics with Application 1997; 34:115–131.
[20] Lin MS, Chang MS, Chen DJ, Ku KL. The distributed program reliability analysis on ring-type topologies. Computers and Operations Research 2001; 28:625–635.
[21] Meyer J. On evaluating the performability of degradable computing systems. IEEE Transactions on Computers 1980; 29:720–731.
[22] Grassi V, Donatiello L, Iazeolla G. Performability evaluation of multicomponent fault tolerant systems. IEEE Transactions on Reliability 1988; 37(2):216–222.
[23] Tai A, Meyer J, Avizienis A. Performability enhancement of fault-tolerant software. IEEE Transactions on Reliability 1993; 42(2):227–237.
[24] Levitin G. Universal generating function in reliability analysis and optimization. Berlin: Springer, 2005.

66

Status and Trends in the Performance Assessment of Fault Tolerant Systems

John Kontoleon

Dept. of Electrical and Computer Engineering
Aristotle University of Thessaloniki, Thessaloniki, Greece

Abstract: Fault tolerance (FT) covers a wide spectrum of application areas and includes numerous considerations, such as, to refer to a few, system architecture, hardware and software design, operating systems, Internet protocol (IP) network communications, parallel and grid processing, and verification and testing. As fault tolerant systems are designed to perform even in the presence of faults, errors or attacks, their performance can be evaluated by taking into account the consequences of the embedded fault handling actions. After a brief description of the basic concepts, this chapter presents the general aspects of fault handling techniques in both hardware and software. Global FT issues, such as those encountered in modern computer networks are also presented. A discussion on the expected future trends points out the challenges in this critical area.

66.1 Introduction

The evolution in computer technology and architecture, with an increased VLSI replication, massive parallel and grid processing, and large-scale distributed systems, has been accompanied by advances in fault tolerant design [1]–[6]. Fault tolerance aims at preserving the delivery of correct service in the presence of faults. The design of fault tolerance into a system must be faced at the early stages of its conceptualization. Performance of fault tolerant systems is a measure of their ability to deliver efficiently the required service. The price of building fault tolerant systems in terms of performance depends on the requirements of their delivered service and can be justified after the systematic investigation of different ways for improving fault tolerance in the same application. The fundamental idea behind building in a fault tolerance capability is to provide the system with redundant resources in order to overcome the effects of faults. So far, there have been numerous research contributions, covering various aspects of fault tolerance and fault tolerant design related techniques, both in hardware and software. Broadly speaking, in recent years, much research in this area has been motivated by technological advances, micro-architectural innovations, high levels of VLSI integration, and internetworking [7],[8]. A fault tolerant system may be able to tolerate a set of single or multiple faults. System faults can be either fail-silent or Byzantine faults [9].

These faults are handled according to their nature, extent, and duration. Hardware may fail in a non-

predictable way causing arbitrary behavior before the system is halted. Software is hardly ever free of bugs and may also exhibit an unpredictable behavior. Last but not least, attacks are so widespread that they are a significant source of malicious corruption of nodes in distributed applications [10],[11]. The effectiveness of fault handling techniques, referred to as coverage, can be accomplished through modeling or fault injection. A system usually delivers more than one levels of service quality. Faults may cause the reduction of the quality of service even though that service remains satisfactory. Such degradation may also be due to additional computation demands associated with error processing or may be the consequence of fault related actions, as for example reconfiguration. An example could be the failure of a node in a computer cluster, causing the performance drop or even the temporal interruption of the service.

Over the last decade there has been a tremendous growth in the market of computer networks having varying capabilities both in hardware and software [12]. While in the past the network performance issues were approached by providing sufficient bandwidth, in recent years it has been recognized that this alone is not sufficient for managing complex heterogeneous networks. Network fault management has become more sophisticated by moving the intelligent code to the nodes where data is resident or through the application of artificial intelligence and expert systems methods. For instance, network reconfiguration is an intelligent activity that changes service requirements on the basis of the system's change. Fault management, proactive or reactive, centralized or not, enhances network's fault tolerance by handling problems that could otherwise cause the performance drop or even the interruption of the provided services.

This chapter serves three purposes. Firstly, to define the relevant kinds of redundancy, together with the implications, for approaching the wide area of hardware faults tolerance. Some system models are briefly revisited to sketch fault tolerant computing. Next to address the software fault tolerance, by briefly touching traditional and more novel techniques. Software fault tolerance is not as mature as hardware and its application relies mostly on the development of diverse software. Finally, to focus on global fault tolerant issues encountered in large computer architectures and in an internetworking environment. A section with a case study of a RAM system fault tolerant architecture and its performance evaluation is also included.

66.2 Hardware Fault Tolerant Architectures and Techniques

The common approach to fault tolerant design is redundancy. Hardware redundancy may be passive, active or a combination of both, so called, hybrid redundancy [13]. The choice for the most appropriate form of redundancy is usually dictated by the complexity of the functions of the particular system as well as that of the additional hardware for implementing and managing fault tolerance.

66.2.1 Passive Redundancy

Passive redundancy, assumes a number of replicas for the purpose of masking single or multiple failures. Fault detection and notification of the malfunction of a replica are often based on the assumption that only one replica can fail at a time. A good example of this type of redundancy is TMR (see Figure 66.1), in which three independent modules are used together with a voter. The voter provides the output on the basis of the majority of votes of the individual modules. This architecture can tolerate a single failure, failing silently, and at the same time provides an early warning on the "health" of the participating modules.

One basic prerequisite for TMR is that the module and voter reliabilities must be at least 0.75 and 0.889, respectively. NMR, an extension of this approach, can tolerate multiple failures. Obviously, TMR and NMR are quite costly, but more importantly, they rely on the proper function of the voter, which in the "chain" example, possibly adds a weak link in the chain. In general, depending on the particular functions of the modules, the voter can be a very simple or a very complex system. In applying TMR, NMR or any other passive redundancy technique (*e.g.*, quadded logic, *etc.*)

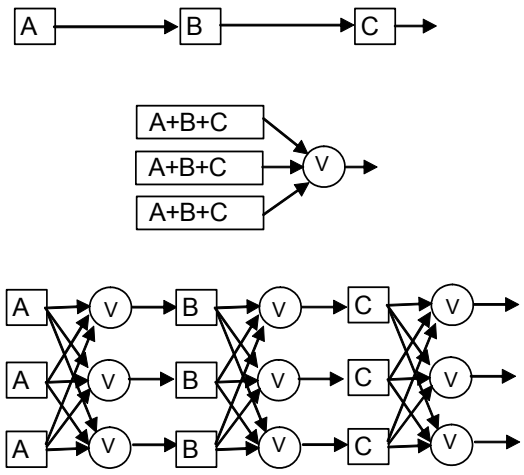


Figure 66.1. Application of triple modular redundancy at the system and subsystem levels

one has to consider very carefully factors such as the level of system modularization, the module complexity, and the voter complexity at the specific module level.

66.2.2 Dynamic and Hybrid Techniques

While in passive redundancy any failed modules still participate in the decision making of system's output, in active or dynamic redundancy, fault tolerance is achieved by having one main module providing the required service and a number of spares, which may be online or offline (dynamic sparing). Upon the main module failure, the first standby undertakes its duties becoming the main and so on. Failed modules no longer play any role in the system. In general, to implement this fault tolerant strategy the basic steps involve fault detection, reconfiguration, and recovery. In computing systems fault detection can be carried out, to some extent, by running diagnostics (see Figure 66.2), but the usual approach is by duplication and comparison (see Figure 66.3). Reconfiguration aims at isolating or replacing a failed unit and recovery, when needed, *i.e.*, at eliminating the effects of errors. In general, dynamic redundancy can be applied at various system levels, but one major consideration on making such a decision is

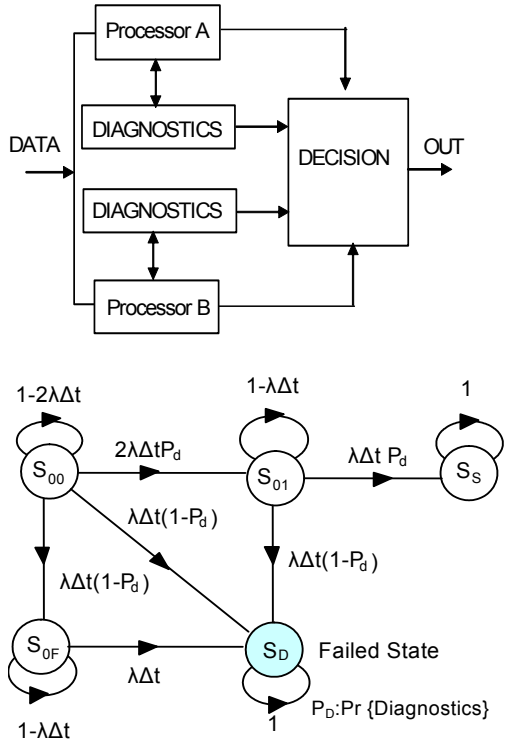


Figure 66.2. Processor duplication with independent self-diagnostics

the complexity of the fault detection and reconfiguration circuitry.

A more fault tolerant distributed approach in computing systems is to provide full reconfiguration at the processor level as well as at the memory module level (Figure 66.4); the system is configured with two CPUs, one active and one backup, and two parity based memory modules.

Each memory "write" by the active CPU is made to both memory modules and on every memory "read" the output of both memory modules is compared. If a mismatch is detected, the processor believes the memory module with the correct parity. The other memory module is marked and a fault trigger is generated. The backup processor monitors the health of the active, so that if a fault is detected in the active processor, the standby takes over both memory modules.

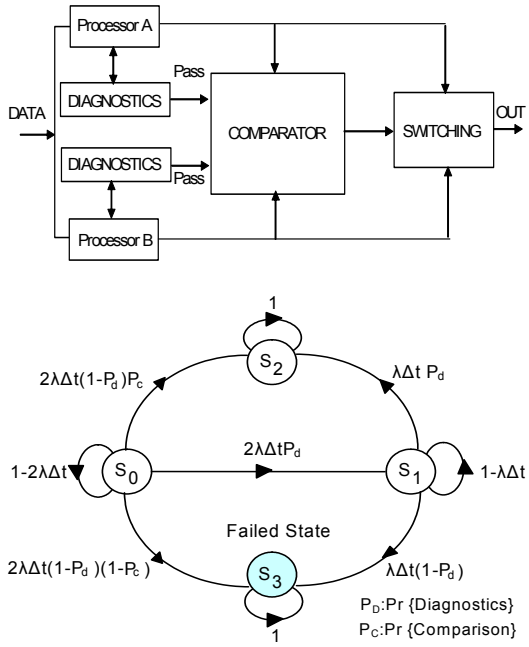


Figure 66.3. Processor duplication with self-diagnostics followed by comparison

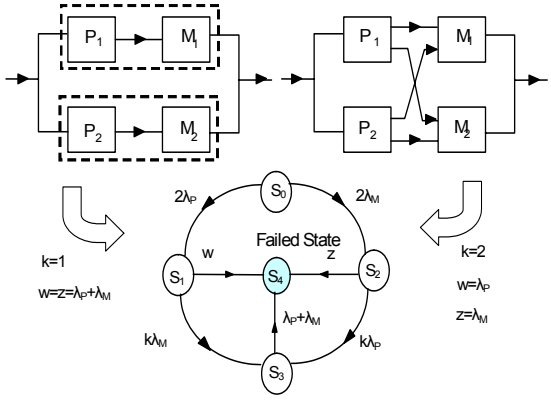


Figure 66.4. A duplex processor-memory system with reconfiguration at the memory module level

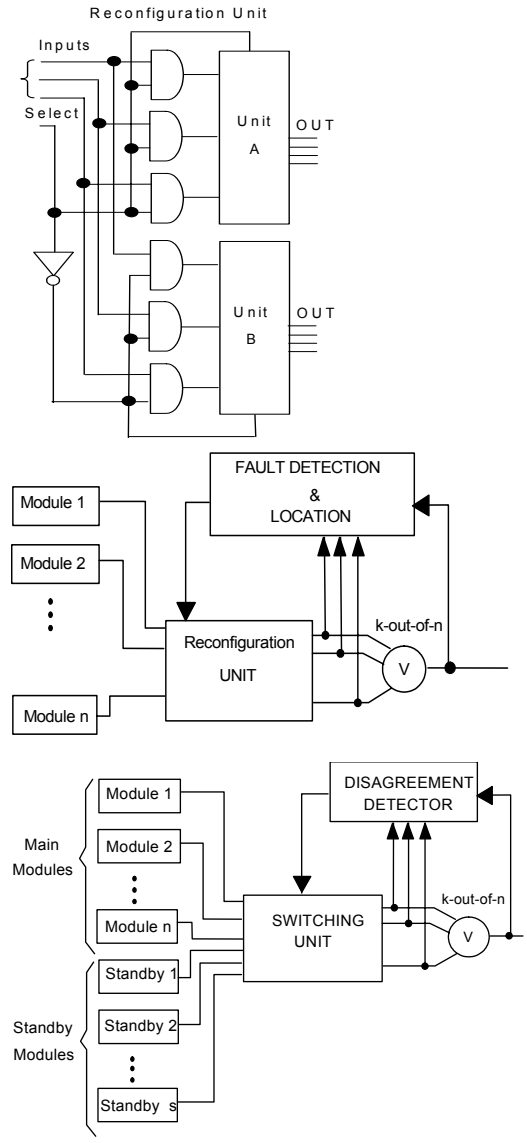


Figure 66.5. Fault tolerant implementations by hybrid redundancy

Hybrid redundancy (Figure 66.5) combines fault masking and dynamic redundancy to provide a high fault tolerant configuration, usually at much higher cost; fault masking prevents the system from delivering an incorrect service and dynamic redundancy restores its capability for fault masking by replacing any faulty units.

66.2.3 Information Redundancy

Information redundancy provides fault tolerance by replicating or coding data. Both approaches require large amounts of extra hardware resources and most often, in critical applications, a combination of both is used. Encoding/decoding [14] allows the detection or correction of information that is retrieved from storage or transmitted *via* communication links. Both processes use the rules of a code to convert data words to codewords and *vice versa*. Some examples of data coding are the parity codes, the linear codes, the cyclic codes, and the arithmetic codes. In general, three techniques are usually employed to provide error detection/ correction in memories:

Coding: Parity codes are widely used in large memory systems to provide error detection since they are fast and inexpensive. SEC-DED (single error correction/double error detection) Hamming codes, however, have become more popular because of their error correcting capabilities. Other codes have also been proposed, most of which are designed to handle specific types of multiple errors.

Replication: The use of multiple memory copies results in highly reliable systems, but significantly increases the hardware overhead. While duplication provides fast on-line error detection, triplication (with voting) provides efficient multiple error correction. This may become more popular if memory prices continue to decrease.

Re-addressing: This technique is based on permuting the memory addresses and/or data lines between the memory arrays and the CPU to eliminate errors. Spare memory units may be used to replace defective elements. Complex control circuits are usually needed to accomplish reconfiguration. Error detection and fault diagnosis circuits, to distinguish hard and soft errors, are also required. In order to eliminate soft errors some degree of redundancy must be introduced either in hardware or software or both. Some work in recent years has addressed this subject to some extent. In high-speed memories the most commonly used codes are the Hamming SEC and SEC-DED codes. In addition to SEC-DED, high data integrity implementations can also afford memory duplication, as the one shown in Figure 66.6.

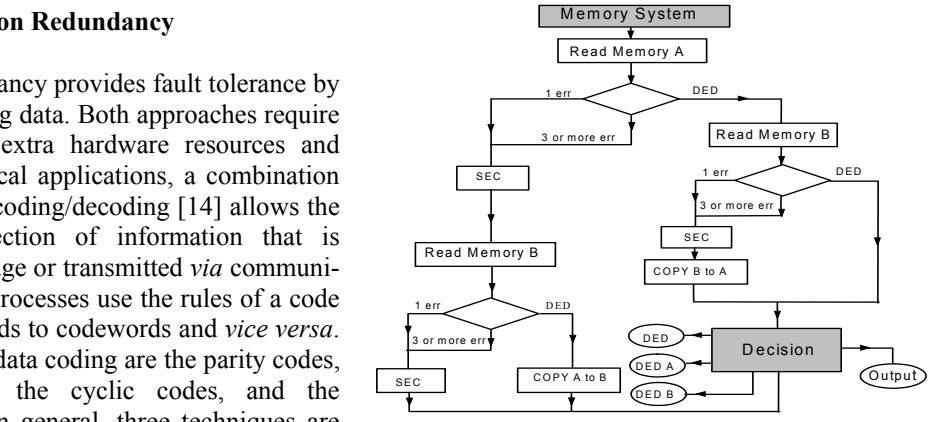


Figure 66.6. Duplex RAM with SEC-DED encoding/decoding

66.3 Software FT: Learning from Hardware

Despite the fact that most real time systems focus on hardware fault tolerance, the contribution of software errors (bugs) to system outages remains great. Software failures, as they are not due to wearing out processes but to design or data errors, are receiving increased attention [15]. Such failures occur when software is called to work in an environment for which it was not designed or tested. Software fault tolerance, as it happens in hardware, is achieved by the introduction of some kind of software redundancy. This redundancy covers errors occurring during software development, in improperly translating or implementing the algorithm into a programming language. As in hardware, software structuring is a prerequisite for effectively handling the software complexity. For instance, N-tier systems use hardware and software resources dynamically to allow each layer of a component part to be developed and managed independently. Thus, a computer application can be divided into logical layers (tiers) with embedded fault tolerance mechanisms to give the ability to recover from an error. Considerations, such as the extent of system decomposition and the layers to be diversified must be carefully examined. It can

be stated, but it is not always true, that smaller components facilitate the fault handling actions, such as confinement, and the larger components facilitate the diversity. As a single fault may affect many redundant functions or even the selection mechanism of these functions, making impossible for the system to recover, it is imperative to secure independence at all levels of software development. Currently, various fault injection techniques and tools are used to evaluate software performance, by simulating faults during the execution of the code under test.

66.3.1 Basic Issues: Diversity and Redundancy

Computer software is one example where design and specification errors are particularly relevant. Traditional fault tolerant hardware techniques, dealing mainly with permanent or transient hard failures, have inspired many existing software strategies. However, unless diversity is used, redundancy alone is not enough for tolerating software design faults [16],[17]. For a redundant configuration with two computer systems with identical software, there will not be any tolerance to single points of failure since the software will have common mode failures. Diverse software involves separate software implementations with the aim of achieving independence at the level of software faults. Assuming that this requirement is fulfilled, it will be most unlikely to have the simultaneous failure of two or more software versions for all sets of input data.

Many software faults are also data-dependent, in the sense that they will never occur unless a specific sequence of data inputs is encountered. This has led to the development of data diverse fault tolerant techniques for complementing the design diverse techniques [18]. In overall, fault tolerant software must cope with both design and data-dependent faults. Fault tolerant software implies redundant diverse software mechanisms for detecting errors and limiting their propagation. It also requires a means of rolling back the system to such a point in time before the fault was encountered and restoring all parts of the system that have been affected. As in hardware there exist numerous possibilities for the amount and level of software redundancy allocation. In hardware, redundancy is allocated at the component, subsystem and the system level. In analogy, redundancy in software is usually applied to the procedure, the process or to the complete software level. This, in the "chain of links" analogy, is a strengthening an individual link or an ensample of adjacent links or as introducing an additional chain. Deciding on the level of redundancy allocation has much to do with the difficulty of introducing redundancy at a specific level. For instance, it is much more complex to make a logic circuit fault tolerant by allocating redundancy at the gate or chip level than by replicating it. In analogy to this, one has to consider the amount of additional software complexity required by the various redundancy allocation levels.

66.3.2 Space and Time Redundancy

Unlike hardware, in order for the software to perform the required functions it must always be accompanied by hardware. Digital hardware, such as that of a computing system, is the underline framework of software and it plays a very important role in the development of fault tolerant software mechanisms. Upon program execution the computer can be instructed to hold results that are more likely to be incorrect. Assuming that the cause of the incorrect results is a transient error, it is expected that a second trial, *i.e.*, the use of time redundancy, can render the correct results. Time redundancy is fairly common in software and usually is accompanied by space redundancy, *i.e.*, diverse versions of software. Space redundancy provides separate diverse copies of software or data and time redundancy allows the recomputation by shifting the information in time.

Fault detection is a very basic consideration in providing fault tolerance. Neither space nor time redundancy can be introduced in software without having first detected that an error has occurred. Software failure is detected by watchdog and/or health messages. As a consequence, processor automatically reboots from a ROM resident image or restarts the offending tasks without needing an operating system reboot. A watchdog timer [19], implemented in hardware or software, is a widely

used means for checking proper system function. A timeout signals that some time constrain has been violated and a corrective action is required. This corrective action can take the form of retry or abort. The choice between these two depends on the criticality of the encountered function, but most often abort follows the unsuccessful repetition of retry, a number of times. Fault detection in many software techniques is accomplished by some type of an acceptance test.

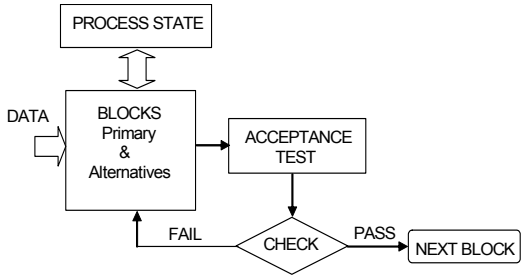


Figure 66.7. Backward error recovery

In general, software fault tolerance is based on dynamic and masking redundancy. In dynamic redundancy, several components are used, but only one is active at any time. In the case of an error, the active component is replaced by a spare component. In masking redundancy, all components are active but the effects of single or multiple errors are masked. Traditional techniques, such as the recovery block (RB) and the N-version programming (NVP), for tolerating software design faults relate to passive and active dynamic redundancy. One difference is that the first of these is usually applied at the subsystem (software module) level while the other at the software system level. In RB there exist many software implementations, each decomposed into a number of blocks. As in standby sparing, only one implementation, starting with the first block of the primary, is used at a time. This technique (Figure 66.7), uses acceptance tests and checkpointing for accomplishing backward recovery; upon the detection of a fault in a block the state of the process is restored to its previous state and an alternative is executed. Checkpointing, at the cost of system performance, can be introduced not only at the initial process state, but also in other intermediate states. Again, the implementation of RB rises the question of redundancy allocation and the extent of software modularization. One possibility for increasing the effectiveness of RB is to employ, instead of cold, "hot" alternatives, or in terms of hardware terminology, a modular hot standby system. This, in digital system terms, leads to the parallel execution of the alternative versions.

Data diversity techniques, such as retry blocks and N-copy programming, can also be used to improve the efficiency of check pointing. NVP (Figure 66.8), in analogy to static NMR redundancy in hardware, employs a number of diverse versions of software and a selection mechanism (voter). These versions are executed in parallel and the selection mechanism decides for the output. The effectiveness of NVP greatly depends on the degree of independence of the software versions. An improvement of NVP that allows voting on a subset of versions is the $t/(n-1)$-variant programming. Adaptive NVP introduces weighting factors in the versions for the purpose of adaptively influencing the voting.

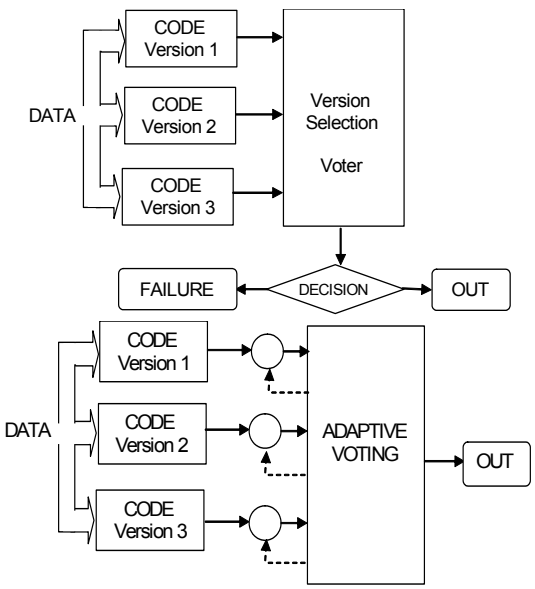


Figure 66.8. N-version programming (three levels) and adaptive NVP

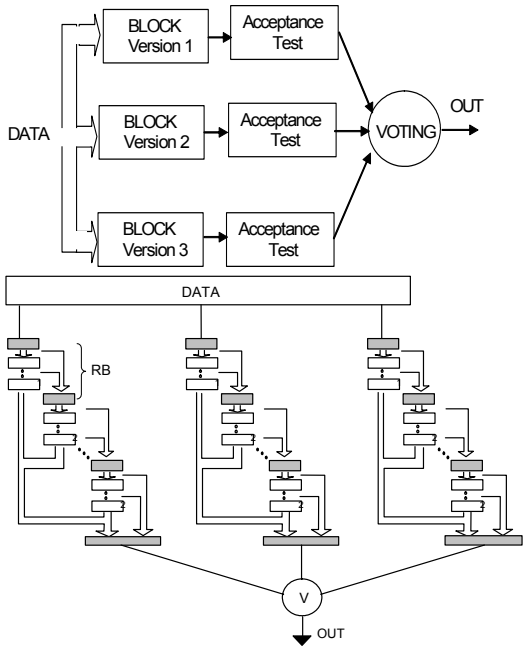


Figure 66.9. N-self-checking programming

Numerous voting techniques, such as majority voting, fuzzy voting, median and average voting, and so on, are used for selecting the correct output from the different software versions. It must be pointed out that the voter complexity may have a severe impact on performance and reliability. The combination of RB and NVP into the N-self-checking programming technique (Figure 66.9), though more complicated, provides a means for achieving fault tolerance in critical applications. A cost effective technique capable of tolerating arbitrary replica behavior is the Byzantine fault tolerance (BFT) in which replicas can be repaired periodically, on the basis of an abstract view of the states of correct replicas. Byzantine fault tolerance requires a minimum of $3f+1$ replicas to tolerate f Byzantine faults and is designed to protect against arbitrary behavior including software bugs and security violations. It can function correctly even if a number of its replicas act arbitrarily and not according to specification.

Software fault tolerance techniques based on RB and NVP are not cost effective compared to algorithmic-based techniques (ABFT) and assertion and sanity-based techniques (ASBT) [20]. In ABFT, fault tolerance is achieved by embedding tailored software for checking and possibly correcting the computations. The technique is not applicable to arbitrary programs, but it is very effective in regular data structures. Assertions provide an error detection mechanism by introducing logical statements or by specifying few sanity checks within a program. A prerequisite for its application is the specific knowledge of the algorithm and program. This technique is very simple, does not require any hardware and does not degrade performance. To deal with software "aging" a technique known as rejuvenation [21] is often used. Software rejuvenation is a proactive fault management technique aimed at cleaning up the system internal state to prevent the occurrence of more severe crash failures in the future.

66.4 Global Fault Tolerance Issues

Today, various services are developed over multiple interconnected networks with different technologies and infrastructures. The great interest in the use of the Internet platform for providing business-to-business (B2B) services, has been followed by a similar interest in the area of global computing with particular emphasis in security and fault tolerance. As local and global environment characteristics are different, there is a variety of approaches for developing fault tolerant applications [22],[23]. Generally, in such a complex multinetwork environment, there are too many opportunities for failures. Traditionally, such failures were mainly due to hardware malfunctions in a node, ranging from processor or memory failures to network interface or switch and router failures. Today, other types of possible failures/attacks exist, which could remove a large number of nodes from the system or could affect severely its performance. Also, fault tolerance becomes much more difficult in multilayered architectures where software/protocol errors and attacks can propagate from one network to another.

There are numerous failure modes in computing systems and applications, giving rise to a number of various complexity faulty models for

the assessment of their fault tolerance attributes. A fault is a deviation from the expected behavior and may be due, among other things, to hardware, software and communication errors. A fairly general classification for faults in computer networks can be based on the output or response received by a faulty node. Assuming that some output must be received, the lack of such an output may be due to a crash failure or to a communication link failure or to the combination of both. This fault may further be classified in more detail, as transient, intermittent, timing, omission and so on. Assuming, however, that upon its failure a processor continues to run exhibiting arbitrary behavior, a more serious fault condition, known as the Byzantine failure, occurs. That is, fault free computing nodes cannot detect any failed nodes.

66.4.1 Fault Tolerant Computer Networks

Many high availability implementations in the computer internetworking are based on active replication solutions. A secondary idle node (stanby) is used for the purpose of monitoring a primary node (active). It undertakes its duties in the case of primary node failure. Since standby has to take over under fault conditions, it must be synchronized with the active node. This synchronization can be achieved in various ways, each having different hardware and performance costs. For instance, in bus cycle level synchronization the active and the standby nodes are locked at processor bus cycle level. The standby watches each processor instruction that is performed by the active and it performs the same instruction in the next bus cycle in order to compare its output with that of the active unit. Clearly, this approach introduces wait states in bus cycle execution and lowers the overall performance. Active replication can also be applied for multiple backup nodes for the primary. All nodes process the same inputs generating results that are compared using a Byzantine algorithm. Nodes producing incorrect output beyond a threshold number of times, are declared as faulty and ignored. Back up servers work poorly with Byzantine faults since the backup will be receiving erroneous data without being able to recognize them as wrong.

The standby solution does not take advantage of the processing power of the standby nodes and offers no scalability. To increase reliability and performance, the process of computer clustering is widely used; this additionally allows expandability, which leads to computer power upgrade and the preservation of the existing computer system investment. While many implementations use clustering to build a more powerful virtual server, at the same time they provide a higher level of fault tolerance. Resources are shared among multiple systems by running some requests on one physical server and other requests on another server. The decision on which server handles the requests is taken by appropriate management software. In the case of a server failure, a request is rerouted to the next available server (Figure 66.10). This, in the "chain of links" analogy is as strengthening an individual link without the need of introducing additional links. In some critical cases, it may even be necessary to allow several such links to be consolidated into one. Clustering is also used in Web services to maintain continuous access and provide multiple connections. Clusters, as they have redundant nodes, can tolerate single and multiple failures and at the same time provide high performance by splitting a computational task across many different nodes. Nodes, in computer clusters are centrally managed and usually communicate through fast LANs. Memory storage is shared among all nodes. Grid clusters, are closely related to cluster computing but the workstations involved operate more like a computing utility rather than like a single computer; grids manage the allocation of jobs that are performed independently.

66.4.2 Network Protocol-based Fault Tolerance

The basic functionality of a network is to allow communication among its members by the use of certain rules, the protocols [24],[25]. In recent years, extensive studies have been carried out on unicast and multicast routing protocols. Interconnected networks are made up of numerous components such as fiber cables, interfaces, hubs, switches, routers, transceivers, and so on. The

design of network fault tolerance has to take into account many considerations, among which network performance is of paramount importance.

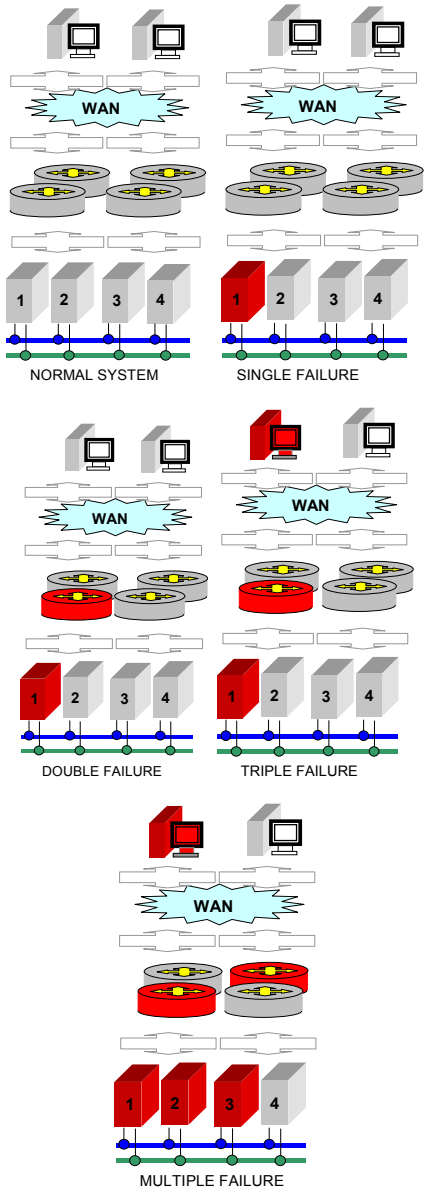


Figure 66.10. Fault tolerant system with active replication at the subsystem level

Failures in networks, usually cause the interruption of the communication within or between sub networks or lead to a degraded performance. The communication path between a client and a server contains networking devices that can be viewed as links in a chain. The longer the chain, the higher the probability of path failure. In the Internet infrastructure the weak links are single points of failure and performance bottlenecks. The latter are due to network elements that do not have enough resources to handle the amount of traffic they receive. Deciding on the network infrastructure and the amount and the level of redundancy allocation is becoming a major consideration for achieving fault tolerance. Within this context, different routing and router protocols are used.

Unicast link state routing protocols are used to calculate the best working route to destination, by acquiring knowledge on any faulty links. One example is the Spanning Tree Protocol (STP), widely used in Ethernet LANs, working in a switched/bridged environment; bridges send periodically a “hello” packet and listen from others. If a bridge has not heard any packets, and the timeout has been reached, the bridge calculates a new route. Virtual LAN's can have multiple STP processes running, providing fault tolerance to link failures and traffic load balancing. With links in their intact state, different routes can be assigned to the same destination. If one link fails, the traffic in that link is moved to some other link. The Open Shortest Path First (OSPF) protocol, very popular in Internet, provides fault tolerance in network backbone. Similarly, Cisco’s Enhanced Interior Gateway Protocol (EIGRP), determines link distances on the basis of available bandwidth, delay, load utilization, and link status. Unicast protocols can be used to implement multicast communications, but they consume much bandwidth and cause longer delays. So far many multicast communications routing protocols have been developed that are based on source tree and shared tree routing.

Data packets travel between two hosts through a number of routers, located at gateways. Their role is to find the best path to route packets. Routers, apart from dedicated hardware, contain various software components to implement a variety of functions such as, virtual private networks (VPN), routing protocols, network address translations, dynamic address

allocation and firewalls. Router protocols [26],[27] do not participate in routing but they provide fault tolerant router interface to clients by the collection of the network's topological data through the exchange of adjacent link information and the use of this information for deciding on the shortest path from source to destination or the (re)construction of its routing table. The concept of virtual routers assumes a group of routers with a virtual IP address for the group apart from the IP addresses of its group members. The highest priority member in a group is the active router, the others being acting as standby routers. Each router monitors the other router's health by transmitting "hello" packets (advertisements). Switchover is automatic and rapid and takes place upon the failure of a router, which is revealed by the absence of its packet transmissions. In the case of an active router failure the high priority standby member assumes its duties. In Cisco's Hot Standby Router Protocol (HSRP), the network load is shared among all the group routers, until a failure occurs. HSRP, supported on Ethernet, Fast Ethernet, Token Ring, FDDI, and ATM, is a solution that allows network topology changes to be transparent to the host. This is based on the exchange of multicast messages that advertise priority among similarly configured routers and typically host rerouting takes approximately 10 seconds. Similar to this is the Virtual Router Redundancy Protocol (VRRP) in which only the standby routers monitor the health of the active router. Multigroup HSRP (MHSRP) equipped with adequate hardware, allows a single router interface to participate to more than one hot standby group.

By considering the contribution of link failures to network low performance and unavailability it can be stated that this of WAN links is critical because they form the backbone network connecting diverse sites. Routers can automatically compensate for failed WAN links through routing algorithms. By supporting load balancing, duplication of a WAN link (Figure 66.11(1)) not only provides a backup link but also leads to a better performance as a result of the increased link bandwidth. Network load balancing is a different flavor of load sharing. However, other alternatives have to be considered as for example, to add a link between the front routers (Figure 66.11 (2)). This offsets the effect of a failure in any single link and improves performance due to the distributed functionality. In general, meshed networks provide alternative paths, allowing the router to compensate for link failures. Whereas, in either case, the additional link improves fault tolerance and performance this cannot be generalized. Other possibilities for improving fault tolerance at the subnetwok level are also possible. One of these is at the level of an Ethernet LAN by adding another active

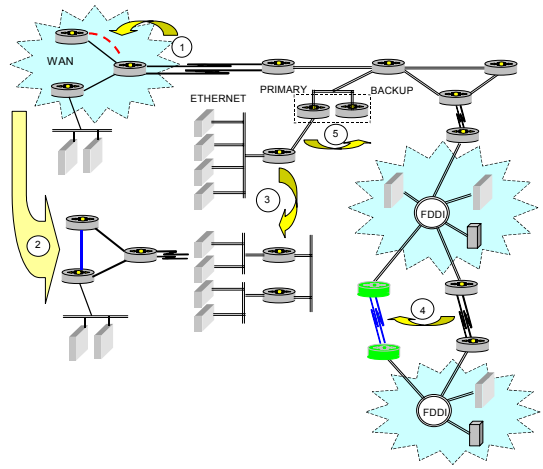


Figure 66.11. Internetworking fault tolerance

router (Figure 66.11(3)). This, doubles the cost of network connectivity for each end station, and it is only practical when full redundancy is required. Typically, when dual routers are used (Figure 66.11 (4, 5)), the backup routers are not used unless the primary router fails.

Typical fault tolerant internetworking configurations contain multiple routers connecting LANs. As mentioned above, after a link failure, routing protocols undertake the task to find new paths for maintaining network connectivity and/or an acceptable performance. However, the LANs performance characteristics are limited by the speed at which their hosts can detect a topology update. Also, routers add new vulnerable "links" in the chain of paths, which finally may cause adverse effects on performance and reliability. As fault tolerant networks are designed to perform even in the presence of failures, their performance can be evaluated by taking into account the consequences

of fault handling protocols and actions. In some cases the fault handling actions can result in a degraded performance but in others they may be inefficient for handling severe faults or too slow for meeting performance requirements. Algorithms in routing protocols have to support routes of arbitrary length, from source to destination, and to this end, they require different convergence time. IP routing protocols, as they are often based on distance vector strategies, have the drawback that often the required convergence time is too long. Overlay networks (Figure 66.12), with virtual links connecting two edge nodes of the physical network, can alleviate this problem by making many nodes that are many hops apart to appear as if they are directly connected.

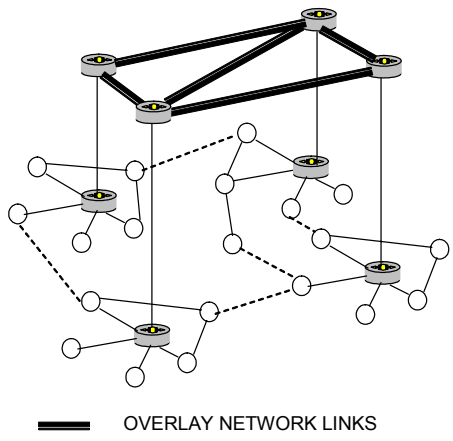


Figure 66.12. Virtual overlay network links with application level routers on top of the physical network

66.4.3 Fault Tolerance Management

There are many opportunities for hardware/software failures in a network node, starting from the failure of a simple network interface up to the failure of a processor or the hang of software. Fault tolerance problems arise because application components may eventually fail due to hardware failures, operator mistakes or design faults. Traditionally, fault tolerance was introduced by adding extra hardware resources. The most common means of providing fault tolerance is by passive and active replication. Hardware fault tolerance includes redundant communications, replicated processors, additional memory, and redundant power supplies. The hang of software can result from a bug in the application running at the node or even a hardware fault. The usual approach for handling application failures is to periodically checkpoint the computational state of the application so that it can be restored in the event of a system failure. In many situations, common cause failures can remove a large number of nodes causing the applications running on the affected nodes to crash or produce incorrect results. By managing the hardware resources, the computer increases its ability to continue its operation. High availability computing cluster implementations attempt to manage the redundancy inherent in a cluster, by eliminating single points of failure. Clustering also provides load balancing by distributing the load to a number of identical back end servers, so that the overall throughput is multiplied. To fail over, the healthy nodes take over the traffic from any failed node without interrupting the traffic flow. The management of the available resources in the cluster's nodes is a critical responsibility and is carried out in the centralized management nodes. Centralized management nodes handle all node monitoring responsibilities and job allocation by identifying faults and initiating the necessary fault handing actions, depending on the cluster configuration.

A computer cluster can be configured to be symmetrical or asymmetrical, on the basis of the roles of the individual servers. In the symmetrical type, as in the three-server cluster of Figure 66.13, all servers have the same role and the only difference is in the sequence with which each server undertakes the role of another. That is, in the case of the active server failure, the first backup server undertakes its duties and in the case of a backup server failure the next priority backup assumes its duties. Such clusters are not used in critical applications and, therefore, no real time synchronization among their members is required. In the asymmetrical cluster type, all servers are active and their roles are different. In order for a server to be able to undertake the role of another server, full synchronization is required. Such clusters have a common memory, accessed from all

active servers, so that the memory content of each server is synchronized with that in the common memory. Node management tools facilitate the processes of role allocation to the servers and distinguish on a logical layer the role of each server in a cluster. These roles can change automatically according to the system requirements and the predefined processes:

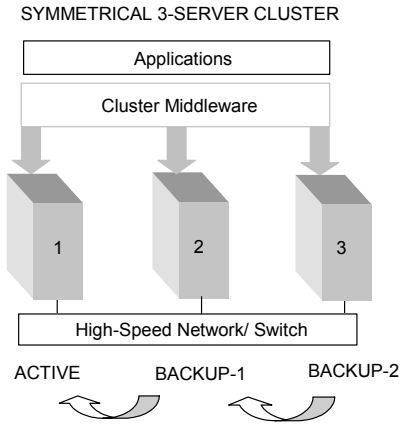


Figure 66.13. Symmetrical three-server cluster

Normal: A normal server can support an active application and also act as "live" for another application. In a data base management system, a normal server can manage actively the database of a particular service and can also have the role of "live" for other services. Short "alive" messages monitor its health by other servers.

Live: A live server is in a state to undertake the duties of the normal server, as soon as a problem with the normal server is revealed. It can also act as the normal server in another application. Within its duties are the synchronization with the normal server, the monitoring of the health of the normal server, the changeover to normal, and the reporting to other nodes about its new role.

Stand-by: A stand-by server is synchronized with the live server and monitors its health. It can also act as backup for another application. Among its duties is the synchronization with the backup so that the backup can undertake its duties. In this case it reports to all other nodes about its new duties.

Backup: A backup server for an application can replace a stand-by server and can also act as stand-by for another application. In the case of its promotion to standby, it reports about its new role to all other nodes.

Many present day powerful servers have many processors supporting micropartitioning and dynamic logical partitioning with complete independence among partitions. By proper monitoring, a faulty processor is automatically disabled and replaced with the backup without any interruption of the system operation (Figure 66.14).

Managing the fault tolerance in distributed computing systems [28] is a major issue, presenting a challenge to system designers. A

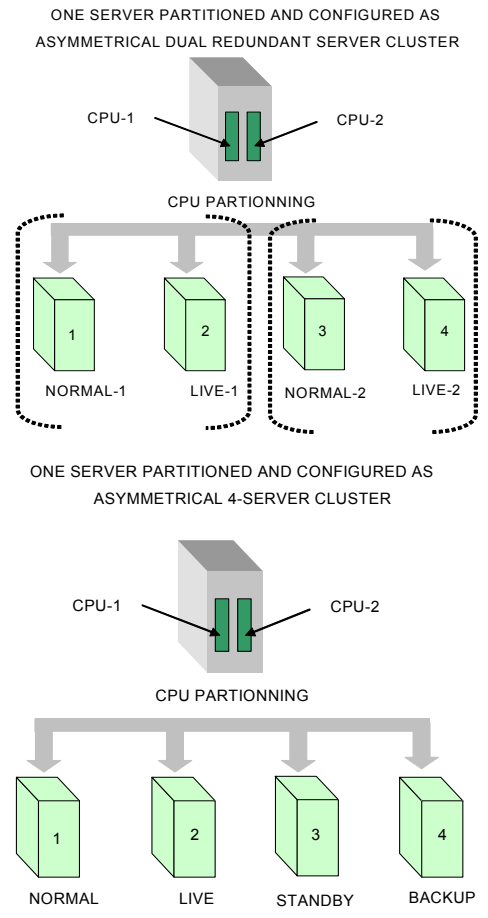


Figure 66.14. Multiprocessor server partitioned and configured as a dual redundant server and as an asymmetrical four-server cluster

failure of a component in the system may result from a fault in the component itself or from the propagation of a fault in another part in the system. Thus, failures in the system depend on the global execution state of the system, *i.e.*, the combined states of all the components in the system. A fault tolerant distributed system employs a distributed collection of processes such that a corruption of one process is not affecting the functionality of the whole system. In distributed systems fault tolerance is also achieved by replicating critical components. Replicas handle faults as well as the system workload. While in a local system synchronization is not a problem, a distributed system comprises a set of autonomous machines (see Figure 66.15), each with its own clock. Computing nodes exchange messages *via* communication links. The synchronization primitives, which are easily implemented in a local system, are much more complicated. Algorithms for asynchronous systems are prone to malfunction if the imposed timing bounds, on message transmission and response times, are violated. In a local system, a critical region is used to control access to a shared resource, so that only one thread can access that resource concurrently.

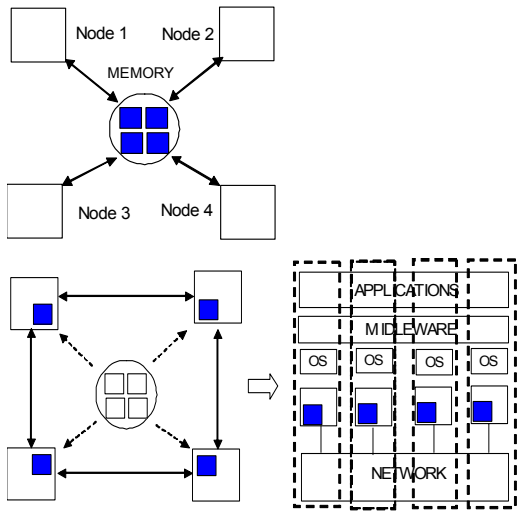


Figure 66.15. Migration of shared memory: local system *vs*. distributed system

Implementing a distributed system requires that all nodes need to have consensus on their exact state and make collective decisions without conflicts. As long as the state between the nodes is consistent, the system can successfully handle a failure. Each node can establish a checkpoint, but it is not possible to establish a checkpoint of all the nodes simultaneously. Thus, synchronization between group members is essential in order to detect a faulty process and to reach a consistent state. In distributed checkpointing [29] all processes cooperate to establish their local checkpoints, so that their ensemble represents a consistent global state. A lack of synchronization can lead to an uncontrolled rollback to the state at the start of execution, known as domino effect. Consistency is often achieved by group membership negotiated protocols, which ensure that all nodes share a common view of the system configuration. Achieving agreement on group membership is an essential prerequisite for reliable group communication. Despite the numerous algorithms and techniques developed to confront failures, the area of fault tolerant distributed computing presents many challenging problems. Byzantine fault tolerance has recently been shown to be practical for the development of certain classes of client-server, distributed applications; however, more research is needed for incorporating it into multitier distributed applications. Centralized applications are generally perceived to be more reliable than distributed applications.

Most real time systems comprise software running in parallel across multiple processors, implying that data is also distributed. Due to a number of reasons, such as software bugs and processor reboot, data may become inconsistent. The RAID technology improves performance and provides a fault tolerant solution of storing data by the use of two or more disks. This solution is based on redundancy management of disk space and can be implemented by hardware or software. The hardware solution has advantages over the software as it does not occupy host's system memory, it is not dependent on server CPU performance and load, and it does not consume CPU cycles. Also, hardware arrays have more fault tolerance, as they are not dependent on software that can potentially be unavailable due to a faulty disk. RAID systems appear as one drive and can be configured in

different ways each with different performance and fault tolerant attributes. Disk mirroring, used in RAID level 1 (Figure 66.16), writes simultaneously all data to two hard disks, in order to provide protection against the failure of either of the disks. In the event of a drive failure, a copy of the data is taken from the other. The controller must be able to perform two concurrent separate reads *per* mirrored pair.

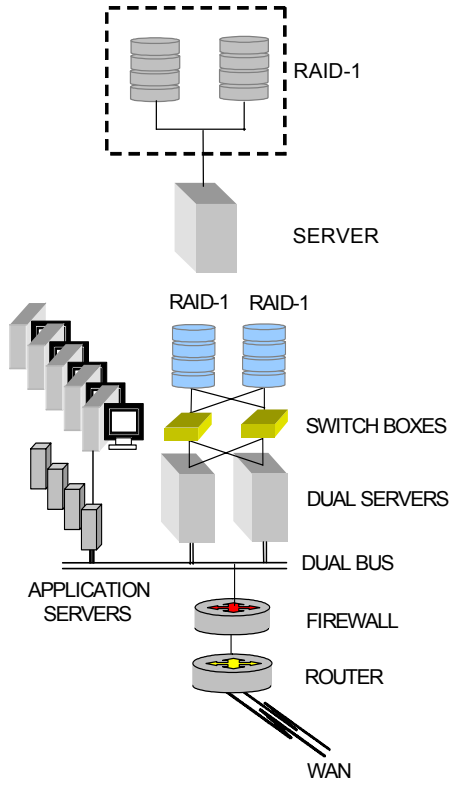


Figure 66.16. Server and fault tolerant dual central system supported with RAID-1

Disk duplexing improves fault tolerance, by the use of more than one controller to control the mirrored hard drives. To maximize throughput of the storage system the I/O load is balanced across all drives, so that drives can be, as much as possible, equally busy. A very good load balancing is achieved by striping, *i.e.*, by partitioning the disk space into stripes that are written alternatively into different disks. Stripes can be as small as one sector and as large as several megabytes; to optimize performance the size of stripes should be large enough to accommodate the size of records. In such a case, I/O operations can be performed on different drives and the data will be evenly distributed.

In RAID-2 all stripes are stored in different disk drives with each data word having its ECC word (Hamming) on separate disks. On read operation, the ECC code can correct "on the fly" single bit errors. RAID-3, 4, and 5 employ disk stripping with EEC parity information stored on one or more drives. RAID 0+1 (or RAID 10), implemented as a striped array whose segments are RAID-1 arrays, has the same fault tolerance as RAID-1 and it is recommended for its high performance and fault tolerance.

66.5 Performance Evaluation: A RAM Case Study

In recent years, there has been a noticeable activity in relation to performability and performance analyses in specific applications [30]–[32]. These applications mainly refer to the computer-based technology such as microprocessors, random access memories, multiprocessor systems, and mass storage systems. Evaluating or predicting performance overheads due to the fault tolerance mechanisms is not an easy task, particularly if performance in the presence of faults is degradable.

Assessing the performance of fault tolerance mechanisms can be accomplished by developing system models that adequately describe their complete fault handling functionality and by fault injection. System modeling relies on the development of a formal mathematical representation of the complete system and its functionality. Fault injection is used for fault removal during the system building and aims to remove design and implementation deficiencies, and fault forecasting, after the system's complete implementation, to assess the performance of the system's fault tolerant mechanism. Figure 66.17 shows the hardware architecture and modeling of a duplex RAM memory system with SEC and memory scrubbing for eliminating soft errors [33]. Soft errors are due

to external events, such as noise and alpha particles that do not cause permanent memory damage, but may cause incorrect data or code execution. Scrubbing [34],[35] offers an effective method to recover from soft errors, by reading and rewriting the memory content at regular time intervals. In general MTTF is accepted as an appropriate metric for system reliability. The proper selection of the scrubbing interval T_S has a key role in achieving an acceptable MTTF (see Figure 66.18).

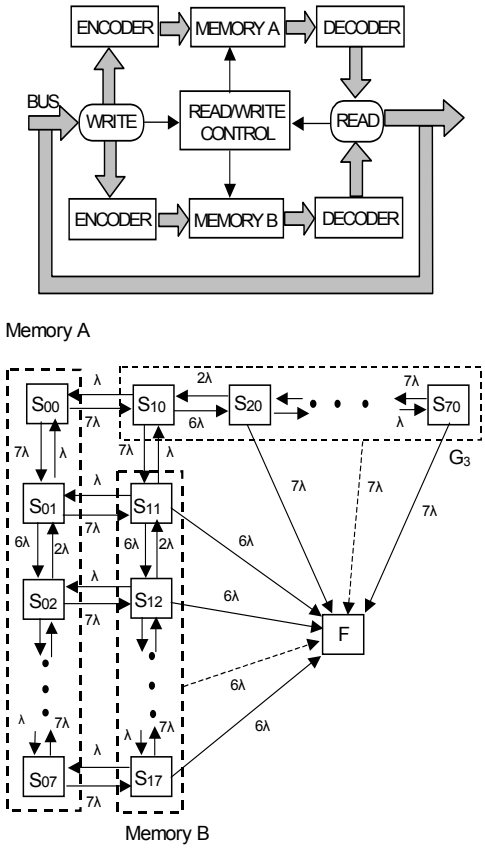


Figure 66.17. Duplex memory system modeling with SEC and memory scrubbing

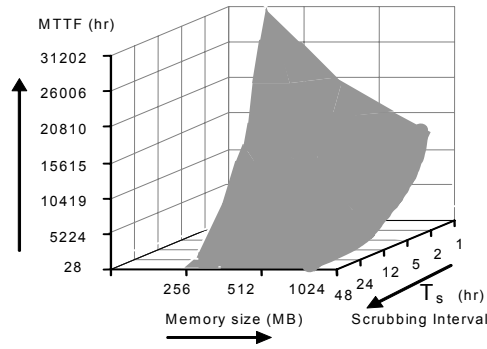


Figure 66.18. Performance of a duplex memory system with SEC and memory scrubbing

In a large memory system an enormous number of complex fault patterns can developed during normal system operation, making the performance analysis very time consuming. A performance assessment of the general architecture of SEC-DED self testing and repairing (STAR)-RAM [36]–[38] (Figure 66.19) is facilitated using the state-merging and assorted random testing (SMART) approach [36], which is a Monte Carlo-based simulation that deals with groups of elements involving huge number of components. The system is modeled in terms of a collection of group state vectors, where each group vector represents a series of group states in the presence of consecutive fault hits, and contains one or more dummy states to trap a group and/or system failure

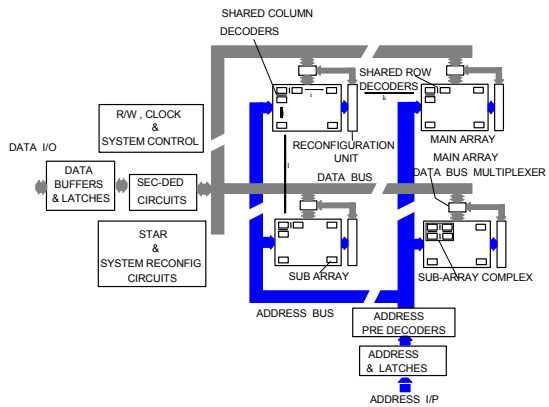


Figure 66.19. Architecture of STAR-RAM

state. A single group vector is generated for one of all identical system groups and is then linked to all these groups resulting in a substantial reduction in the total number of generated system vectors. A random fault pattern is then generated in each experiment and is mapped to the currently simulated group vector. The vector is examined to determine the group condition and its impact on the subsequent system state to decide whether it is correctable or not.

The discrimination between soft and hard faults is based on the fact that memory locations containing hardware faults cannot correctly store the applied test patterns, in opposition to those locations containing soft faults. Upon error detection during a normal memory read cycle, BIST circuits are triggered for repairing the currently accessed memory location. The algorithm first copies the contents of the tested location to the scratch memory so that data can later be restored, it then applies four subsequent test patterns with interchanged adjacent bit values for detecting all cell stuck-at faults and word single coupling faults. Finally, the repair of hard-failed locations is carried out. When a memory byte is verified to have a hard fault, the first available spare is assigned the address of this byte. Any attempt to access this location is then sent to the allocated spare by redirecting the memory data-bus. If, however, the fault is determined to be a soft error, the data is corrected, rewritten to the suspected location, and is sent to the host. This prevents the build up of soft errors in the memory, providing highest data reliability and error free operation of the system. The STAR engine can be configured so that BIST is triggered upon either single or double error detection. Single error triggering offers better data reliability by preventing accumulation of soft and hard errors, but it results in a degraded performance (slower memory access) because each time an error is detected a full test cycle is executed. In contrast, double error BIST triggering yields faster access when single errors are detected but reduces data reliability as double errors cannot be recovered. In both cases however, the memory system hardware reliability is not affected.

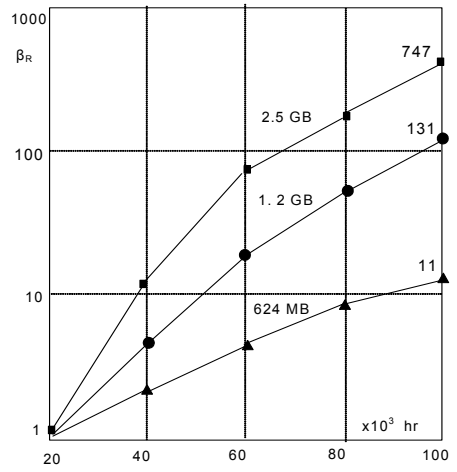


Figure 66.20. STAR-RAM performance enhancement

Based on the approximate device count of SEC-DED RAM, the additional hardware overhead required by the STAR circuits is less than 1% of the total chip area. This is due to the very small number of spares in the main array reconfiguration unit required to yield a high level of memory reliability. In comparison with conventional memory systems without error detection/ correction, the SEC-DED memory introduces hardware overhead in the range 10–40% of the total chip area. Compared to the simple SEC-DED system, the STAR memory system performance is affected by the frequency of error occurrence and on the error weight triggering of the BIST circuits. Performance, as assessed by the reliability enhancement factor β_R, (ratio of reliabilities of the STAR over the non-STAR system), for up to 100000 hours of operation, is shown in Figure 66.20.

66.6 Conclusions and Future Trends

Fault tolerance has matured into a very broad discipline encompassing many aspects of hardware and software system design. Recent rapid changes in computer architectures, with increased integration in VLSI devices, new parallel processing capabilities, and widely distributed networks have been accompanied by further advances in fault tolerant design. The development

of submicron fabrication technologies, with ever-smaller devices, promises further improvements in the performance of VLSI circuits, yet it also leads to several new technical challenges, due to increased design complexity. The declining device dimensions and voltages have caused an increased rate of soft errors due to noise and alpha particle radiation. The usual approach for developing fault tolerant architectures, which include both defects in the chip and soft errors during operation, is to provide spatial and temporal redundancy. As new technologies are developed and new applications arise, new fault tolerance approaches are also needed. In this regard, mention is made of the widespread use of field programmable gate array (FPGA) technology that has caused the migration of many software-based applications to hardware. However, as this technology proliferates in high performance systems the impact of path delay faults becomes more pronounced.

In software, many techniques have been developed for implementing fault tolerance. A lot of these are variations of old traditional techniques or have a philosophy that originates from hardware-based techniques. Software systems are characterized by a very large number of states without the regularity that would allow their merging into a relatively small number of equivalent state groups. Therefore, software correctness can only be verified to some extent, thus, leaving the possibility for the manifestation of any design faults. More research is needed on developing methods capable of handling the present day computational complexity with sufficient verification and coverage. Yet, newer reported techniques have to prove their effectiveness in real systems and applications. Currently, a broad based comparison of the performance of newer methods does not exist.

Computer clusters, massively parallel architectures, and other large-scale distributed systems with complex interconnection networks present new challenges in system control performance and fault tolerance. Despite the flexibility in system composition provided by such systems, improving fault tolerance of services collaborating in multiple application scenarios remains a challenging task. Although today's architectures are usually robust enough to survive node failures without suffering complete system failure, many high performance computing applications have to restart from the beginning whenever a node fails. The large number of computing nodes incorporated within a cluster dramatically increases the likelihood of node failures during program executions. Therefore, ongoing research focuses on graceful degradation and the continuation of program execution despite individual node failures.

The growing need for networked environments is posing new challenges to the fault tolerant design. Much research remains to be done to face network reliability in today's complex networking environment. As new technologies are developed and new applications arise, new fault tolerance approaches are also needed. In a multitechnology multinetwork environment, in each of the networking layers, different types of failures/attacks and responses are possible. Further research is needed to exploit the impact of the failure propagation from one network to another as layer restoration processes may affect each other. Also, the efficiency and performance of the network management coordination, at each of the interacting layers, needs to be addressed. Network architecture and management should be also revisited to examine optimal network reconfiguration after an attack. Software protocols, operations errors, and software attacks define a broad area where more sophisticated mechanisms and algorithms are needed for providing high fault tolerant services and avoid bottlenecks and congestion. Research on intrusion detection mechanisms has to demonstrate how severely the network's performance can be affected if protocol failure or a software attack occurs.

Both hardware and software systems have seen a large increase in their complexity. Concerns for reliability grow in many technological areas, including space reconfigurable VLSI technology, cluster based FPGA architectures and computing platforms with numerous processors. As the requirement for high performability is a major factor, driving the interest in fault tolerance, it is expected that the movement in the research and application fields toward more sophisticated error handling mechanisms and algorithms will be more pronounced.

References

[1] Avizienis A. Fault-tolerance: The survival attribute of digital systems. Proceedings IEEE 1978; 66:1109–1125.

[2] Siewiorek DP. Architecture of fault-tolerant computers. IEEE Computer 1984;17(8):9–18.

[3] Tanenbaum AS. Distributed operating systems. Prentice-Hall, Englewood Cliffs, NJ, 1996.

[4] Pham H. Software reliability. Springer, Berlin, 2000.

[5] Kontoleon JM. On the reliability modeling of RAM/ROM fault-tolerant memories. Microelectronics and Reliability 1992; 32(9):1231–1236.

[6] Ciciani B. Fault-tolerance considerations for redundant binary-tree dynamic random access memory (RAM) chips. IEEE Transactions on Reliability 1992; 41(1):139–148.

[7] Banatre A. *et al.,* An architecture for tolerating processor failures in shared-memory multiprocessors. IEEE Transactions on Computers 1996; 45(10):1101–1115.

[8] Tanenbaum AS. Computer networks. Prentice-Hall, Englewood Cliffs, NJ, 2003.

[9] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems 2002; 20(4):398–461.

[10] Lynch N. Distributed algorithms. Morgan Kaufmann Publishers, San Francisco, CA, 1996.

[11] Gartner FC. Fundamentals of fault-tolerant distributed computing in asynchronous environments. ACM Computing Surveys 1999; 31(1): 1–26.

[12] Laprie J-C, Arlat J, Beounes C, Kanoun K. Definition and analysis of hardware- and software-fault-tolerance architectures. IEEE Computer 1990; 23(7):39–51.

[13] Siewiorek DP, Swarz RS. The theory and practice of reliable system design. Digital Press, Bethlehem, PA, 1982.

[14] Rao TRN, Fujiwara E. Error control coding for computer systems. Prentice Hall, Englewood Cliffs, NJ, 1989.

[15] Hudak J. *et al.,* Evaluation and comparison of fault-tolerant software techniques. IEEE Transactions on Reliability 1993; 42(2):190–204.

[16] Lyu MR. Editor in Chief, Handbook of software reliability engineering. IEEE Computer Society Press, McGraw-Hill, New York, 1996.

[17] Randell B. System structure for software fault tolerance. IEEE Transactions on Software Engineering 1975; 1(2): 220–232.

[18] Ammann PE, Knight JC. Data diversity: An approach to software fault tolerance. IEEE Transactions on Computers 1988; 37(4):418–426.

[19] Mahmood A, McCluskey EJ. Concurrent error detection using watchdog processors – A survey. IEEE Transactions on Computers 1988; 37(2):160–174.

[20] Castro M, Rodrigues M, Liskov B. Using abstraction to improve fault-tolerance. ACM Transactions on Computer Systems 2003;12(3):136–179.

[21] Yurcik W, Doss D. Achieving fault-tolerant software with rejuvenation and reconfiguration. IEEE Software 2001; July/August:48–52.

[22] Donatiello L, Grassi V. On evaluating the cumulative performance distribution of fault-tolerant computer systems. IEEE Transactions on Computers 1991; 40(11):1301–1307.

[23] Tennenhouse JM, *et al.,* A survey of active network research. IEEE Communication Magazine 1997; 35(1):80–86.

[24] Savage S, *et al.,* Detour: A case of informed internet routing and transport. IEEE Micro 1999; 19(1):50–59.

[25] Pattipati KR, Li Y, Blom HAP. A unified framework for the performability evaluation of fault-tolerant computer systems. IEEE Transactions on Computers 1993; 42(3):312–326.

[26] Weijia J, *et al.,* An efficient fault-tolerant multicast routing protocol with core-based tree techniques. IEEE Transactions on Parallel Distributed Systems 1999; 10(10):984–1000.

[27] Elnozahy EN, *et al.,* A survey of rollback-recovery protocols in message-passing systems. ACM Computing Surveys 2002; 34(3): 375–408.

[28] Kaashoek MF, *et al.,* FLIP: an interconnected protocol for supporting distributed systems. ACM Transactions on Computer Systems 1993; 11(1):77–106.

[29] Plank JS, Thomason MG. Processor allocation and checkpoint interval selection in cluster computing systems. Journal of Parallel Distributed Computers 2001; 61(11):1570–1590.

[30] Kontoleon JM, Stergiou A. Reliability analysis of a fault-tolerant random access memory system. Microelectronics and Reliability 1991; 31(6):1063–1067.

[31] Mehdi KA, Kontoleon JM. Design and analysis of a fault-tolerant reconfigurable random access memory chip. Microelectronics and Reliability 1994; 34(2):297–315.

[32] Shyue-Kung L, Chih-Hsien H. Fault-tolerance techniques for high capacity RAM. IEEE Transactions on Reliability 2006; 55(2):293–306.
[33] Baumann RC. Soft errors in advanced semiconductor devices – Part I: The three radiation sources. IEEE Transactions on Device and Materials Reliability 2001; 1(1):17–22.
[34] Saleh AM, Serrano JJ, Lanak H, Patel LH. Reliability analysis of scrubbing recovery-techniques for memory systems. IEEE Transactions on Reliability 1990; 39(1): 114–122.
[35] Kontoleon JM, Andrianakis J. Reliability analysis of simplex and duplex memory systems with SEC and soft-error scrubbing recovery. International Journal of Quality and Reliability Management 2000; 17(7):594–596.
[36] Mehdi KA, Kontoleon JM. A rapid SMART approach for the reliability and failure mode analysis of memories and large systems. Microelectronics and Reliability 1996; 36(10):1547–1556.
[37] Mehdi KA, Kontoleon JM. Design and analysis of a self-testing-and-repairing random access memory STAR-RAM with error correction. Microelectronics and Reliability. 1998; 38(4):605–617.
[38] Kontoleon JM, Mehdi KA. A distributed-bit SEC-DED RAM with a self-testing and repairing engine. International Journal of Performability Engineering 2005; 1(1):79–98.

67

Prognostics and Health Monitoring of Electronics

Nikhil Vichare, Brian Tuchband, and Michael Pecht

Center for Advanced Life Cycle Engineering (CALCE), University of Maryland, College Park, USA

Abstract: This chapter provides a basic understanding of prognostics and health monitoring of products and systems, and the techniques being developed at CALCE to enable prognostics for electronic systems.

67.1 Introduction

As a result of intense global competition, companies are considering novel approaches to enhance the operational efficiency of their products. For many products and systems, especially those with long life-cycle reliability requirements, high in-service reliability can be a means to ensure customer satisfaction. In addition, competitive market requirements, as well as demands for increased warranties and the severe liability of product failures, have forced manufacturers to improve the reliability of their products. Higher field reliability and operational availability[1] requires knowledge of in-service use and life-cycle operational and environmental conditions.

In particular, many data collection and reliability prediction schemes are designed before in-service operational and environmental aspects of the system are entirely understood. As a result, outputs from these schemes may not satisfy all the user requirements. In addition, with reductions in product development cycle times, there is limited time to carry out extensive reliability trials.

Interest has been growing in monitoring the ongoing health of products and systems in order to predict failures and provide warnings in advance of catastrophic failure. Here, relative health is defined as the extent of degradation or deviation from an expected normal condition. Prognostic is the prediction of the future state of health based on current and historical health conditions [1].

While the application of health monitoring is well established for the assessment of mechanical systems, this is not the case for electronic systems. However, electronics are integral to the functionality of most systems today, and their reliability is often critical for system reliability [2]. This chapter provides a basic understanding of prognostics and health monitoring of products and systems and the techniques being developed to enable prognostics for electronic systems.

[1] Operational Availability: The degree (expressed as a decimal between 0 and 1, or the percentage equivalent) to which a piece of equipment or system can be expected to work properly when required. Operational availability is often calculated by dividing uptime by the sum of uptime and downtime

67.2 Reliability and Prognostics

Reliability is the ability of a product or system to perform as intended (*i.e.*, without failure and within specified performance limits) for a specified time, in its life-cycle environment. Commonly used electronics reliability prediction methods generally do not accurately account for the life-cycle environment of electronic equipment. This arises from fundamental flaws in the reliability assessment methodologies used [3], and uncertainties about the product life-cycle loads [4]. In fact, traditional reliability prediction methods based on the use of handbooks have been shown to be misleading and to provide erroneous life predictions [3], a fact that led the U.S. military to abandon their electronics reliability prediction methods [4]. Although the use of stress and damage models permits a more accurate account of the physics-of-failure [5], their application to long-term reliability predictions based on extrapolated short-term life testing data or field data is typically constrained by insufficient knowledge of the actual operating and environmental application conditions of the product.

Prognostics and health monitoring (PHM) techniques combine sensing, recording, and interpretation of environmental, operational, and performance-related parameters indicative of a system's health. Product health monitoring can be implemented through the use of various techniques to sense and interpret the parameters indicative of (i) performance degradation, such as deviation of operating parameters from their expected values; (ii) physical or electrical degradation, such as material cracking, corrosion, interfacial delamination, or increases in electrical resistance or threshold voltage; or (iii) changes in a life-cycle environment, such as usage duration and frequency, ambient temperature and humidity, vibration, and shock. Based on the product's health, determined by its monitored life-cycle conditions, maintenance procedures can be developed. Health monitoring therefore permits new products to be concurrently designed for a life-cycle environment known through monitoring [1].

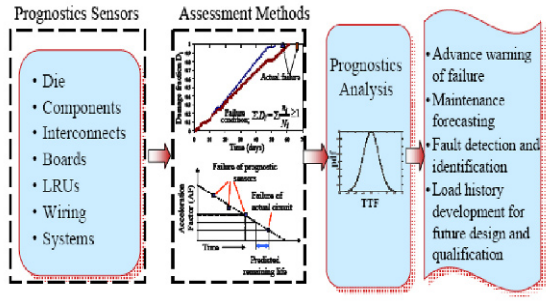


Figure 67.1. Framework for prognostics and health monitoring

The framework for prognostics is shown in Figure 67.1. Sensor data from various levels of an electronic product or system will be monitored *in situ* and analyzed using prognostic algorithms. Different implementation approaches can be adopted individually or in combination. These approaches will be discussed in detail in the next section. Ultimately, the objective is to predict the advent of failure in terms of a distribution of remaining life, level of degradation, or probability of mission survival.

67.3 PHM for Electronics

PHM has emerged as one of the key enablers for achieving efficient system-level maintenance and lowering life-cycle costs. In November 2002, the U.S. Deputy under Secretary of Defense for Logistics and Materiel Readiness released a policy called condition-based maintenance plus (CBM+) [6].

CBM+ represents an effort to shift unscheduled corrective equipment maintenance of new and legacy systems to preventive and predictive approaches that schedule maintenance based upon the evidence of need. The importance of PHM implementation was explicitly stated in the DoD 5000.2 policy document on defense acquisition [7], which states that "program managers shall optimize operational readiness through affordable, integrated, embedded diagnostics and prognostics, and embedded training and testing, serialized item management, automatic identification technology (AIT), and iterative technology refreshment." Thus, PHM has become a requirement for any

system sold to the DoD. A 2005 survey of eleven CBM programs highlighted "electronics prognostics" as one of the most needed maintenance-related features or applications, without regard for cost [8], a view also shared by the avionics industry [9].

Safety-critical mechanical systems and structures, such as propulsion engines, aircraft structures, bridges, buildings, roads, pressure vessels, rotary equipment, and gears, have been known to benefit from advanced sensor systems and models, developed specifically for *in situ* fault diagnosis and prognosis (often called health and usage monitoring or condition monitoring) [10]–[14]. Thus, for mechanical systems, there is a considerable body of knowledge on health monitoring.

Today, most products and systems contain significant electronics content to provide needed functionality and performance. However, the application of PHM concepts to electronics is rare. If one can assess the extent of deviation or degradation from an expected normal operating condition for electronics, this information can be used to meet several powerful goals, which include (1) advanced warning of failures; (2) minimizing unscheduled maintenance, extending maintenance cycles, and maintaining effectiveness through timely repair actions; (3) reducing the life-cycle cost of equipment by decreasing inspection costs, downtime, and inventory; and (4) improving qualification and assisting in the design and logistical support of fielded and future systems. In other words, since electronics are playing an increasingly large role in providing operational capabilities for today's systems, prognostic techniques have become highly desirable.

67.4 PHM Concepts and Methods

The first efforts in diagnostic health monitoring of electronics involved the use of built-in test (BIT), defined as an on-board hardware-software diagnostic means to identify and locate faults. A BIT can consist of error detection and correction circuits, totally self-checking circuits, and self-verification circuits [1].

Two types of BIT concepts are employed in electronic systems: interruptive BIT (I-BIT) and continuous BIT (C-BIT). The concept behind I-BIT is that normal equipment operation is suspended during BIT operation. The concept behind C-BIT is that equipment is monitored continuously and automatically without affecting normal operation. BIT concepts are still being developed to reduce the occurrence of spurious failure indications.

Several studies [15],[16] conducted on the use of BIT for fault identification and diagnostics showed that BIT can be prone to false alarms and can result in unnecessary costly replacement, re-qualification, delayed shipping, and loss of system availability. However, there is also reason to believe that many of the failures were "real" but intermittent in nature [17]. The persistence of such issues over the years is perhaps because the use of BIT has been restricted to low-volume systems. Thus, BIT has generally not been designed to provide prognostics or remaining useful life due to accumulated damage or progression of faults. Rather, it has served primarily as a diagnostic tool.

The different approaches to prognostics and the state of research in electronics PHM are presented here. Three current approaches include (1) the use of fuses and canary devices; (2) monitoring and reasoning of failure precursors; and (3) monitoring environmental and usage loads for damage modeling.

67.4.1 Fuses and Canaries

Expendable devices, such as fuses and canaries, have been a traditional method of protection for structures and electrical power systems. Fuses and circuit breakers are examples of elements used in electronic products to sense excessive current drain and to disconnect power from the concerned part. Fuses within circuits safeguard parts against voltage transients or excessive power dissipation, and protect power supplies from shorted parts. For example, thermostats can be used to sense critical temperature limiting conditions, and to shut down the product, or a part of the system, until the temperature returns to normal. In some products, self-checking circuitry can also be incorporated to

sense abnormal conditions and to make adjustments to restore normal conditions, or to activate switching means to compensate for the malfunction [18].

The word "canary" is derived from one of coal mining's earliest systems for warning of the presence of hazardous gas using the canary bird. Because the canary is more sensitive to hazardous gases than humans, the death or sickening of the canary was an indication to the miners to get out of the shaft. The canary thus provided an effective early warning of catastrophic failure that was easy to interpret. The same approach has been employed in prognostic health monitoring. Canary devices mounted on the actual product can also be used to provide advance warning of failure due to specific wearout failure mechanisms. Mishra *et al*. [19] studied the applicability of semiconductor-level health monitors by using pre-calibrated cells (circuits) located on the same chip with the actual circuitry. The prognostics cell approach, known as Sentinel Semiconductor™ technology, has been commercialized by Ridgetop Group to provide an early warning sentinel for upcoming device failures [20]. The prognostic cells are available for 0.35, 0.25, and 0.18 micron CMOS processes; the power consumption is approximately 600 microwatts. The cell size is typically 800 μm^2 at the 0.25 micron process size. Currently, prognostic cells are available for semiconductor failure mechanisms such as electrostatic discharge (ESD), hot carrier, metal migration, dielectric breakdown, and radiation effects.

The time to failure of these prognostic cells can be pre-calibrated with respect to the time to failure of the actual product. Because of their location, these cells contain and experience substantially similar dependencies as does the actual product. The stresses that contribute to degradation of the circuit include voltage, current, temperature, humidity, and radiation. Since the operational stresses are the same, the damage rate is expected to be the same for both the circuits. However, the prognostic cell is designed to fail faster through increased stress on the cell structure by means of scaling.

Scaling can be achieved by controlled increase of the current density inside the cells. With the same amount of current passing through both circuits, if the cross-sectional area of the current-carrying paths in the cells is decreased, a higher current density is achieved. Further control in current density can be achieved by increasing the voltage level applied to the cells. A combination of both of these techniques can also be used. Higher current density leads to higher internal (joule) heating, causing greater stress on the cells. When a current of higher density passes through the cells, they are expected to fail faster than the actual circuit [19].

Figure 67.2 shows the failure distribution of the actual product and the canary health monitors. Under the same environmental and operational loading conditions, the canary health monitors wear out faster to indicate the impending failure of the actual product. Canaries can be calibrated to provide sufficient advance warning of failure (prognostic distance) to enable appropriate maintenance and replacement activities. This point can be adjusted to some other early indication level. Multiple trigger points can also be provided, using multiple cells evenly spaced over the bathtub curve.

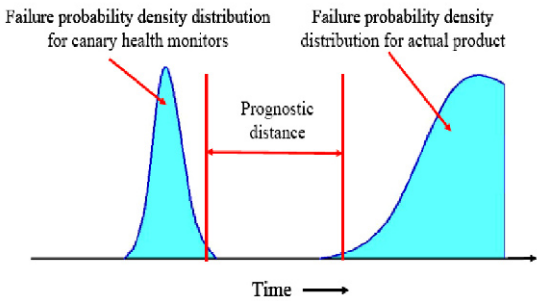


Figure 67.2. Advanced warning of failure using canary structures

The extension of this approach to board-level failures was proposed by Anderson *et al*. [21], who created canary components (located on the same printed circuit board) that include the same mechanisms that lead to failure in actual components. Anderson *et al*., identified two prospective failure mechanisms: (1) low cycle fatigue of solder joints, assessed by monitoring solder joints on and within the canary package; and (2) corrosion monitoring, using circuits that are

susceptible to corrosion. The environmental degradation of these canaries was assessed using accelerated testing, and degradation levels were calibrated and correlated to actual failure levels of the main system. The corrosion test device included an electrical circuitry susceptible to various corrosion-induced mechanisms. Impedance spectroscopy was proposed for identifying changes in the circuits by measuring the magnitude and phase angle of impedance as a function of frequency. The change in impedance characteristics can be correlated to indicate specific degradation mechanisms.

Still, there remain unanswered questions with the use of fuses and canaries for PHM. For example, if a canary monitoring a circuit is replaced, what is the impact when the product is re-energized? What protective architectures are appropriate for post-repair operations? What maintenance guidance must be documented and followed when fail-safe protective architectures have or have not been included? This approach is difficult to implement in legacy systems, because it may require re-qualification of the entire system with the canary module. Also, the integration of fuses and canaries with the host electronic system could be an issue with respect to real estate on semiconductors and boards. Finally, the company must ensure that the additional cost of implementing PHM can be recovered through increased operational and maintenance efficiencies.

67.4.2 Monitoring and Reasoning of Failure Precursors

A failure precursor is an event that signifies impending failure. A precursor indication is usually a change in a measurable variable that can be associated with subsequent failure. For example, a shift in the output voltage of a power supply would suggest impending failure due to a damaged feedback regulator and opto-isolator circuitry. Failures can then be predicted by using a causal relationship between a measured variable that can be correlated with subsequent failure.

A first step in PHM is to select the life-cycle parameters to be monitored. Parameters can be identified based on factors that are crucial for safety, that are likely to cause catastrophic failures, that are essential for mission completeness, or that can result in long downtimes. Selection can also be based on knowledge of the critical parameters established by past experience and field failure data on similar products and on qualification testing. More systematic methods, such as failure mode mechanisms and effects analysis (FMMEA) [22], can be used to determine parameters that need to be monitored.

Pecht *et al*. [23] proposed several measurable parameters that can be used as failure precursors for electronic components including switching power supplies, cables and connectors, CMOS integrated circuits, and voltage-controlled high-frequency oscillators (see Table 67.1).

Testing was conducted to demonstrate the potential of select parameters for viably detecting incipient failures in electronic systems. Supply current monitoring is routinely performed for testing of CMOS ICs. This method is based upon the notion that defective circuits produce an abnormal or at least significantly different amount of current than the current produced by fault-free circuits. This excess current can be sensed to detect faults. The power supply current (Idd) can be defined by two elements: the Iddq-quiescent current and the Iddt-transient or dynamic current. Iddq is the leakage current drawn by the CMOS circuit when it is in a stable (quiescent) state. Iddt is the supply current produced by circuits under test during a transition period after the input has been applied. Iddq has been reported to have the potential for detecting defects such as bridging, opens, and parasitic transistor defects. Operational and environmental stresses, such as temperature, voltage, and radiation, can quickly degrade previously undetected faults and increase the leakage current (Iddq). There is extensive literature on Iddq testing, but little has been done on using Iddq for *in situ* PHM. Monitoring Iddq has been more popular than monitoring Iddt [24]–[26].

Smith and Campbell [27] developed a quiescent current monitor (QCM) that can detect elevated Iddq current in real time during operation. The QCM performed leakage current measurements on every transition of the system clock to get maximum coverage of the IC in real time. Pecuh *et*

al. [25] and Xue and Walker [26] proposed a low-power built-in current monitor for CMOS devices. In the Pecuh *et al*., study, the current monitor was developed and tested on a series of inverters for simulating open and short faults. Both fault types were successfully detected and operational speeds of up to 100 MHz were achieved with negligible effect on the performance of the circuit under test. The current sensor developed by Xue and Walker enabled Iddq monitoring at a resolution level of 10 pA. The system translated the current level into a digital signal with scan chain readout. This concept was verified by fabrication on a test chip.

GMA Industries [28]–[30] proposed embedding molecular test equipment (MTE) within ICs to enable them to continuously test themselves during normal operation and to provide a visual indication that they have failed. The molecular test equipment could be fabricated and embedded within the individual integrated circuit in the chip substrate. The molecular-sized sensor "sea of needles" could be used to measure voltage, current, and other electrical parameters, as well as sense changes in the chemical structure of integrated circuits that are indicative of pending or actual circuit failure. This research focuses on the development of specialized doping techniques for carbon nanotubes to form the basic structure comprising the sensors. The integration of these sensors within conventional IC circuit devices, as well as the use of molecular wires for the interconnection of sensor networks, is an important factor in this research. However, no product or prototype has been developed to date.

Kanniche and Mamat-Ibrahim [31] developed an algorithm for health monitoring of voltage source inverters with pulse width modulation. The algorithm was designed to detect and identify transistor open circuit faults and intermittent misfiring faults occurring in electronic drives. The mathematical foundations of the algorithm were based on discrete wavelet transform (DWT) and fuzzy logic (FL). Current waveforms were monitored and continuously analyzed using DWT to identify faults that may occur due to constant stress, voltage swings, rapid speed variations, frequent stop/start-ups, and constant overloads. After fault detection, "if-then" fuzzy rules were used for VLSI fault diagnosis to pinpoint the fault device. The algorithm was demonstrated to detect certain intermittent faults under laboratory experimental conditions.

Table 67.1. Potential failure precursors for electronics

Electronic subsystem	Failure precursor
Switching power supply	• DC output (voltage and current levels) • Ripple • Pulse width duty cycle • Efficiency • Feedback (voltage and current levels) • Leakage current • RF noise
Cables and connectors	• Impedance changes • Physical damage • High-energy dielectric breakdown
CMOS IC	• Supply leakage current • Supply current variation • Operating signature • Current noise • Logic level variations
Voltage-controlled oscillator	• Output frequency • Power loss • Efficiency • Phase distortion • Noise
Field effect transistor	• Gate leakage current/resistance • Drain-source leakage current/resistance
Ceramic chip capacitor	• Leakage current/resistance • Dissipation factor • RF noise
General purpose diode	• Reverse leakage current • Forward voltage drop • Thermal resistance • Power dissipation • RF noise
Electrolytic capacitor	• Leakage current/resistance • Dissipation factor • RF noise
RF power amplifier	• Voltage standing wave ratio (VSWR) • Power dissipation • Leakage current

Lall *et al*. [32],[33] have developed a damage precursor-based residual life computation approach for various package elements to prognosticate electronic systems prior to the appearance of any

macro-indicators of damage. In order to implement the system-health monitoring, precursor variables have been identified for various package elements and failure mechanisms. Model algorithms have been developed to correlate precursors with impending failure for computation of residual life. Package elements investigated include first-level interconnects, dielectrics, chip interconnects, underfills, and semiconductors. Examples of damage proxies include the phase growth rate of solder interconnects, intermetallics, normal stress at chip interface, and interfacial shear stress. Lall *et al*., suggest that the precursor-based damage computation approach eliminates the need for knowledge of prior or posterior operational stresses and enables the management of system reliability of deployed non-pristine materials under unknown loading conditions. The approach can be used on redeployed parts, sub-systems, and systems, since it does not depend on the availability of prior stress histories.

Self-monitoring analysis and reporting technology (SMART), currently employed in select computing equipment for hard disk drives (HDD), is another example of precursor monitoring [34],[35]. HDD operating parameters, including the flying height of the head, error counts, variations in spin time, temperature, and data transfer rates, are monitored to provide advance warning of failures (see Table 67.2). This is achieved through an interface between the computer's start-up program (BIOS) and the hard disk drive.

Systems for early fault detection and failure prediction are being developed using variables such as current, voltage, and temperature, continuously monitored at various locations inside the system. Sun Microsystems refers to this approach as continuous system telemetry harnesses [36]. Along with sensor information, soft performance parameters such as loads, throughputs, queue lengths, and bit error rates are tracked. Prior to PHM implementation, characterization is conducted by monitoring the signals of different variables to learn a multivariate state estimation technique (MSET) model. Once the model is established using this data, it is used to predict the signal of a particular variable based on learned correlations among all variables [37]. Based on the expected variability in the value of a particular variable during application, a sequential probability ratio test (SPRT) is constructed. During actual monitoring the SPRT will be used to detect the deviations of the actual signal from the expected signal based on distributions (and not on single threshold value) [38],[39].

During implementation, the performance variables are continuously monitored using sensors already existing in Sun Microsystems' servers and recorded in a circular file structure. The file retains data collected at high sampling rates for seventy-two hours and data collected at a lower sampling rate for thirty days. For each signal being monitored, an expected signal is generated using the MSET model.

Table 67.2. Monitoring parameters based on reliability concerns in hard drives

Reliability issues	Parameters monitored
• Head assembly - crack on head - head contamination or resonance - bad connection to electronics module • Motors/bearings - motor failure - worn bearing - excessive run-out - no spin • Electronic module - circuit/chip failure - interconnection/solder joint failure - bad connection to drive or bus • Media - scratch/defects - retries - bad servo - ECC corrections	• Head flying height: A downward trend in flying height will often precede a head crash. • Error checking and correction (ECC) use and error counts: The number of errors encountered by the drive, even if corrected internally, often signals problems developing with the drive. • Spin-up time: Changes in spin-up time can reflect problems with the spindle motor. • Temperature: Increases in drive temperature often signal spindle motor problems. • Data throughput: Reduction in the transfer rate of data can signal various internal problems.

This signal is generated in real time based on learned correlations during characterization (see Figure 67.3). A new signal of residuals is generated, which is the arithmetic difference of the actual and expected time-series signal values. These differences are used as input to the SPRT model, which continuously analyzes the deviations and provides an alarm if the deviations are of concern [37]. The monitored data is analyzed to (1) provide alarms based on leading indicators of failure, and (2) enable use of monitored signals for fault diagnosis, root-cause analysis of no-fault-founds (NFF), and analysis of faults due to software aging [40].

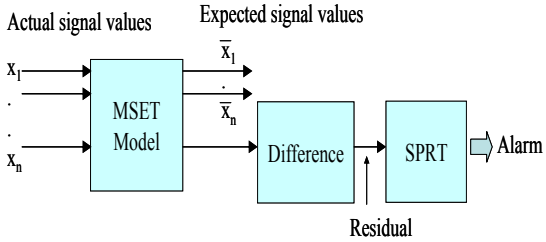


Figure 67.3. Sun Microsystems' approach to PHM

Brown *et al*. [41] demonstrated that the remaining useful life of a commercial global positioning system (GPS) can be predicted by using a precursor-to-failure approach. The failure modes for GPS included precision failure, due to an increase in position error, and solution failure, due to increased outage probability. These failure progressions were monitored *in situ* by recording system-level features reported using the national marine electronics association (NMEA) protocol 0183. The GPS was characterized to collect the principal feature value for a range of operating conditions. The approach was validated by conducting accelerated thermal cycling of the GPS with the offset of the principal feature value measured *in situ*. Based on experimental results, parametric models were developed to correlate the offset in the principal feature value with solution failure. During the experiment, the BIT provided no indication of an impending solution failure [41].

In general, to implement a precursor reasoning-based PHM system, it is necessary to identify the precursor variables for monitoring, and then develop a reasoning algorithm to correlate the change in the precursor variable with the impending failure. This characterization is typically performed by measuring the precursor variable under an expected or accelerated usage profile. Based on the characterization, a model is developed--typically a parametric curve-fit, neural-network, Bayesian network, or a time-series trending of a precursor signal. This approach assumes that there is one or more expected usage profiles that are predictable and can be simulated in a laboratory setup. In some products the usage profiles are predictable, but this is not always true.

For a fielded product with highly varying usage profiles, an unexpected change in the usage profile could result in a different (non-characterized) change in the precursor signal. If the precursor reasoning model is not characterized to factor in the uncertainty in life-cycle usage and environmental profiles, it may provide false alarms. Additionally, it may not always be possible to characterize the precursor signals under all possible usage scenarios (assuming they are known and can be simulated). Thus, the characterization and model development process can often be time-consuming and costly and may not always work.

67.4.3 Monitoring Environmental and Usage Loads for Damage Modeling

The life-cycle environment of a product consists of manufacturing, storage, handling, operating and non-operating conditions. The life-cycle loads (Table 67.3), either individually or in various combinations, may lead to performance or physical degradation of the product and reduce its service life [42]. The extent and rate of product degradation depends upon the magnitude and duration of exposure (usage rate, frequency, and severity) to such loads. If one can measure these loads *in situ*, the load profiles can be used in conjunction with damage models to assess the degradation due to cumulative load exposures.

The assessment of the impact of life-cycle usage and environmental loads on electronic structures and components was studied by Ramakrishnan and Pecht [42]. This study introduced the life-consumption monitoring (LCM) methodology

Table 67.3. Examples of life-cycle loads

Load	Load conditions
Thermal	Steady-state temperature, temperature ranges, temperature cycles, temperature gradients, ramp rates, heat dissipation
Mechanical	Pressure magnitude, pressure gradient, vibration, shock load, acoustic level, strain, stress
Chemical	Aggressive versus inert environment, humidity level, contamination, ozone, pollution, fuel spills
Physical	Radiation, electromagnetic interference, altitude
Electrical	Current, voltage, power, resistance

(Figure 67.4), which combined *in situ* measured loads with physics-based stress and damage models for assessing the life consumed.

The application of the LCM methodology to electronics PHM was illustrated with two case studies [42],[43]. The test vehicle consisted of an electronic component-board assembly placed under the hood of an automobile and subjected to normal driving conditions in the Washington, DC, area. The test board incorporated eight surface-mount leadless inductors soldered onto an FR-4 substrate using eutectic tin-lead solder. Solder joint fatigue was identified as the dominant failure mechanism. Temperature and vibrations were measured *in situ* on the board in the application environment. Using the monitored environmental data, stress and damage models were developed and used to estimate consumed life.

The remaining life of the test board, estimated by LCM, is compared in Figure 67.5 with estimates obtained using similarity analysis, SAE handbook data, and the actual measured life. As shown in Figure 67.5, the remaining life estimated by either similarity analysis or using data from SAE handbook differs significantly from the actual life of the board, whereas the remaining life estimated by LCM is in excellent agreement with actual life. The discrepancies between either similarity analysis or SAE estimates and actual life are attributed to the fact that neither approach accounts for the accident that the car experienced on day 22 [42]. Only LCM accounted for this unforeseen event because the operating environment was being monitored *in situ*.

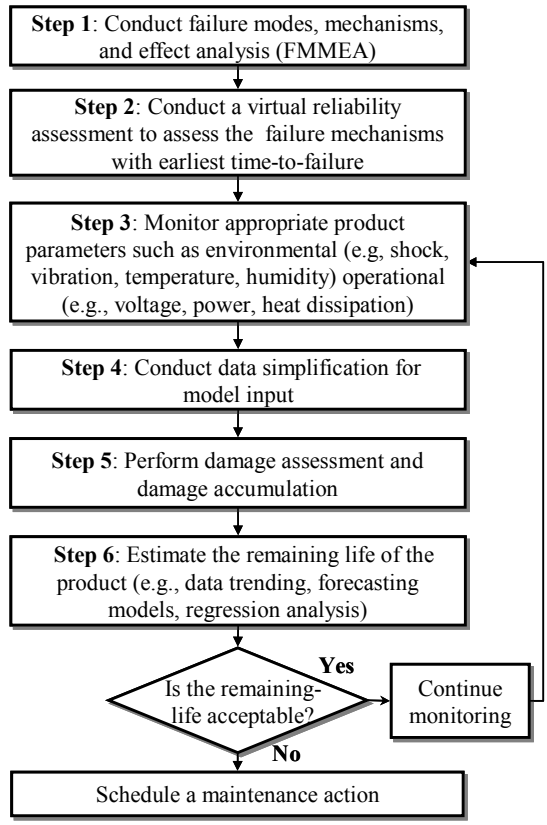


Figure 67.4. CALCE life-consumption monitoring methodology

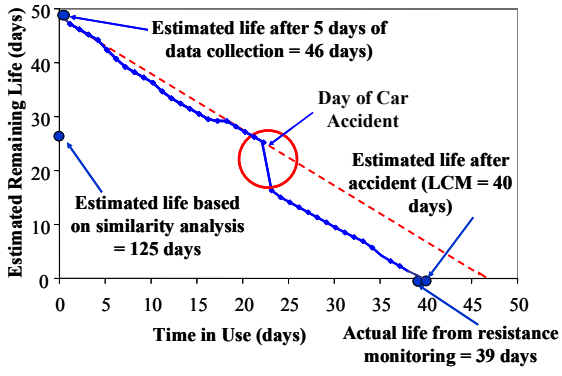


Figure 67.5. Remaining-life estimation of test board

Mathew *et al*. [44] applied the LCM methodology in conducting a prognostic remaining-life assessment of circuit cards inside a space shuttle solid rocket booster (SRB). Vibration-time history, recorded on the SRB from the pre-launch stage to splashdown, was used in conjunction with physics-based models to assess the damage caused due to vibration and shock loads. Using the entire life-cycle loading profile of the SRBs, the remaining life of the components and structures on the circuit cards were predicted. It was determined that an electrical failure was not expected within another forty missions. However, vibration and shock analysis exposed an unexpected failure of the circuit card due to a broken aluminum bracket mounted on the circuit card. Damage accumulation analysis determined that the aluminum brackets had lost significant life due to shock loading.

Shetty *et al*. [45] applied the LCM methodology for conducting a prognostic remaining-life assessment of the end effector electronics unit (EEEU) inside the robotic arm of the space shuttle remote manipulator system (SMRS). A life-cycle loading profile for thermal and vibrational loads was developed for the EEEU boards. Damage assessment was conducted using physics-based mechanical and thermomechanical damage models. A prognostic estimate using a combination of damage models, inspection, and accelerated testing showed that there was little degradation in the electronics and they could be expected to last another twenty years.

Vichare *et al*. [2] outlined generic strategies for *in situ* load monitoring, including selecting appropriate parameters to monitor and designing an effective monitoring plan. Methods for processing the raw sensor data during *in situ* monitoring to reduce the memory requirements and power consumption of the monitoring device were presented. Approaches were also presented for embedding intelligent front-end data processing capabilities in monitoring systems to enable data reduction and simplification (without sacrificing relevant load information) prior to input in damage models for health assessment and prognostics.

Embedding the data reduction and load parameter extraction algorithms into the sensor modules as suggested by Vichare *et al*. [46] can lead to reduction in on-board storage space, low power consumption, and uninterrupted data collection over longer durations. A time-load signal can be monitored *in situ* using sensors, and further processed to extract cyclic range (Δs), cyclic mean load (Smean), and rate of change of load (ds/dt), using embedded load extraction algorithms. The extracted load parameters can be stored in appropriately binned histograms to achieve further data reduction. After the binned data is downloaded, it can be used to estimate the distributions of the load parameters. The usage history is used for damage accumulation and remaining life prediction.

Efforts to monitor life-cycle load data on avionics modules can be found in time-stress measurement device (TSMD) studies. Over the years TSMD designs have been upgraded using advanced sensors, and miniaturized TSMDs are being developed due to advances in microprocessor and non-volatile memory technologies [47].

Searls *et al*. [48] undertook *in situ* temperature measurements in both notebook and desktop computers used in different parts of the world. In terms of the commercial applications of this approach, IBM has installed temperature sensors on hard drives (Drive-TIP) [49] to mitigate risks due to severe temperature conditions, such as thermal tilt of the disk stack and actuator arm, off-track writing, data corruptions on adjacent cylinders, and outgassing of lubricants on the spindle motor. The sensor is controlled using a dedicated algorithm to generate errors and control fan speeds.

Strategies for efficient *in situ* health monitoring of notebook computers were provided by Vichare *et al*. [50]. In this study, the authors monitored and statistically analyzed the temperatures inside a notebook computer, including those experienced during usage, storage, and transportation, and discussed the need to collect such data both to improve the thermal design of the product and to monitor prognostic health. The temperature data was processed using two algorithms: (1) ordered overall range (OOR) to convert an irregular time-temperature history into peaks and valleys and also to remove noise due to small cycles and sensor variations, and (2) a three-parameter Rainflow

algorithm to process the OOR results to extract full and half cycles with cyclic range, mean, and ramp rates. The effects of power cycles, usage history, CPU computing resources usage, and external thermal environment on peak transient thermal loads were characterized.

The European Union funded a project from September 2001 through February 2005, named environmental life-cycle information management and acquisition for consumer products (ELIMA), which aimed to develop ways of better managing the life cycles of products using technology to collect vital information during a product's life to lead to better and more sustainable products [51]. Though the focus of this work was not on prognostics, the project demonstrated the monitoring of the life-cycle conditions of electronic products by field trials. ELIMA partners built and tested two special prototype consumer products with data collection features, and investigated the implications for producers, users, and recyclers. The ELIMA technology included sensors and memory built into the product to record dynamic data such as operation time, temperature, and power consumption. This was added to static data about materials and manufacture. Both a direct communication (*via* GSM module) as well as a two-step communication with the database (RFID data retrieval followed by an Internet data transfer) was applied. As a case study, the member companies monitored the application conditions of a game console and a household refrigerator-freezer.

Skormin *et al*. [52] developed a data-mining model for failure prognostics of avionics units. The model provides a means of efficiently clustering data on parameters measured during operation, such as vibration, temperature, power supply, functional overload, and air pressure. These parameters are monitored *in situ* on the flight using time-stress measurement devices. The objectives of the model are (1) to investigate the role of measured environmental factors in the development of particular failure; (2) to investigate the role of combined effects of several factors; and (3) to re-evaluate the probability of failure on the basis of known exposure to particular adverse conditions. Unlike the physics-based assessments made by Ramakrishnan and Pecht [42], the data-mining model relies on the statistical data available from the records of a time-stress measurement device (TSMD) on cumulative exposure to environmental factors and operational conditions. The TSMD records, along with calculations of probability of failure of avionics units, are used for developing the prognostic model. The data mining enables an understanding of the usage history and allows tracing the cause of failure to individual operational and environmental conditions.

67.5 Implementation of PHM in a System

Implementing an effective PHM strategy for a complete product or system may require integrating different prognostic health monitoring approaches. The first step is an analysis to determine the weak link(s) in the system based on the potential failure modes and mechanisms to enable a more focused monitoring process. Once the potential failure modes, mechanisms, and effects (FMMEA) have been identified, a combination of canaries, precursor reasoning, and life-cycle damage modeling may be necessary, depending on the failure attributes. In fact, different approaches can be implemented based on the same sensor data.

For example, operational loads of computer system electronics such as temperature, voltage, current, and acceleration, can be used with damage models to calculate the susceptibility to electromigration between metallizations and thermal fatigue of interconnects, plated-through holes, and die attach. Also, the processor usage, current, and CPU temperature data can be used to build a statistical model that is based on the correlations between these parameters. This model can be appropriately trained to detect thermal anomalies and identify signs for certain transistor degradation.

Future electronic system designs will integrate sensing and processing modules that will enable *in situ* PHM. Advances in sensors, microprocessors, compact non-volatile memory, battery technologies, and wireless telemetry have already

enabled the implementation of sensor modules and autonomous data loggers. Integrated, miniaturized, low-power, reliable sensor systems operated using portable power supplies (such as batteries) are being developed. These sensor systems have a self-contained architecture requiring minimum or no intrusion into the host product, in addition to specialized sensors for monitoring localized parameters. Sensors with embedded algorithms will enable fault detection, diagnostics, and remaining life prognostics, which will ultimately drive the supply chain. The prognostic information will be linked *via* wireless communications to relay needs to maintenance officers. Automatic identification techniques such as radio frequency identification (RFID) will be used to locate parts in the supply chain, all integrated through a secure web portal to acquire and deliver replacement parts quickly on an as-needed basis.

67.6 Health Monitoring for Product Take-back and End-of-life Decisions

In addition to in-service reliability assessment and maintenance, health monitoring could also be effectively used for supporting product take-back and end-of-life decisions. Product take-back indicates the responsibility of manufacturers for their products over the entire life cycle, including disposal. The motivation driving product take-back is the concept of extended producer responsibility (EPR) for post-consumer electronic waste [53]. The objective of EPR is to make manufacturers and distributors financially responsible for their products when they are no longer needed.

End-of-life product recovery strategies include repair, refurbishing, remanufacturing, reuse of components, material recycling, and disposal. One of the challenges in end-of-life decision making is to determine on an application-specific basis whether any components could be reused and what subset should be disposed of in order to minimize system costs [54]. Several interdependent issues must be considered concurrently to properly determine the optimum component re-use ratio, including assembly/disassembly costs and any defects introduced by either process, product degradation incurred in the original life cycle, and the waste stream associated with the life cycle. Among these factors, the estimate of the degradation of the product in its original life cycle could be the most uncertain input to end-of-life decisions. This task requires knowledge of the entire history of the product's life cycle. This could be effectively carried out using health monitoring.

The methods of assessing product degradation for recovery reported in the literature have focused on the use of non-destructive testing. For example, the Applied Research Lab at Penn State University [55] developed a low-cost assessment approach for the usability of paints beyond their expiration dates, based upon monitoring the paint conductivity and polarization as a function of frequency to extend the shelf life of stock.

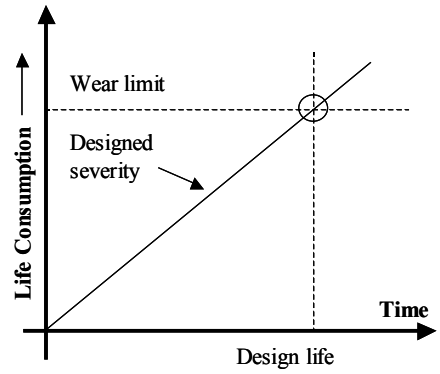
While these approaches are based upon tests conducted after the product is returned or considered expired, efforts to develop *in situ* monitoring techniques enabling product recovery have also been reported. Scheidt *et al*. [56] proposed the development of special electrical ports, referred to as green ports, to retrieve product usage data that could assist in the recycling and reuse of electronic products. Klausner *et al*. [57],[58] proposed the use of an integrated electronic data log (EDL) for recording parameters indicative of product degradation. EDL was implemented on electric motors to increase the reuse of motors. In another study, [59] domestic appliances were monitored for collecting usage data by means of electronic units fitted on the appliances. This work introduced the life-cycle data acquisition unit, which can be used for data collection and also for diagnostics and servicing. Middendorf *et al*. [60] suggested developing life-information modules to record the cycle conditions of products for reliability assessment, product refurbishing, and reuse.

Designers often establish the usable life of products and warranties based on extrapolating the accelerated test results to assumed usage rates and life-cycle conditions. These assumptions may be based on worst-case scenarios of various parameters composing the end user environment. Thus if the assumed conditions and actual use

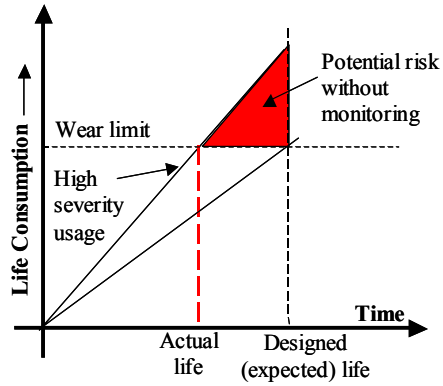
conditions are the same, the product would last for the designed time, as shown in Figure 67.6(a). However, this is rarely true, and usage and environmental conditions could vary significantly from those assumed. For example, consider products equipped with life-consumption monitoring systems for providing *in situ* assessment of remaining life. In this situation, even if the product is used at a higher usage rate and in harsh conditions, it can still avoid unscheduled maintenance and catastrophic failure, maintain safety, and ultimately save cost. These are typically the motivational factors for use of health monitoring or life consumption monitoring, as shown in Figure 67.6(b).

One of the vital inputs in making end-of-life decisions is the estimate of degradation and the remaining life of the product. Figure 67.6(c) illustrates a scenario in which a working product is returned at the end of its designed life. Using the health monitors installed within the product, the reusable life can be assessed. Unlike testing conducted after the product is returned, this estimate can be made without having to disassemble the product.

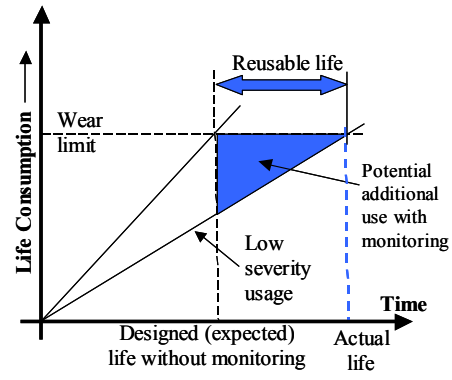
Ultimately, depending on other factors such as cost of the product, demand for spares, cost, and yield in assembly and disassembly, the manufacturer can choose to reuse or dispose. For example, in the case study of LCM, assuming that the car is deemed unusable and is returned by the customer after the accident on day 22, the manufacturer could use the collected data to estimate the remaining life of the board and decide on its reuse or disposal.



(a) Usage as *per* design



(b) More severe usage than intended design



(c) Less severe usage than intended design

Figure 67.6. Application of health monitoring for product reuse

67.7 Conclusions

Prognostics and health monitoring is emerging as a popular alternative over traditional reliability assessment methods. The applicability of PHM to electronic products and systems has been presented. The current approaches for implementing prognostics and health monitoring in products and systems are (1) installing built-in structures that will fail faster than the actual product when subjected to application conditions; (2) monitoring and reasoning of parameters (*e.g.*, system characteristics, defects, performance) that are indicative of an impending failure; and (3) monitoring and modeling environmental and usage data that influence the system's health and converting the measured data into life consumed. A combination of these approaches may be necessary to successfully assess the degradation of the product in real time and subsequently provide the estimate of useful life before the need for maintenance or replacement. Finally, the use of health monitoring in accurately estimating product degradation to assist end-of-life decisions has been presented.

References

[1] Vichare N, Pecht M. Prognostics and health management of electronics. IEEE Transactions on Components and Packaging Technologies 2006; 29(1):222–229.

[2] Vichare N, Rodgers P, Eveloy V, Pecht M. Monitoring Environment and usage of electronic products for health assessment and product design. IEEE Workshop on Accelerated Stress Testing and Reliability (ASTR), Austin, TX, 2005; October 2–5.

[3] Lall P, Pecht M, Hakim E. Influence of temperature on microelectronics and system reliability. CRC Press, New York, 1997.

[4] Pecht M, Das D, Ramakrishnan A. The IEEE standards on reliability program and reliability prediction methods for electronic equipment. Microelectronics Reliability 2002; 42:1259–1266.

[5] Dasgupta A. The physics-of-failure approach at the university of Maryland for the development of reliable electronics. Proceedings of Third International Conference on Thermal and Mechanical Simulation in (Micro) Electronics (EuroSimE). 2002; 10–17.

[6] Condition based maintenance plus. https://akss.dau.mil/DAG/GuideBook/IG_c5.2.1.2.asp

[7] Chapter 5.3 – Performance based logistics. DoD 5000.2 Policy Document, Defense Acquisition Guidebook, 2004; December.

[8] Cutter D. Thompson O., Condition-based maintenance plus select program survey. Report LG301T6, 2005; January. http://www.acq.osd.mil/log/mppr/CBM%2B.htm.

[9] Kirkland L, Pombo T, Nelson K, Berghout F. Avionics Health management: searching for the prognostics grail. Proceedings of the IEEE Aerospace Conference 2004; 6–13 March, 5:3448–3454.

[10] Tumer I, Bajwa A. A survey of aircraft engine health monitoring systems. Proceedings of the AIAA Joint Propulsion Conference, Los Angeles, CA 1999; June.

[11] Carden E, Fanning P. Vibration based condition monitoring: A review. Journal of Structural Health Monitoring 2004; 3(4):355–377.

[12] Chang P, Flatau A, Liu S. Review paper: Health monitoring of civil infrastructure. Journal of Structural Health Monitoring 2003; 3(3): 257–267.

[13] Kacprzynski GM, Roemer M, Modgil G, Palladino A. Enhancement of physics of failure prognostic models with system level features. IEEE Aerospace Conference Proceedings 2002; 6:2925.

[14] Xie J, Pecht M. Application of *in-situ* health monitoring and prognostic sensors. 9th Pan Pacific Microelectronics Symposium Exhibits and Conference, Hawaii 2004; 10–12 February.

[15] Pecht M, Dube M, Natishan M, Knowles I. An evaluation of built-in test. IEEE Transactions on Aerospace and Electronic Systems 2001; January, 37(1):266–272.

[16] Johnson D. Review of fault management techniques used in safety critical avionic systems. Progress in Aerospace Science 1996; October,32(5): 415–431.

[17] Williams R, Banner J, Knowles I, Natishan M, Pecht M. An investigation of "cannot duplicate" failure. Quality and Reliability Engineering International 1998; 14:331–337.

[18] Ramakrishnan A, Syrus T, Pecht M. Electronic hardware reliability. Avionics Handbook, CRC Press, Boca Raton, FL, 2000; December: 22.1–22.21.

[19] Mishra S, Pecht M. *In-situ* sensors for product reliability monitoring. Proceedings of the SPIE 2002; 4755:10–19.

[20] Ridgetop Semiconductor-Sentinel Silicon™ Library, "Hot Carrier (HC) Prognostic Cell," 2004; August.
[21] Anderson N, Wilcoxon R. Framework for prognostics of electronic systems. Proceedings of International Military and Aerospace/Avionics COTS Conference, Seattle, WA, 2004; August 3–5
[22] Ganesan S, Eveloy V, Das D, Pecht M. Identification and utilization of failure mechanisms to enhance FMEA and FMECA. Proceedings of the IEEE Workshop on Accelerated Stress Testing and Reliability (ASTR), Austin, TX 2005; October 3–5.
[23] Pecht M, Radojcic R, Rao G. Guidebook for managing silicon chip reliability. CRC Press, Boca Raton, FL, 1999.
[24] Smith P, Campbell D. Practical implementation of BICS for safety-critical applications. Proceedings of IEEE International Workshop on Current and Defect Based Testing-DBT 2000; 30 April:51–56.
[25] Pecuh I, Margala M, Stopjakova V. 1.5 volts Iddq/Iddt current monitor. Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering 1999; 9–12 May, 1:472–476.
[26] Xue B, Walker D. Built-In Current sensor for IDDQ test. Proceedings of the IEEE International Workshop on Current and Defect Based Testing-DBT 2004; 25 April:3–9.
[27] Smith P, Campbell D. Practical implementation of BICS for safety-critical applications. Proceedings of the IEEE International Workshop on Current and Defect Based Testing-DBT 2000; 30 April:51–56.
[28] Wright R, Kirkland L. Nano-scaled electrical sensor devices for integrated circuit diagnostics. IEEE Aerospace Conference 2003; March 8–15, 6:2549–2555.
[29] Wright R, Zgol M, Adebimpe D, Kirkland L. Functional circuit board testing using nanoscale sensors. IEEE Systems Readiness Technology Conference 2003; 22–25 September:266–272.
[30] Wright R, Zgol M, Keeton S, Kirkland L. Nanotechnology-based molecular test equipment (MTE). IEEE Aerospace and Electronic Systems Magazine, 2001; June, 16(6):15–19.
[31] Kanniche M, Mamat-Ibrahim M. Wavelet based fuzzy algorithm for condition monitoring of voltage source inverters. Electronic Letters 2004; February, 40(4).
[32] Lall P, Islam N, Rahim K, Suhling J, Gale S. Leading indicators-of-failure for prognosis of electronic and MEMS packaging. Proceedings of the Electronics Components and Technology Conference, Las Vegas, NV 2004; June 1–4:1570–1578.
[33] Lall P, Islam N, Suhling J. Prognostication and health monitoring of leaded and lead free electronic and MEMS packages in harsh environments. Proceedings of the 55th IEEE Electronic Components and Technology Conference, Orlando, FL 2005; June 1–3:1305–1313.
[34] Self-monitoring analysis and reporting technology (SMART)", PC Guide, http://www.pcguide.com/ref/hdd/perf/qual/features SMART-c.html, viewed on, 2005; August 30.
[35] Hughes G, Murray J, Kreutz-Delgado K, Elkan C. Improved disk-drive failure warnings. IEEE Transactions on Reliability 2002; 51(3):350–357.
[36] Gross K. Continuous system telemetry harness," Sun Labs Open House, 2004, http://research.sun.com/sunlabsday/docs.2004/talks/1.03_Gross.pdf, viewed in August 2005.
[37] Whisnant K, Gross K, Lingurovska N. Proactive fault monitoring in enterprise servers. 2005 IEEE International Multi-conference on Computer Science and Computer Engineering, Las Vegas, NV 2005; June.
[38] Mishra K, Gross K. Dynamic stimulation tool for improved performance modeling and resource provisioning of enterprise servers. Proceedings of the 14th IEEE International Symposium on Software Reliability Engineering (ISSRE'03), Denver, CO 2003; November.
[39] Cassidy K, Gross K, Malekpour A. Advanced pattern recognition for detection of complex software aging phenomena in online transaction processing servers. Proceedings of the International Performance and Dependability Symposium, Washington, DC 2002; June 23–26.
[40] Vaidyanathan K, Gross K. MSET performance optimization for detection of software aging. Proceedings of the 14th IEEE International Symposium on Software Reliability Engineering, Denver, CO 2003; November.
[41] Brown D, Kalgren P, Byington C, Orsagh R. Electronic prognostics – A case study using global positioning system (GPS). IEEE Autotestcon 2005.
[42] Ramakrishnan A, Pecht M. A life consumption monitoring methodology for electronic systems. IEEE Transactions on Components and Packaging Technologies 2003; 26(3):625–634.
[43] Mishra S, Pecht M, Smith T, McNee I, Harris R. Remaining life prediction of electronic products using life consumption monitoring approach. European Microelectronics Packaging and

Interconnection Symposium, Cracow, Poland. 2002; June 16–18: 136–142.

[44] Mathew S, Das D, Osterman M, Pecht M, Ferebee R. Prognostic assessment of aluminum support structure on a printed circuit board. ASME Journal of Electronic Packaging, 2006; December, 128(4): 339–345.

[45] Shetty V, Das D, Pecht M, Hiemstra D, Martin S. Remaining life assessment of shuttle remote manipulator system end effector. Proceedings of the 22nd Space Simulation Conference, Ellicott City, MD 2002; October 21–23.

[46] Vichare N, Rodgers P, Pecht M. Methods for binning and density estimation of load parameters for prognostics and health management. International Journal of Performability Engineering 2006; April, 2(2):149–161.

[47] Rouet V, Foucher B. Development and use of a miniaturized health monitoring device. Proceedings of the IEEE International Reliability Physics Symposium 2004;645–646.

[48] Searls D, Dishongh T, Dujari P. A strategy for enabling data driven product decisions through a comprehensive understanding of the usage environment. Proceedings of IPACK'01, Kauai, Hawaii, USA, July 8–13, 2001.

[49] Herbst G. IBM's drive temperature indicator processor (Drive-TIP) helps ensure high drive reliability. IBM White Paper, http://www.hc.kz/pdf/drivetemp.pdf, viewed in September 2005.

[50] Vichare N, Rodgers P, Eveloy V, Pecht M. *In situ* temperature measurement of a notebook computer – a case study in health and usage monitoring of electronics. IEEE Transactions on Device and Materials Reliability 2004; December, 4(4):658–663.

[51] Bodenhoefer K. Environmental life cycle information management and acquisition – First experiences and results from field trials. Proceedings of Electronics Goes Green 2004+, Berlin 2004; September 5–8:541-546.

[52] Skormin V, Gorodetski V, Popyack L. Data mining technology for failure prognostic of avionics. IEEE Transactions on Aerospace and Electronic Systems 2002; April, 38(2):388–403.

[53] Rose C, Beiter A, Ishii K. Determining end-of-life strategies as a part of product definition. 1999 IEEE International Symposium on Electronics and the Environment, Piscataway, NJ, USA 1999: 219–224.

[54] Sandborn P, Murphy C. A model for optimizing the assembly and disassembly of electronic systems. IEEE Transactions on Electronics Packaging Manufacturing 1999; April, 22(2):105–117.

[55] Paint shelf life monitoring," http://www.bmpcoe.org/bestpractices/arlps/arlps_18.html, accessed on June 2004.

[56] Scheidt L, Zong S. An approach to achieve reusability of electronic modules. IEEE International Symposium on Electronics and the Environment, New York 1994;331–336.

[57] Klausner M, Grimm M, Hendrickson C. Horvath A., Sensor-based data recording of use conditions for product take-back. IEEE International Symposium on Electronics and the Environment, New York 1998:138–143.

[58] Klausner M, Grimm W, Hendrickson C. Reuse of electric motors in consumer products. Journal of Ecology 1998; 2(2): 89–102.

[59] Simon M, Graham B, Moore P, JunSheng P, Changwen X. Life cycle data acquisition unit – Design, implementation, economics and environmental benefits. IEEE International Symposium on Electronics and the Environment, Piscataway, NJ 2000; 284–289.

[60] Middendorf A, Griese H, Reichl H, Grimm W. Using Life-cycle information for reliability assessment of electronic assemblies. IEEE International Integrated Reliability Workshop, Final Report, Piscataway, NJ 2002; 176–179.

68

RAMS Management of Railway Tracks

Narve Lyngby, Per Hokstad, and Jørn Vatn

Department of Production and Quality Engineering
The Norwegian University of Science and Technology
N-7491 Trondheim, Norway

Abstract: This chapter provides a review of ageing/degradation models relevant for railway tracks. Recent models for maintenance/renewal optimization used in railways will also be presented. Further, some of the methods/techniques are applied in a few case studies, using actual data. Finally some future trends are outlined.

68.1 Introduction

In the past, railway maintenance procedures were traditionally planned based on the knowledge and experience of each company, accumulated over many decades of operation, but without any kind of reliability-based or risk-based approaches. With the major goal of providing a high level of safety to the infrastructures there was not much concern over economical issues [29].

However, nowadays, limitations in budget are forcing railway infrastructure managers to reduce operational expenditure. Therefore, efforts are being made to apply reliability-based and risk-informed approaches for the maintenance optimization of railway infrastructures. The underlying idea is to reduce the operation and maintenance expenditures while still assuring high safety standards [29].

Optimizing maintenance involves an estimation of the degradation of an object or a system and the consequence of this degradation, often in form of cost.

Having knowledge about the degradation, we can estimate when measures are necessary, when a life span reaches its technical and/or economic end, *etc*. Only by estimating these figures correctly, can accurate life cycles, including all maintenance work to be carried out throughout the useful life, be drawn. Especially the possibility of predicting the residual lifetime of any asset is of high importance.

The consequence of degradation affects safety and operational expenditures as well as speed limitations and corrective maintenance actions.

68.2 Railway Tracks

After the Second World War, the national railway companies used designs of their own. Later, international standards were adopted that often implied heavier rails: UIC54 rails and in many countries today, UIC 60 rails [25]. Instead of

jointed rails, continuous welded rails (CWR) became the new standard, which resulted in greater passenger comfort and less maintenance. Improvements to the rails were complemented with innovations in the design of sleepers, fastening sections, and ballast beds.

In addition to these gradual improvements, completely modified track types have also been developed. Firstly, new ballast track sections have recently become available; these have a different sleeper design than conventional ballasted tracks. In Germany a wide-sleeper track has been developed, where the weight of the sleepers themselves has doubled, but the pressure on the ballast bed has been almost halved as a result of the new shape, resulting in considerably less (geometric) maintenance [30]. In Austria a frame sleeper track has been developed, where a longitudinal beam has been added to the traditional sleeper concept. Subsidence has been reduced by two-thirds, thanks to the more continuous support of the rails [31]. In addition, considerable technological progress has also been made in the development of ballast-less track sections that replace ballast by concrete or asphalt beds (slab-tracks).

However, the most common type of railway track is the ballasted railway track. Figure 68.1 shows a ballasted railway track consisting of rails and sleepers, laid in and fixed by ballast on an existing sub-grade. This economic design, which was chosen on the basis of experience, has remained virtually unchanged despite technological developments in the components. Tracks are long, large structures stretching hundreds or thousands of kilometers. In addition to its economical benefits, the design is a rational structure for supporting heavy fast trains on soft ground.

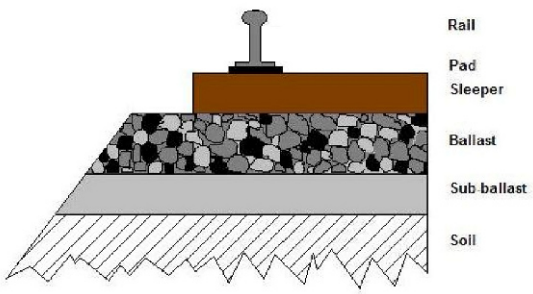


Figure 68.1. Configuration of a railway track

Rails are longitudinal steel members that guide and support the train wheels, and transfer concentrated wheel loads to the supporting sleepers spaced evenly along its length. The rails are held to the sleepers with steel fasteners that ensure that they do not move vertically, longitudinally, or laterally. Tracks with concrete sleepers have a rubber pad placed between the rail and the sleeper in order to reduce the peak forces from the rails onto the sleepers [6]. The sleepers provide a solid, even and flat platform for the rails, and form the basis of a rail fastening section. They hold the rails in position and maintain the designed rail gauge. Sleepers are laid on top of compacted ballast layer at a distance of typically 60–70 cm. Sleepers receive concentrated vertical, lateral, and longitudinal loads from the wheels and rails, and distribute them over a wider ballast area to decrease the stress to an acceptable level [6]. The ballast transmits these vertical forces into the sub-grade [7]. The secondary function of the ballast is to give the track a good lateral stability. The lateral strength of a railway track is to a large extent defined by ballast lateral resistance. After maintenance and renewal actions of the ballast layer, the ballast particles are not consolidated well enough, and lateral resistance is low. This means that the geometrical settlement of the track is quite fast in the first period before the track settles.

Sub-ballast is a layer of aggregates between the ballast layer and the sub-grade, and is usually comprised of well-graded crushed rock or sand/gravel mixtures. It prevents penetration of ballast grains into the sub-grade, and also prevents upward migration of fines into the ballast layer. Sub-ballast, therefore, acts as a filter and separating layer in the track sub-structure, transmits and distributes stress from the ballast layer down to the sub-grade over a wider area, and acts as a limited drainage medium.

Sub-grade is the ground where rail track structure is constructed. It may be naturally deposited sub-grade or specially placed fill material. The sub-grade must be stiff and have a sufficient bearing capacity to resist traffic induced stresses at the sub-ballast/sub-grade interface.

Instability or failure of the sub-grade will result in an unacceptable distortion of the track geometry and alignment, even with excellent ballast and sub-ballast layers.

In addition, the track consists of a drainage section (sub-drain, trench, *etc*.) to avoid moisture problems in the track. Moisture in the track is by many regarded as the main parameter affecting the degradation progression, and is therefore a very important asset to consider in the optimization of maintenance.

68.2.1 Railway Track Degradation

A railway track degrades even if it is not in use or maintained [24]. This is visible on disused railway tracks where the vegetation has taken over. The vegetation is forcing its way from the side of the track to finally cover the track completely. This natural degradation is slower on tracks with traffic, but will still make a contribution to the overall degradation. Vegetation and remnants of vegetation bind up moisture, which can lead to freezing and worsen the stability of the track.

Together with this natural degradation, the traffic contributes to the degradation of the track. Forces from trains passing put stress on the railway track components. The whole track degrades at the same time, but the different maintenance points degrade at different rates [24].

It would be too great of a task to describe the degradation of all railway track components and their interaction in this chapter. Instead, a description of the settlement of tracks and the degradation of rails is given in a few words. These degradation processes will later be used as examples in some case studies on RAMS.

68.2.1.1 Track Settlement

Trains subject the track structure to repeated loading and unloading as they pass. Each load–unload cycle causes deformation of the track, part of which is elastic and recovers; while part suffers permanent deformation.

Track settlement is an integrated process in which settlement of one component affects that of another. As soon as the track geometry starts to deteriorate, the variations of the train/track interaction forces increase, and this speeds up the track deterioration process. According to Dahlberg [2] track settlement occurs in two major phases. Directly after a major maintenance action of the ballast the settlement is relatively fast until the gaps between the ballast particles have been reduced and the ballast is consolidated. The second phase of settlement is slower and is caused by several basic mechanisms of ballast and sub-grade behavior, for example, continued volume reduction, *i.e.*, densification caused by particle rearrangement, sub-ballast and/or sub-grade penetration into ballast voids, volume reduction caused by particle breakdown, volume reduction caused by abrasive wear, inelastic recovery on unloading due to micro-slip between ballast particles, movement of ballast and sub-grade particles, and so on.

Measurement of track geometry irregularities is the most used automated condition monitoring technique in railway infrastructure maintenance. Most problems with tracks (at least the ones concerning the ballast and sub-structure) are revealed as track geometry irregularities [1].

68.2.1.2 Rail Degradation

Rail degradation is basically due to wear and fatigue [12]. These mechanisms vary in strength depending on the track load. In this respect, the track curvature has a major influence on the following relationships of degradation:

- narrow curves implies wear,
- tangent track implies fatigue.

This is shown as a plot in Figure 68.2.

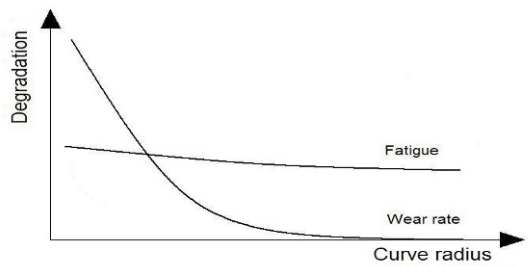


Figure 68.2. Wear and fatigue mechanisms as a function of curve radii. The degradation index corresponds to a relative degradation rate [12]

Wear occurs due to interaction of rail and wheel. It includes abrasive wear and adhesive wear. Adhesive wear is predominant in curves and dry conditions [14]. Abrasive wear is observed at the wheel tread and rail crown, and adhesive wear is observed at the wheel flange and gauge face.

In order to reduce the rate of wear, wheels and rail are lubricated. Lubrication helps to reduce rail gauge face wear and reduces energy or fuel consumption along with noise reduction [13]. In other words; lubrication is good economy.

Rail fatigue accounted for about 60% of defects found by East Japan Railways in the late 1990s, while in France (SNCF) and UK (Railtrack) the figures were about 25% and 15%, respectively. Fatigue is a major future concern as business demands for higher speed; higher axle loads, higher traffic density, and higher tractive forces increase [13].

Effective ways to reduce the initiation and propagation of fatigue failures is an important field of research, see [15][16][17][18][20]. Lubrication reduces the wear rate and damage to the rails but on the other hand, it also causes fluid entrapment in cracks, which leads to crack pressurization and reduces the crack face friction that allows relative shear of the crack faces. This accelerates crack propagation. The presence of manufacturing defects in the rail sub-surface and the direction of the crack mouth on the rail surface are both responsible for guiding the direction of crack development [32][33]. The presence of water or snow on the rails may also increase the crack propagation rate. When these minute head checks are filled with water or lubricants they do not dry up easily. During wheel rail contact, these liquids become trapped in the crack cavities and build up very high localized pressure, which may even be greater than the compressive stress. If head checks are in the direction of train traffic, crack growth takes place due to liquid entrapment, but when head checks are in the opposite direction to train traffic, the liquid is forced out before it is entrapped..

68.2.2 Inspections and Interventions

Maintenance of railway tracks includes inspections and interventions. With the inspections, infra-structure managers employ various methods to obtain information about the tracks. These methods are complementary and provide a wealth of information for maintenance planning, as well as ensuring track safety.

68.2.2.1 Inspections

The inspection methods used on railway tracks include both manual and automated methods. Visual inspection is a much used method. To accomplish this, a trained inspector walks the track or rides on a slow moving track vehicle and looks for track problems. However, many rail defects cannot be seen with the naked eye, hence other methods must be utilized to supplement the visual process. Special equipment travelling over the rails that incorporates ultrasonic or inductive methods for detecting those internal, small, and otherwise not visible defects is then used. Track geometry problems such as variations in track gage, cross level, twist, profile, and alignment can be measured manually with the use of hand devices, but it is a time consuming process. More efficient is a vehicle that continuously measures the track geometry as it travels along the track. Most of these vehicles use laser measurements or accelerometers. Laser measurement can also generate transverse rail profiles. These profiles can be used to measure wear or identify areas of plastic flow.

68.2.2.2 Interventions

Intervention is here used as actions carried out to improve the quality of an asset, including both maintenance (preventive and corrective) and renewal actions. There are different types of interventions ordered by data from inspections or at fixed intervals, such as; tamping, grinding, track lifting, ballast cleaning, rail renewal, sleeper renewal, *etc*. Some of the interventions that are more important for permanent railway track are described below.

Tamping is the common term for the operation of lining, leveling, and tamping, since it is performed by the same machine. The maintenance action is performed by lifting the track and literally squeezing the ballast beneath the sleeper to fill the void spaces generated by the lifting operation.

Tamping is an effective process for re-adjusting the track geometry [10]. However, some detrimental effects, such as ballast damage, loosening of the ballast bed, and reduced track resistance accompany it. Loosening of ballast by the tamping process causes high settlement in the track. Tamping is eventually needed again over a shorter period of time, and in the long run, ballast gradually becomes contaminated by fines, which impairs drainage and its ability to hold the track geometry. Eventually fouled ballast will need to be replaced, or cleaned and re-used in the track [10].

The ballast layer can be fouled due to ballast breakdown, infiltration from the ballast surface, sleeper wear, infiltration from the underlying granular layers, and sub-grade infiltration. This will affect the bearing capacity of the ballast bed and the drainage function, which in turn will cause the ballast to function less effectively. A ballast cleaner removes the fouled ballast and put the cleaned ballast back in the track.

Grinding has been undertaken for many years to maintain rail to increase rail life. Rail grinding objectives have included the removal of corrugation (undulations on the rail surface that increase dynamic forces), the removal of rail surface damage (which also improves ultrasonic inspection), and rail re-profiling to improve vehicle steering. In the last two decades increasing emphasis has been given to grinding to remove cracks produced by rolling contact fatigue (RCF). Such cracks form on almost all railways, from transit sections to high-speed passenger railway s and heavy-haul freight railways. While much theoretical and experimental work is in progress to understand RCF; most railways see grinding as the only tool that is currently available to control the development of small cracks into significant defects.

68.3 Degradation Modeling

So far, we have described the railway track and its, degradation briefly. However, moving on to the realm of modeling, it may be helpful to start looking at the railway track from the point of view of reliability. This stochastic point of view will also form the basis in the maintenance optimization described later.

68.3.1 Stochastic Modeling

The track is considered to be reliable when it performs its intended function under operating conditions for a specified period of time. When this is not the case, the track "fails". The probability that the track will fail in a small time interval from time t to $t + \Delta t$, given that the item has survived up to time t, is called the hazard rate. The concept of the hazard rate is involved in most methods and approaches to maintenance analysis [34]. The hazard rate function can have several behaviors. As far as the railway is concerned, the most likely character is the so-called bath tub curve, as shown in Figure 68.3.

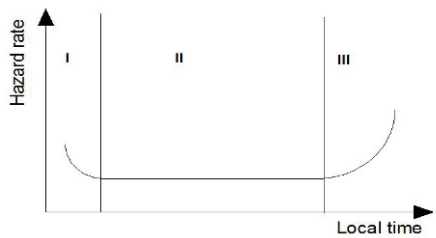


Figure 68.3. Bathtub curve with a local time-dependent hazard rate

As illustrated in Figure 68.3, the bathtub curve may be divided into three phases:

I. Infant mortality (infancy) period.
II. Useful life period.
III. Wear-out period.

During the early life of an item (I), there are early failures caused by initial weakness or defects in material, poor quality control, inadequate manufacturing methods, human error, initial settlement, *etc*. Early failures show up early in the life of an item and are characterized by a high failure rate in the beginning, which keeps decreasing as time elapses. Other terms for this decreasing failure rate period are the burn-in period, the break-in period, the early failure period, the wear-in period, and the debugging period.

During the second part of the bathtub curve (II), the hazard rate is approximately constant. This period of life is known as the useful life during which only random failures occur. There are various reasons for the occurrence of failures in this period, for example, power surges, temperature fluctuations, human errors, overloading, earthquakes, *etc*. Screening techniques or maintenance practices cannot eliminate these failures, but by making the design of the item more robust with respect to the environments, the effects can be reduced.

After the useful life the wear-out period starts (III), when the failure rate increases. The causes for these "wear-out" failures include wear due to aging, fatigue cracking, corrosion and creep, short designed-in life of the maintenance point under consideration, poor maintenance, wear due to friction, and incorrect overhaul practices.

In Figure 68.3, the word "local time" is used to emphasize the fact that time is relative to the last failure. The bathtub curve indicates that the number of failures will be reduced if an item is maintained before it reaches the right extreme of the curve.

There is also another bathtub curve related to the global section time, as shown in Figure 68.4, where the local bathtub curves are also illustrated.

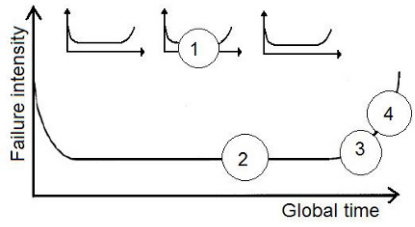


Figure 68.4. Bathtub curve with a global time-dependent failure intensity [34]

Note that on the *y*-axis the dimension is *failure intensity, or performance loss.* This reflects that the important issue now is the number of failures (overall degradation) *per* time unit, or generally loss of performance, independent of what has happened up to time *t*.

In Figure 68.4 the numbers 1, 2, 3, and 4 are identified, where the following maintenance situations apply:

1. Point maintenance, related to the explicit failure modes of a maintenance point.
2. Life extension maintenance. The idea here is to carry out maintenance that prolongs the life length of the section. A typical example is rail grinding to extend the life length of rails.
3. Maintenance carried out in order to improve performance, but not renewal. A typical example is adding ballast to pumping sections to improve track quality and reduce the need for track adjustment
4. Complete renewal of major railway maintenance points or sections.

Transferring this theory to railway track maintenance, the following distinguish between local curves as failures within maintenance points and global curves as failures in sections. Here maintenance points are defined as points along the track susceptible to inspection and/or interventions, whereas sections are longer parts of track, often with defined parameter values.

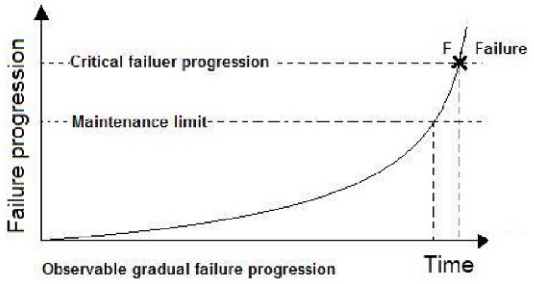
68.3.2 Degradation in Local Time

As mentioned; the bathtub curve indicates a wear-out zone. However, the shapes of the degradation in this wear-out zone differ depending on which maintenance point that is observed.

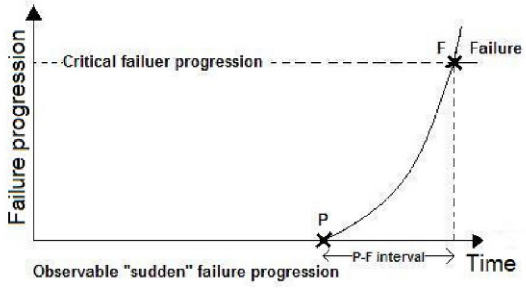
Vatn [34] has classified different failure classes related to the characteristics of maintenance point degradation:

a. gradual failure progression, and
b. "sudden" failure progression.

In addition to these failure models, Vatn described two models where the failure progression is not observable for some reason. These models are not included here, as it is expected that it will be possible to observe the failure progression for all maintenance points of the railway track.



(a)



(b)

Figure 68.5. Two different failure models

The two different classes of failures are illustrated in Figure 68.5.

a. Observable Gradual Failure Progression

With gradual failure progression, it is assumed that the progression of failure can be observed. The geometrical degradation of a railway track is a typical example. In order to ensure full capacity of the track, the geometrical deviations must be below a certain limit. If we exceed this limit, action must be taken in the form of speed restrictions or a full stopping of the line. A failure occurs when the geometrical deviation exceeds a specified limit.

b. Observable "Sudden" Failure Progression (PF Interval)

Now assume that the track section can operate for a very long time without any sign of potential failure, but at some point of time a potential failure would be evident. In Figure 68.5(a) "P" indicates potential failure, *i.e.*, the time where an impending failure is observable. The time interval before the failure is first observable, and the time until a failure occurs is very often denoted the PF interval. In practical terms, then, the PF interval is the grace time available to detect the presence of a defect before it causes the actual failure.

An example of this is a rail that is exposed to a combination of fatigue and a flat wheel that initiates a crack (potential failure, P). However, such cracks can be detected by ultrasonic inspection, and hopefully so before the crack propagates to a failure.

68.3.3 Degradation of Sections

When we look at the sections, the life spans changes along with the consideration of the degraded state. From a life span of one to five years for maintenance points, we now consider the whole section implying a life span of 30 to 60 years. While considering a section, the overall degradation must be considered. This implies a change from following the degradation of one maintenance point until failure to a number of failures, *e.g.,* loss of performance or quality.

The challenge in looking at sections lies in the consideration of many factors that eventually lead to the degradation. Underlying degradation processes of maintenance points together with changing effect of maintenance carried out within the life span are considered. Zoeteman [35] refers to a figure by Ebershon and Ruppert [22] (Figure 68.6), visualizing the problem and showing a theoretical degradation for the geometry of a railway track. The track roughness increases with the amount of time/tonnage carried. At some point, intervention is needed. The broken lines show that replacing the track can be postponed through tamping. After some time the effectiveness of this maintenance may become inadequate, which is reflected in a decreased interval. Replacement becomes necessary before the track condition passes the "operational limit" when the safety of traffic may be at stake. Figure 68.6 also shows an entirely different option, which is to upgrade the section, *e.g.,* with an improved ballast bed; the reduced amount of maintenance and extended life should be traded off against this investment.

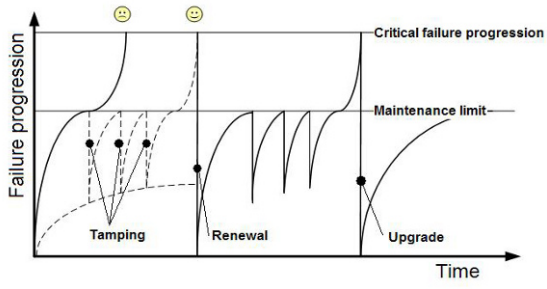


Figure 68.6. Degradation of track geometry [22]

Degradation is a complicated process. The rate at which the degradation occurs is a function of time and/or usage intensity. If all railway track sections were identical, operated under exactly the same conditions and in exactly the same environment, then, all sections would degrade in the exact same manner. However, usage intensity or operating conditions together with environmental conditions, and material varies between sections.

Several attempts have been made to make empirical models based on records or measurements made on tracks to explain the complicated degradation process.

Four models explaining track settlement are presented as examples:

1. An empirical track settlement model based on Japanese experience [11].
2. A statistical deterioration model made by the Office for Research and Experiments of the International Union of Railways (ORE).
3. A series of equations predicting settlement rate from ballast pressure based on experiments at the Technical University of Munich [3].
4. An Austrian model looking at development of track quality from a passenger's point of view.

The degradation process is explained in these models through a set of variables, which more or less remain the same for various models. The most important variables according to the Japanese model [11] are traffic, time, track condition, and humidity. This choice of variables is supported by the German and the Austrian models with some deviations; the German and Austrian models do not consider humidity, however both models regard vehicle characteristics as an important variable. The UIC model [2] contains no track parameters but only loading parameters such as traffic volume, dynamic axle load, and speed.

As can be seen from these models, the settlement is modeled quite differently, even though the variables used are more or less the same. In the models from Japan and ORE, the settlement grows linearly with respect to the loading, whereas in the German model the settlement grows only logarithmically with respect to loading [the term containing log (N)]. The discrepancy between the two models might be large, especially if the parameters in the equations are determined for a relatively small number of loading cycles and the equations are thereafter used to determine the settlement after a large number of loading cycles. The difference is even larger comparing the German model to the Austrian one, which is proclaims an exponential development of the settlement. Instead of saying that the sub-grade and ballast are more compact over time (that it settles), which in turn slows the settlement, the Austrian model says that the rougher the track becomes the more dynamic forces are created when trains pass, which in turn increases the settlement.

68.3.3.1 The Japanese Study

In early 1960, the Japanese railway companies published a relationship that enables an estimation of the settlement of railway ballast when subjected to cyclic loading. Originally developed from laboratory results, the following equation is currently used to estimate the deformation, y, of both the heavy haul narrow gauge and the high standard gauge:

$$y = \gamma\left(1 - e^{-\alpha x}\right) + \beta x\,, \qquad (68.1)$$

where x is the repeated number of loadings or tonnage carried by the track, α is the vertical acceleration required to initiate slip and can be measured using spring loaded plates of the ballast material on a vibrating table, β is a coefficient proportional to the sleeper pressure and peak acceleration experienced by the ballast particles

and is affected by the type and condition of the ballast material and the presence of water, and γ is a constant dependent on the initial packing of the ballast material.

68.3.3.2 The Heavy Axle Load Study (ORE)

ORE has suggested a model to estimate track deterioration, e [8]. The deterioration is divided into two parts: the first part describes the deterioration directly after tamping, e_0, and the second part describes the deterioration depending on traffic volume T, dynamic axle load $2Q$ and speed v. The relationship reads

$$e = e_0 + hT^{\alpha}(2Q)^{\beta}v^{\gamma}, \qquad (68.2)$$

where h is a constant and the parameters α, β, and γ have to be estimated from experimental data. Due to a lack of data, UIC suggests α=1 and β=3. Further, it is assumed that the influence of the speed can be neglected, implying that v^{γ} need not be treated separately, but may be included in the proportionality factor h.

68.3.3.3 The German Study

Experiments under well controlled laboratory conditions at the Technical University of Munich representative of vehicles passing a dipped joint have been used to establish equations to calculate rate of settlement (S) [3]. The ballast pressure is multiplied by the log of the number of axle passes as follows:

$$S = a \times p \times \ln \Delta N + b \times p^{1.21} \times \ln N \quad , (68.3)$$

As can be seen from the equation a logarithmic settlement law has been used. The first term represents the fast settlement just after a maintenance action. ΔN expresses a pre-loading period comprising the first passing axles. ΔN should be ≤ 10000 and N in the second part should express the total number of passing axles. The ballast pressure p should be calculated with the Zimmermann method [3]. The parameters a and b are constants suggested to be in the value range; 1.57–2.33 (a) and 3.04–15.2 (b).

68.3.3.4 The Austrian Study

TU Graz has examined settlement developments in Austria by the quality figure MDZ, which represents accelerations in the vehicle caused by track imperfections [9]. The MDZ figure comprises of both horizontal and vertical deviations in tracks together with a lack of super elevation and speed [5]. An exponential development of the MDZ figure over time was found giving the following expression for track quality:

$$Q = Q_0 \times e^{-b \times t}, \qquad (68.4)$$

where Q is the track quality represented by the MDZ number and Q_0 the initial track quality. TU Graz has also examined the assets management problem [4].

68.4 Methods for Optimizing Maintenance and Renewal

Using the models of degradation as the basis, the maintenance in form of inspection and intervention intervals can be optimized with respect to the total cost of maintenance and risk.

68.4.1 Optimizing Point Maintenance

In the degradation models, a limit called “critical failure progression” is defined. This is a limit saying that degradation passing this limit is assumed to be critical. However, in real life there often exists more than just one level. In the Norwegian rail administration there are three limits. A maintenance limit (ML) indicates further investigation, an action limit (AL) says that maintenance is required, and finally operational restriction and maintenance is mandatory when passing a safety limit (SL).

The failure progression is a random variable. When the failure progression exceeds the maintenance limit a corrective maintenance action is performed, which resets the section. If the failure progression exceeds the failure limit a failure occurs. The failure progress can be specified in various ways. Two common used models for the failure progression are the Wiener process and the

Gamma process. Both processes are continuous-time stochastic processes.

A limitation of these processes is that the degradation is assumed to be linear with time. This is problematic when, *e.g.*, cracks are modeled, since the failure progression is believed to go faster and faster as the crack size increases.

Yet another limitation is the assumption of independence, which is often used in reliability analysis. It means that if one maintenance point in a section fails and is repaired, all the other maintenance points in the section will function as normal without regard to the repair going on. For many sections this assumption will be unrealistic, and other approaches have to be used to determine the section availability. An alternative approach is to base the analysis on Markov models. By using Markov models a wide range of dependencies can be taken into account. [21].

Another important method used within the railway industry is Monte Carlo simulation. The simulation is carried out by generating certain random and discrete events in a computer model in order to create a realistic or "typical lifetime scenario of the section. In the Monte Carlo approach a realization of the life process is simulated on the computer and, after having observed the simulated process for some time, estimates are made of the desired measures of performance, thus the simulation is treated as a series of real experiments. Simulation is an attractive alternative because it allows the modeling of virtually any time to failure distribution, as well as allowing behaviors that preclude analytic solution. Further, simulation may be a more efficient approach in complex sections where it would be to time consuming to develop analytical models. The major disadvantage of simulation is the long simulation times needed to achieve high accuracy. In addition, in many situations, a sort of "black box" with little insight in the processes going on will be created.

68.4.1.1 Barrier Modeling

A risk model with a format that allows the prediction the risk level as a function of the maintenance level is a useful tool when calculating costs. An example of such a model is the barrier model, which looks at the outcome in term of cost if barriers in connection with the maintenance point should fail. A barrier is defined as that part of a section that prevents the occurrence, or at least lowers the occurrence probability to a minimum, of the so called "top-event", if a maintenance point fails. A "top-event" describes the worst direct consequence of any failure. Normally there is more than one barrier preventing the occurrence of the 'top-event'. The idea of barrier thinking is illustrated in Figure 68.7, where the case of crack growth in rails is illustrated:

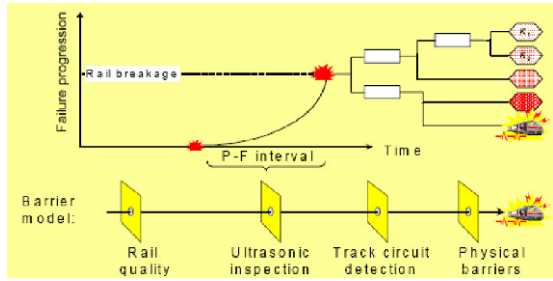


Figure 68.7. Barrier modeling, printout from [34]

It is only because of the existence of these barriers, that railways can be run in the way they are. Up to now for most maintenance points the existing barriers have been defined, but their influence is only estimated. It will take a lot of further work to calculate their true factors explicitly. Still, it is regarded as most important to integrate those barriers in the calculations, because it is always better to take facts that obviously exist into account even if the exact figures are not known, than not to include any value.

68.4.1.2 Cost Analysis

In order to optimize the maintenance effort, the maintenance point performance measures and the cost model must be combined, and then balance with the maintenance cost. The maintenance cost is specified by:

PM_{Cost}	Cost *per* preventive maintenance (PM) activity (intervention).
I_{Cost}	Cost per inspection.
CM_{Cost}	Cost per corrective maintenance

(CM) action.

The cost *per* unit time is now given by:

$$C(\tau) = C_R(\tau) + [1/\tau_{Int} + rr(\tau)]PM_{Cost}, \\ + I_{Cost}/\tau_{Insp} + \lambda(\tau)CM_{Cost}, \quad (68.5)$$

where $C_R(\tau)$ are costs calculated from risk model. $\lambda(\tau)$ and $rr(\tau)$ are the effective failure rate and the renewal rate, respectively. In the equation τ_{Int} is used to denote the maintenance interval in case of interventions, whereas τ_{Insp} denotes the maintenance interval in the case of periodic inspections. Further τ is used without any index when the interval must be found from the type of maintenance activity. To find the optimum maintenance interval $C(\tau)$ from the equation for various values of the maintenance interval, τ, can be calculated and then the value for τ that minimizes $C(\tau)$ can be chosen. The output of such an optimization task can also be plotted in a diagram as illustrated by Figure 68.8.

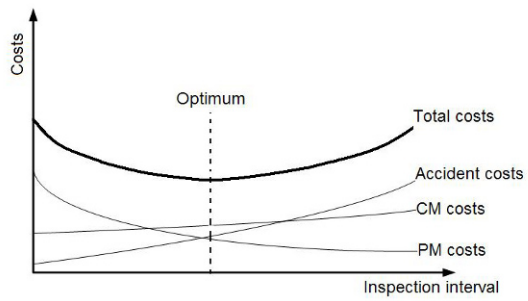


Figure 68.8. Optimization of maintenance intervals

Here the cost of corrective maintenance as a consequence of failures is measured upon the cost of preventive maintenance.

68.4.2 Optimizing Section Maintenance and Renewal

Here the objective is to establish a sound basis for the optimization of maintenance and renewal. The idea is to choose maintenance activities in time and space such that costs are minimized in the long run. Different "headings" are used for such an analysis, *e.g.*, LCC analysis, cost/benefit analysis and NPV (net present value) analysis.

As in the latter approaches, the degradation as a function of time is the background of this approach as well. This degradation can be transformed into cost functions, and when the cost becomes very large it might be beneficial to perform maintenance or renewal activities on the infrastructure. In the following, the notation $c(t)$ is introduced for the costs as a function of time. The costs included in this function mainly include

- punctuality loss,
- accident cost, and
- extra operational and maintenance costs due to reduced track quality.

By a maintenance or renewal action the function *c(t)* is typically reset, either to zero, or at least a level significantly below the current value. Thus, the operating costs will be reduced in the future if investments in a maintenance or renewal project are made.

Figure 68.9 shows the savings in operational costs, $c(t) - c^*(t)$, if maintenance or renewal at time T is performed. In addition to the savings in operational costs, savings due to an increased "residual life time" will also often be achieved.

Special attention will be paid to projects that aim at extending the life length of a railway section. A typical example is rail grinding to extend the life length of the rail, but also for the fastenings, sleepers, and ballast. Figure 68.10 shows how a smart activity ( ) may suppress the increase in *c(t)* and thereby extend the point of time before the cost explodes and a renewal is necessary.

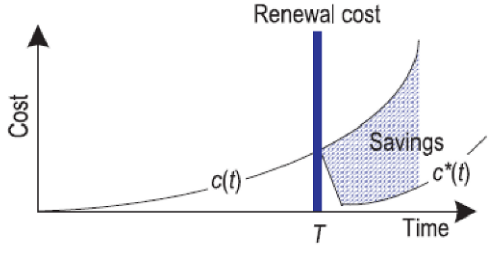


Figure 68.9. Cost savings [34]

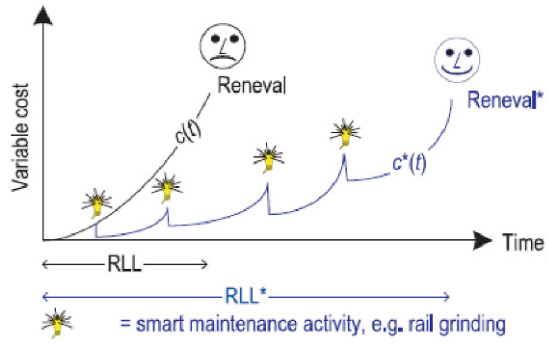


Figure 68.10. Life length extension [34]

Following this line of argument, from a cost-benefit point of view, all projects with a cost–benefit ratio higher than or equal to one should be carried out. The challenge lies in finding the optimal time to carry out the project. However, due to a lack of financial resources and insufficient work capacity, the infrastructure managers might have to drop some of the projects. A tool design to help prioritizing projects, *i.e*, the Norwegian PRIFO tool has been conceived. Figure 68.11 illustrates the output of the PRIFO tool.

Project Nr.	Rating	Cost/Benefit Ratio	
Project 5	1	6,4	
Project 3	2	6,2	
Project 12	3	5,4	Projects are supposed to be run
Project 11	4	5,1	
Project 1	5	4,3	
Project 7	6	3,4	
Project 2	7	3,2	limit line due to financial restrictions
Project 13	8	2,8	
Project 4	9	1,5	Economic, but not executed projects
Project 9	10	1,2	
Project 7	11	1	economic limit line
Project 10	12	0,8	Projects should never be run
Project 8	13	0,5	

Figure 68.11. Ranking of projects, printout of the PRIFO tool

The results of the PRIFO tool are supposed to be listed and rated according to their cost–benefit ratio. The higher this figure is, the more economically beneficial is the assessed project.

68.5 Case Studies on RAMS

Examples of optimization of inspection intervals for the ultrasonic inspection car and the geometrical inspection car are presented in two cases.

68.5.1 Optimizing Ultrasonic Inspection Intervals

68.5.1.1 Introduction

Failure and inspection data from *Dovrebanen* (a part of the Norwegian railway line from Trondheim to Oslo) are analyzed. The degradation/repair process within the fixed inspection interval is modeled as a time continuous Markov chain. Also the change of state implemented at the end of an inspection interval is modeled as a (time discrete) Markov chain.

The model will demonstrate how reliability depends on the inspection interval, and will thus support identification of the most cost effective preventive maintenance strategy for the railway line in question.

The critical failures (*i.e.*, the broken rail) can either be seen as shocks (*i.e.*, with no "warning"), or as a gradual degradation, where the line goes through various degraded states (with cracks) until it gets a critical failure. When a degraded failure occurs, the railway line is still functioning, and the crack can only be revealed by inspections of the line. Those inspections are performed at regular intervals by ultrasonic inspection cars (UIC). However, at each inspection there is only a probability q of detecting a degraded failure. A piece of rail that is degraded is more prone to suffer a critical failure than a piece of rail that is not degraded (*i.e.*, in the OK state). When a critical failure occurs, the failure has to be repaired in order to maintain regular traffic. More details are given in [26], and we note that the same data has also been analyzed in [27].

68.5.1.2 A General Markov Failure Model

A phase type distribution is used for time to failure. The failure model includes two different states for degraded failures and two different states for critical failures. In addition we have an OK state (see Figure 68.12).

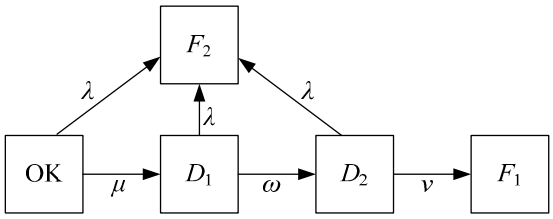


Figure 68.12. A general Markov failure model

The critical failures can be divided into two categories: failures due to degradation, denoted F_1 and "shock" failures, denoted F_2. The latter failures happen when the rail is exposed to large external forces like rolling stock. Those failures cannot be avoided by inspection. The critical failures due to degradation, however, can be avoided by preventive repair if they are discovered at inspections.

The first degraded state, denoted D_1, is for minor degraded failures (cracks). If a rail is detected to be in this state, the observations are made more frequently so that a critical failure due to degradation should not be possible. When the degraded state D_2 is detected (larger cracks) the failure is repaired immediately.

The development of degraded and critical failures is modeled by a time continuous Markov chain, see Figure 68.12. If the railway line does not have a critical failure, there is a constant rate λ for getting a shock failure F_2. In order to reach the critical failure state F_1 the rail has to go through the degraded states D_1 and D_2.

We partition the rail into small pieces of rail so that one piece is in only one of the states OK, D_1, D_2, F_1, or F_2, (and the above rates refer to these small pieces with the length of 1 m).

68.5.1.3 A Specific Failure Model for the Railway Case

In the following illustrations, for simplicity we ignore the state F_2 (see Figure 68.13) . The effect of this failure category can afterwards be incorporated by just adding an additional failure rate, λ (see Figure 68.12).

However, in order to later also model the maintenance of the degradation failures, we split the degradation states, according to whether these are detected or not. A subscript *u* on the degraded states indicates that a degraded failure is undetected (by UIC). Likewise, a subscript *d* indicates a degraded failure that is detected. Thus, at the beginning of an inspection interval, we can start in one of the states OK, D_{1u}, or D_{2u} D_{1d}. The Markov diagram is presented in Figure 68.13, which is valid for the complete inspection interval of length *T*. Note that if we during the inspection detect that the line is in the state D_1, then the next inspection interval will start in state D_{1d}. Here ρ refers to the transition rate caused by additional inspection in a detected state D_1 as explained above.

D_{1u} = Minor degraded failure (crack) being undetected.

D_{1d} = Minor degraded failure detected by UIC; then the observations are made more intensive (frequent) so that a critical failure due to degradation is not possible.

D_{2u} = Major degraded failure (crack) being undetected; (state believed to be OK).

D_{2d} = Undetected major degraded failure when the piece of line earlier has been detected to be in state D_1; and is therefore it is closely monitored, but it is *not* known that the state D_2 is reached. As soon as the state D_2 is detected the failure is repaired immediately and the piece of rail goes to OK.

The direct rate to OK follows by the assumption of immediate repair. For simplicity, we introduce an absorbing state OK*, and transfer to OK is carried out at the start of the next inspection interval. Thus both the states F_1 and OK* are made absorbing states in the time continuous chain, meaning that a fresh start in OK always takes place at the beginning of an interval. This means that the same piece of rail can never have two failures or visits to D_{2u} within the same interval, and we do not *start* in OK in the middle of an interval. This is a computationally simplifying assumption that will not affect our results to a great extent.

Further, note that the modeling allows transitions from D_1 to D_2 to have different rates, depending on whether the degradation to D_1 is detected or not. The rate of failures (to F_1) is, however, assumed to be the same for both D_{2u} and D_{2d}.

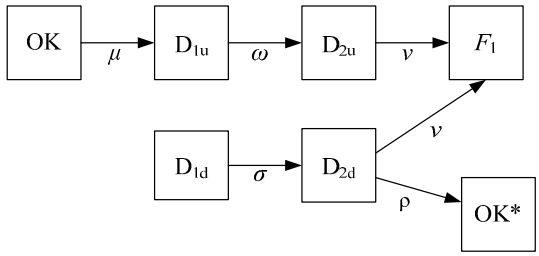


Figure 68.13. Markov model adapted to the railway case (now ignoring state F_2)

Using transition rates as in Figure 68.3, we can now easily write the intensity matrix, Q, of this time continuous Markov chain, now numbering the states as OK = 1, D_{1u} = 2, D_{1d} = 3, D_{2u} = 4, D_{2d} =5, F_1 = 6, OK* = 7. This 7x7 matrix is of the form

$$Q = \begin{bmatrix} A & K \\ 0 & 0 \end{bmatrix} \tag{68.6}$$

where A is a 5x5 matrix and the "0"s here are matrices consisting of zeros only.

Then using a suitable method for solving Markov chains, for example, the computer package Maple, we can easily find the transition probabilities of the process. Let $X_n(t)$, n=1, 2, ….., be the state of the time continuous Markov chain at time t in the nth inspection interval, and let

$$p_{jk}(t) = \mathrm{P}(X_n(t) = k \mid X_n(0) = j) \tag{68.7}$$

We denote this matrix of transition probabilities by $P(t)$ and get

$$P(t) = \begin{bmatrix} e^{tA} & A^{-1}(e^{tA} - I)K \\ 0 & I \end{bmatrix}, \tag{68.8}$$

where I is the identity matrix of appropriate dimension.

68.5.1.4 The Maintenance Model

Next we introduce the Markov chain for transitions at the inspection. The states $X_n(0)$ and $X_n(T)$ are of particular interest, where T is the length of the interval. Now consider the transitions of state that may occur as the result of the inspection (occurring at times T, $2T$, ….). In order to be able to fit the model to the failure/inspection data, we now introduce the variables U_n and V_n. U_n tells the true state for a small piece of rail immediately before inspection, and V_n tells the true state immediately after inspection, *i.e.*, at the start of the next inspection interval. Thus actually

$$U_n = X_n(T), \quad n = 1, 2, \ldots \tag{68.9}$$

$$V_n = X_{n+1}(0), \quad n = 1, 2, \ldots \tag{68.10}$$

These have the asymptotic distributions

$$\pi_k = \mathrm{P}(U_n = k); \quad k = 1, \ldots.., 7 \tag{68.11}$$

$$\psi_k = \mathrm{P}(V_n = k); \quad k = 1, \ldots, 7, \tag{68.12}$$

and the corresponding row vectors (vectors in bold) are:

$$\boldsymbol{\pi} = (\pi_1, \pi_2, \ldots\ldots.., \pi_7), \tag{68.13}$$

$$\boldsymbol{\psi} = (\psi_1, \psi_2, \ldots\ldots, \psi_7). \tag{68.14}$$

Further, we introduce probabilities that degraded failures are detected by inspection:

q_1 = Probability that state D_1 of a line segment is detected.

q_2 = Probability that a degraded failure, D_2 is detected by the inspection; not knowing in advance that the state D_1 was reached.

q_3 = Probability that a degraded failure, D_2 is detected by the inspection; knowing in advance that the state D_1 was reached.

We can then introduce the matrix, R, for the transitions at the inspections, *i.e.*, transitions from U_n to V_n.

$$R = \begin{array}{c} \begin{matrix} \text{OK} & \text{D}_{1u} & \text{D}_{1d} & \text{D}_{2u} & \text{D}_{2d} & \text{F}_1 & \text{OK*} \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1-q_1 & q_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ q_2 & 0 & 0 & 1-q_2 & 0 & 0 & 0 \\ q_3 & 0 & 0 & 0 & 1-q_3 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array} \tag{68.15}$$

Now the transition matrix for U_n equals R · P(T), and similarly the transition matrix for V_n equals

P(T) · R. Now the asymptotic distributions of U_n and V_n , are determined from the relations

$$\psi = \pi \cdot R, \quad (68.16)$$

$$\pi = \psi \cdot P(T). \quad (68.17)$$

Thus, the vector $\boldsymbol{\pi}$ is found from

$$\boldsymbol{\pi} = \boldsymbol{\pi} \cdot R \cdot P(T). \quad (68.18)$$

68.5.1.5 Overall Model and Assumptions

As indicated above the two Markov chains can be combined into one total model, see Figure 68.14. Here we give the state numbers 1, …., 7 in addition to the notation OK. *etc*., and again for simplicity we ignore the state F_2. The solid lines represent the possible transitions within an inspection interval T, (*cf.* matrix P(T)). Recall that we make the simplifying assumption that one small piece of rail can only have one visit to OK* and F_1 (and F_2) within one inspection interval. Therefore we actually treat these as absorbing states in the time continuous Markov chain, and the process always start in state OK at the beginning of the next interval.

The dotted lines of Figure 68.14 indicate transitions at the end of the test interval (*cf.* matrix R). With probability q_1 we leave D_{1u} and with probability q_2 we leave D_{2u} (thus observing state D_2 but then going directly to OK, which is the starting state at the beginning of next interval). Further, with probability q_3 we leave D_{2d} (thus actually observing D_2), and there will also be transitions from the "absorbing states" OK* and F_1 to OK.

Thus, in the total the model we have a time-continuous Markov chain in the time spans between inspections, while at the inspections we have transitions following a time discrete Markov chain.

The model and the estimation are based on some assumptions:

- The processes U_n and V_n, are assumed to be stationary processes (the actual railway line is quite old so this is a rather realistic assumption).
- The probability distributions of the time continuous processes are identical for all inspection intervals (*i.e.,* stationarity is assumed also in this respect).

Failures are equally distributed over the railway line (homogeneity). However, the estimated rates can be seen as averages for the line in question.

We treat the critically failed states as absorbing states that are also repaired at the inspections. This implies that one small piece of rail cannot fail critically twice within one inspection interval. The mean time to repair (MTTR) = 0.

68.5.1.6 Input Data

The input parameters for the estimation of model parameters are listed in Table 68.1. Degraded failures have been recorded since 1 January 1991 and had been exposed to eight tests by October 2002. Critical failures have been recorded since 1 January 1989, and assuming the same length of the test interval (T=4299/8=537 days) also for these, this implies that these have been exposed to 9.4 tests. In total 800 degraded failures were observed. For 22 of these the severity was not recorded (*i.e.* not categorized as D_1 or D_2), and these 22 failures were just distributed proportionally amongst the two categories, giving in total 331 failures of type D_1 and 469 of type D_2.

Further, 20 of the D_2 failures had already been observed in state D_1 (*i.e.* coming from state D_{1d} and are actually monitored closely). It is then assumed that the test detects the transition to D_2, and so these failures are corrected, and there is a transition back to state OK. The 449 detected failures of type D_{2u} represent transitions from D_{1u}, *i.e.*, the degradations are observed for the first time. These are a fraction q_2 of the actual number of rail

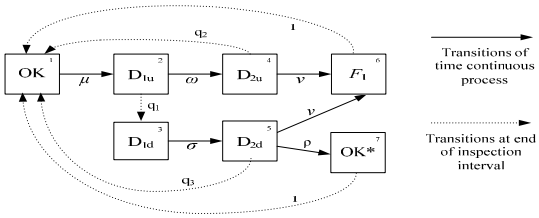


Figure 68.14. Overall failure/maintenance model, (state F_2 not included)

Table 68.1. Input data to analysis

Parameter definition	Parameter	Value
Length of rail	L	365 km = 365 000 m
Number of tests/inspections 1989–2002	n_{TF}	9.4
Number of tests/inspections 1991–2002	n_{TD}	8
Number of days, 1989–2002	N_1	5027
Number of days, 1991–2002	N_2	4299
Length of test/inspection interval	T	537 days
Number of observations in state D_1, (*i.e.*, transitions from D_{1u} to D_{1d})	N_{D1}	331
Number of observations in D_2 when it was not known that state was degraded, (*i.e.*, transitions from D_{2u})	N_{D2a}	449
Number of observations in D_2 when it was known that state was degraded, (*i.e.*, transitions from D_{1d})	N_{D2b}	20
Number of observations in F_1	N_{F1}	249
Number of observations in F_2	N_{F2}	81
Probability of detecting D_1 failure at test	q_1	0.4 (expert judgment)
Probability of detecting D_2 failure at test (state D_1 not detected previously)	q_2	0.7 (expert judgment)
Probability of detecting D_2 failure at test (state D_1 already detected)	q_3	0.9 (expert judgment)
Rate of detecting D_2 in additional inspections; (assuming on the average two additional inspections within each interval T)	ρ	$(2/T)q_3$ (exp. judgm.)

pieces in state D_{2u}, and will by the test be brought back to the state OK. The other will remain in state D_{2u}. Finally, the number of critical failures of type F_1 and F_2 are given as 249 and 81, respectively.

In order to carry out the estimation of the unknown rates some parameters must be estimated by expert judgments (operational experience). These are the probabilities q_1, q_2 and q_3, and the rate (ρ) of reaching state D_2 under additional inspections when state D_1 is detected.

68.5.1.7 Estimation

It is now quite easy to estimate the distribution of U_n under stationarity. For instance, the estimate of π_6 is given by the number of observations in F_1. The equations for π_4 and π_2 are obtained similarly. Finally, the estimated π_5 and π_7 are found from the number of detections of state D_2 given that degradation D_1 is already known. One third of these observations are assumed to be carried out at the ordinary inspections (see bottom of Table 68.1), and two thirds at the additional inspections, thus resulting in transitions to state OK*. Further, the estimate of π_3 can be obtained from the following relation:

$$\pi_3 = (\pi_2 \cdot q_1 + \pi_3) \cdot (1 - e^{-\sigma T}) . \quad (68.19)$$

The argument is that if $U_n = 3$, then either $U_{n-1} = 3$ *or* $U_{n-1} = 2$, and D_1 being detected, giving a transition from state 2 to 3, *and* in addition no transition has occurred in the last inspection interval. Finally we have the normalization equation.

Now, a joint estimation of the stationary distribution, $\boldsymbol{\pi}$, and the unknown rates (μ, ω, σ, ν),

are obtained by a recursive approach (see [26]), and we get the following estimates for the stationary probabilities π_j (for 1 m rail):

$$(\hat{\pi}_1,\hat{\pi}_2,...,\hat{\pi}_7) = (0.99935,\ 2.83\cdot10^{-4},\ 7.25\cdot10^{-5},\ 2.20\cdot10^{-4},\ 2.54\cdot10^{-6},\ 7.30\cdot10^{-5},\ 4.57\cdot10^{-6})\ . \quad (68.20)$$

Further we get the following estimated rates (*per* day):

$$\hat{\mu} = 5.9\cdot10^{-7}\ /\text{m}\ \hat{\lambda} = 4.4\cdot10^{-8}\ /\text{m}\ , \quad (68.21)$$

$$\hat{\omega} = 1.6\cdot10^{-3}\ , \quad (68.22)$$

$$\hat{\sigma} = 9.2\cdot10^{-4}\ , \quad (68.23)$$

$$\hat{\nu} = 9.3\cdot10^{-4}\ , \quad (68.24)$$

$$\hat{\rho} = 3.4\cdot10^{-3}, \quad (68.25)$$

Observe that the estimate for ρ was obtained directly from expert judgment (Table 68.1), and λ was estimated directly from the number of F_2 failures, (N_{F2}) the total number of days N_1, and the rail length, *i.e.*, $\hat{\lambda} = N_{F2}/(N_1\cdot L)$.

Further, observe that now the distribution of V_n is also found using the R-matrix ($\boldsymbol{\psi} = \boldsymbol{\pi}\cdot R$). There are five possible states at the start of a test interval $(\psi_6 = \psi_7 = 0)$ and

$$(\hat{\psi}_1,\hat{\psi}_2,.....,\hat{\psi}_5) = (0.99958,\ 1.7\cdot10^{-4},\ 1.9\cdot10^{-4},\ 6.6\cdot10^{-5},\ 2.5\cdot10^{-7}). \quad (68.26)$$

68.5.1.8 Maintenance Optimization

When the estimates of the rates $\lambda, \mu, \omega, \sigma$, and ν are established it is of interest to consider the effect of various levels of maintenance on basic reliability parameters like:

- the frequency (rate) of entries into failure states, and
- the mean time to failure.

Now introduce MTTFi = mean time to failure for failure mode i (*i.e.* F1 and F2). The rate 1/MTTF = (1/MTTF1 + 1/MTTF2) can also be referred to as the (asymptotic) rate of occurrence of failure, ROCOF1, (see [28]) when there is no maintenance. First observe that

$$\text{MTTF}_1 = (1/\mu+1/\omega+1/\nu) = 9.2 \text{ years}, \quad (68.27)$$

$$\text{MTTF}_2 = 1/\lambda = 62 \text{ years}, \quad (68.28)$$

$$\text{MTTF} = (1/\text{MTTF}_1 + 1/\text{MTTF}_2)^{-1} = 8.0 \text{ years}. \quad (68.29)$$

There are two parameters related to the maintenance that we can control:

- the length of inspection interval, T, and
- the frequency of additional inspections, (*cf.* ρ), when degradation in state D_1 is detected.

As the number of entries to the critically failed state F_2 does not change with the maintenance level, we keep focusing on the failures due to degradation. In particular, the asymptotic rate of entering F_1 and its inverse (MTTF_1) for various values of T is most interesting.

To find such entry rates we need the overall average probability of the time continuous process in various states. The probability for the process $X(t)$ to be in state k at time t equals (remember that $\psi_5 = \psi_6 = 0$):

$$p_k(t) = \sum_{j=1}^{5} \psi_j\, p_{jk}(t)\ . \quad (68.30)$$

Here $p_{jk}(t)$ are the elements of the transition matrix $P(t)$. Now the "average probability" to be in state k equals

$$p_k^* = \sum_{j=1}^{5} \psi_j\, p_{jk}^*\ , \quad (68.31)$$

where

$$p_{jk}^* = \tfrac{1}{T}\int_0^T p_{jk}(t)\,dt\ . \quad (68.32)$$

[1] Here we generally use *ROCOX* as the rate of occurrences of state X (the asymptotic rate of entering state X).

For example, the "overall" (average) probability of the time continuous process to be in state OK is found as

$$P(OK) = \psi 1 \cdot p_1^* = \psi 1 \cdot [1 - e^{-\mu T}] / (\mu \cdot T)$$

$$\approx [1 - e^{-\mu T}] / (\mu \cdot T). \quad (68.33)$$

The rate of entries into the degradation state D_1 (actually D_{1u}) is then found as

$$ROCOD_{1u} = P(OK) \cdot \mu \approx [1 - e^{-\mu T}] / T. \quad (68.34)$$

The most interesting results is obviously the rate of entries into the critical failure state F_1. We then need the probabilities to be in states D_{2u} or D_{2d}. Now,

$$P(D_{2u}) = \psi_1 \cdot p_{14}^* + \psi_2 \cdot p_{24}^* + \psi_4 \cdot p_{44}^* , \quad (68.35)$$

$$P(D_{2d}) = \psi_3 \cdot p_{35}^* + \psi_5 \cdot p_{55}^* \quad (68.36)$$

can be derived. The asymptotic rate into F1 equals

$$ROCOF_1 = [P(D_{2u}) + P(D_{2d})] \cdot \nu. \quad (68.37)$$

So for the maintained system, the asymptotic $MTTF_1 = 1/ ROCOF_1$ is given by these formulas.

Now ROCOD1u, ROCOD2u, ROCOF1 and MTTF1 are computed for a few values of T, and also for some alternative values of ρ. Table 68.2 gives the results for T=365 days and 730 days together with the actual value of the observations (T=537 days). The mean number of observations in state F1 for a time span corresponding to the actual data (*i.e.*, 5027 days) is also given. In Table 68.3 we use T = 537 days, but vary the rate ρ. The rate ρ is given as a percentage of the value used in the analyses above.

Thus, the estimated model shows, for instance, that the MTTF for critical degradation failures of 1 km length of rail decreases from 28.0 years when inspection interval is 1 year, to 14.8 years when the inspection interval is 2 years (Table 68.2). Similarly, mean number of failures is almost doubled when T increases from one year to two years. The frequency of increased inspections when a degraded failure is detected has less effect on the results (Table 68.3).

We note that the computed estimates are valid for the given line only; for another line with a

Table 68.2. Reliability parameters for various values of T

Parameter	Inspection interval T		
	365 days	537 days	730 days
$ROCOD_{1u}$ (per day and km)	$5.88 \cdot 10^{-4}$	$5.88 \cdot 10^{-4}$	$5.88 \cdot 10^{-4}$
$ROCOD_{2u}$ (per day and km)	$2.98 \cdot 10^{-4}$	$3.50 \cdot 10^{-4}$	$3.88 \cdot 10^{-4}$
$ROCOF_1$ (per day and km)	$0.98 \cdot 10^{-4}$	$1.42 \cdot 10^{-4}$	$1.85 \cdot 10^{-4}$
$MTTF_1$ for 1 km rail (years)	28.0	19.3	14.8
Mean no. of failures (in 5027 days)	180	261	339

Table 68.3. Reliability parameters for various values of ρ

ρ (rate of increased inspection by detecting state D_1)	$ROCOF_1$ (per day and km)	$MTTF_1$ for 1 km rail (years)	Mean no. of failures (in 5027 days)
25%	$1.50 \cdot 10^{-4}$	18.3	276
50%	$1.47 \cdot 10^{-4}$	18.6	270
100%	$1.42 \cdot 10^{-4}$	19.3	261
200%	$1.36 \cdot 10^{-4}$	20.1	250
400%	$1.31 \cdot 10^{-4}$	20.9	240

different state of the line and environment one would obviously obtain different estimates for the transition rates. The approach is, however, generally applicable, and the usefulness of analytic models to optimize maintenance is demonstrated.

68.5.2 Optimizing Track Maintenance

In this second case we will address the optimization of track geometry inspections on the Norwegian railway network. The critical failure is twist, and only one failure mechanisms are considered; critical failure occurs as the result of a degradation process. In addition a maintenance limit is defined. If the maintenance limit is reached, an action plan to maintain the degraded area should be planned so that the degraded area is maintained before it can lead to a derailment.

Various types of inspection and maintenance are performed on the line. Inspection by a self-propelled engine that uses three point laser sections to measure the track geometry (ROGER 1000) is carried out at regular intervals. Additional inspection will be initiated on a segment of the line with constant intervals. The degradation/repair process within the inspection interval is modeled as a time continuous Markov chain. Moreover, the change of state implemented at the end of an inspection interval is modeled as a (time discrete) Markov chain. The model is based on actual inspection data for a specific railway lines in Norway. The data are used to estimate the parameters of the model. The given failure/maintenance model and estimation technique should generally be useful for systems that experience deterioration and are subject to imperfect inspection.

68.5.2.1 Basic Model Description

This case resembles the case with broken rails with some differences. In this case, we follow the following assumptions:

- The system is subjected to a degradation process. The degradation is modeled as a Markov chain with 50 states, resembeling values of twist from 0−50 mm. The transition rates from one state to another is based on empirical data.
- The system is periodically inspected.
- The change in twist over time can be both increasing and decreasing, but with a drive towards a worsening state.
- The risk, in this case represented by the possibility of derailment, is given a value different for three parts of the rail. The possibility of a derailment is assumed different, given the same level of twist, depending on whether we have a straight line, a curvature, or a transition curve.
- PM and CM are modeled as perfect in the sense that the system is put back to initial distribution.

68.5.2.2 The Markov Chain Model

A Markov chain model a total of 50 states is introduced, each representing 1 mm in twist (Figure 68.15).

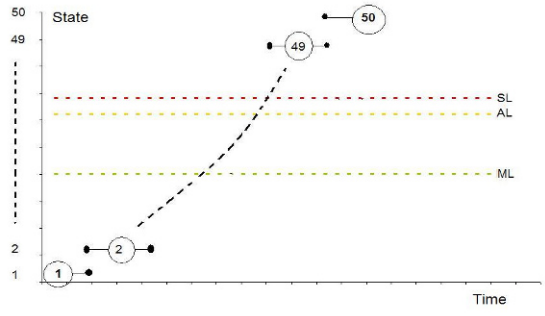


Figure 68.15. Markov state model

The next step is to find the probability that the system is in the various states as a function of time *t*. By letting $P_i(t)$ denote the probability that the system is in the state *i* at time *t*, we obtain the Markov differential equation by standard Markov considerations:

$$P_i(t+\Delta t) = P_i(t)\times(1-\lambda_i\times\Delta t) + P_{i-1}(t)\times\lambda_{i-1}\times\Delta t \,, \quad (68.38)$$

where Δt is a small time interval. However, in our case we have possible transition rates that are both positive and negative, hence the development can

be both encreasing and decreasing. Therefore (68.38) must be rewritten:

$$\begin{aligned} P_i(t+\Delta t) &= P_i(t)\times(1-(\lambda_i + \mu_i)\times\Delta t) \\ &+ P_{i-1}(t) \times \lambda_{i-1} \times \Delta t \\ &+ P_{i+1}(t) \times \mu_{i+1} \times \Delta t \ , \end{aligned} \tag{68.39}$$

where λ_i is the positive transition rate while μ_i is the negative rate. The transition rates of the *i*th state for straight lines, curvatures, and transition curves are given from data collected with the ROGER 1000 in the period from October 2003 to June 2005 on four Norwegian tracks: *Dovrebanen, Nordlandsbanen, Meråkerbanen,* and *Sørlandsbanen*. Having the devolopment of twist we can introduce the matrix, *R*, giving the possibility of changing from one state to another for straight line, curvature, and transition curves. Part of the transition matrix for curvature is given as an example in (68.40):

$$R_{Curvature} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ . \\ 50 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & . & 50 \end{array} \\ \begin{bmatrix} 0{,}57 & 0{,}32 & 0{,}05 & . & . \\ 0{,}12 & 0{,}55 & 0{,}29 & . & . \\ 0{,}03 & 0{,}14 & 0{,}41 & . & . \\ . & . & . & . & . \\ . & . & . & . & . \end{bmatrix} \end{array}. \tag{68.40}$$

From this equation we can retrieve the transition rates $\lambda_{\text{Straight line}}$, $\lambda_{\text{Curvature}}$, $\lambda_{\text{Transition curve}}$, $\mu_{\text{Straight line}}$, $\mu_{\text{Curvature}}$, and $\mu_{\text{Transition curve}}$. The transition rates are given in days (Table 68.4).

Table 68.4. Transition rates

	Straight line	Curvature	Transition curve
λ_i	0.0017	0.0044	0.0034
μ_i	0.0006	0.0012	0.0012

68.4.2.3 Initial State Values

In this case, we use complete tracks as the system, and the tracks have a distribution of twist values to use as a starting point. In other words, we do not have a single value as a starting point, but a distribution of values. We have used the distribution given from empirical data of the track *Meråker banen* in October 2003. Figure 68.16 shows the distribution for curvatures, straight lines, and transition curves of the given level of twist. The distribution is given as meters of twist within a specific state divided by the total length.

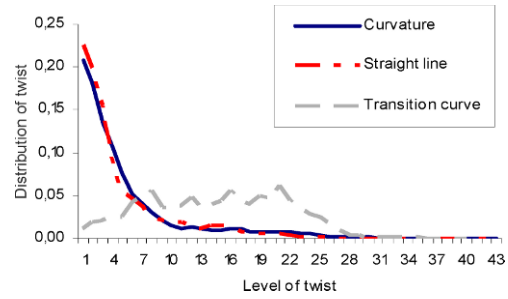


Figure 68.16. Distribution of twist

The probability of derailment is given for the three different track types. The probability is thought to be increasing exponential with the value of twist, giving a value for the probability for each state and track type.

Having these distributions and the transition rates, we can easily obtain the expected number of derailments per year, E(n_D), given different inspection intervals (τ). For this track the expected number of derailments is given in Figure 68.17.

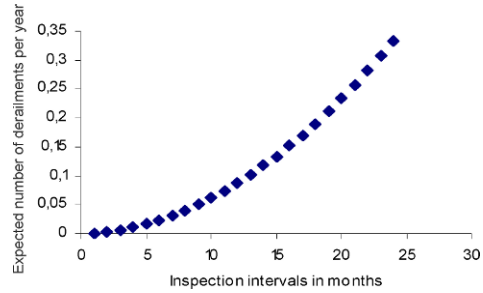


Figure 68.17. Expected number of derailments *per* year due to twist given different inspection intervals

68.4.2.4 Specification of Cost Elements

To optimize inspection intervals and intervention level we must specify the following basic cost elements:

C_D Cost per derailment (= costs for failure consequences, incl. PLL cost, material cost and cost of delay).

C_I Cost for one inspection(= fixed cost of requiring ROGER1000 and personnel operating it).

C_T Cost for one tamping action (= fixed cost of requiring the tamping machine and personnel operating it).

If E(n_D), E(n_I) and E(n_T) denote the expected number of derailments, inspections, and tamping, respectively, per year. The total costs is:

$$C_{tot} = C_D \times E(n_D) + C_I \times E(n_I) + C_T \times E(n_T). \quad (68.41)$$

The expenses were estimated for the derailment, inspection, and tamping costs of an average Norwegian railway track C_D = 15 000 000 NOK, C_I = 100 000 NOK, and C_T = 50 000 NOK, respectively. The total costs are plotted in Figure 68.18.

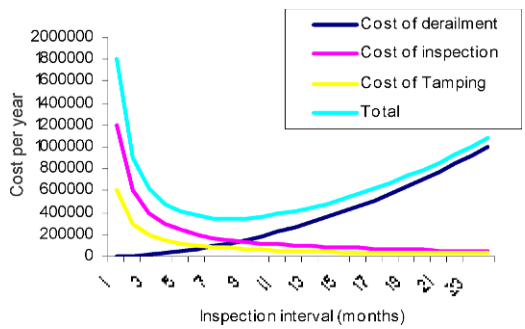


Figure 68.18. Present value of total costs and costs for CM, PM, and inspections

As can be seen from Figure 68.18, an inspection interval of approximately eight to nine months would give the lowest cost *per* year. The present inspection interval is six months, and by this calculation, about 20000 NOK per year could be saved by changing the inspection interval for this specific track.

68.6 Conclusions and Future Challenges

In this chapter we have introduced both aging/ degradation models and recent models for maintenance/renewal optimization that are relevant for railway tracks. Some of the models for maintenance optimization have been illustrated by case studies using data retrieved from inspection on Norwegian railway tracks.

However, there are some future challenges that are not addressed and require attention. The possibility for a degradation process to reverse is not included in the Markov modeling presented above. However, this could very well be the case in geometrical degradation, in particular with twist, as the forces in the track may to some degree reverse the development.

There may also be a challenge that maintenance can reduce the quality of the system. Maintenance action like tamping does not improve the quality of the ballast, but rather worsens it, making the degradation process change after the maintenance action.

Finally, the grouping of maintenance activities should be addressed. Such a grouping will not change the maintenance itself but will reduce the total costs as the logistics are improved.

References

[1] Berggren E. Dynamic track stiffness measurement – A new tool for condition monitoring of track substructure. Licentiate Thesis ISSN 1651-7660, KTH, 2005

[2] Dahlberg T. Some railroad settlement models – A critical review. Proceedings of the Institution of Mechanical Engineers 2001; 215, Part F.

[3] Demharter K. Setzungsverhalten des gleisrostes unter vertikaler Lasteinwirkung. Mitteilungen des Prüfamtes für Bau von Landverkehrswegen der Technischen Univerität München, Heft 1982; 36.

[4] Hummitszch R. Approaches to optimizing asset management of permanent way. Diploma Thesis, Technical University of Graz, 2004.
[5] Hummitszch R. Calculation schemes for MDZ and "modified standard deviation" Technical University of Graz, 2005.
[6] JBV Lærebok i jernbaneteknikk, L533, 1998.
[7] JBV Lærebok i jernbaneteknikk, L521, 1999.
[8] ORE Question D161. Dynamic vehicle/track phenomena, from the point of view of track maintenance. Final report, 1998 (Report no. 3).
[9] Promain Innovations for a cost effective railway track. November 2002 [Online] http://promain.server.de
[10] Salim W. Deformation and settlement aspects of ballast and constitutive modeling under cyclic loading. Doctoral Thesis, University of Wollongong, 2004.
[11] Sato Y. Japanese studies on deterioration of ballasted track. Vehicle System Dynamics 1995; 24:197–208.
[12] Larsson D. A study of the track degradation process related to changes in railway traffic. Licentiate thesis, Lulea University of Technology. 2004; 48 ISSN: 1402–1757.
[13] Kumar S, Chattopadhyay G, Reddy V, Kumar U. Issues and challenges with logistics of rail maintenance. Proceedings of the Second International Logistics Sections Conference; Brisbane, Australia; Feb. 22–23, 2006.
[14] Olofsson U, Nilsson R. Surface cracks and wear of rail: A full.scale test on a commuter train track. Proceedings of the Institution of Mechanical Engineers 2002; 216(4):249–264.
[15] Ringsberg JW, Bergkvist A. On propagation of short rolling contact fatigue cracks. Journal of Fatigue and Fracture of Engineering Materials and structures, 2003; 26.10: 969–983.
[16] Ishida M. Akama M. Kashiwaya K Kapoor A. The current status theory and practice on rail integrity in Japanese railways – Rolling contact fatigue and corrugation. Journal of Fatigue and Fracture of Engineering Materials and structures 2003; 26.10:909–919.
[17] Fletcher DI, Beynon JH. The effect of contact load reduction on the fatigue life of pearlitic rail steel in lubricated rolling-sliding contact. Journal of Fatigue and Fracture of Engineering Materials and structures, 2000; 23.8: 639–650.
[18] Jeong DY. Analytical modelling of rail defects and its application to rail defect management. UIC/WEC Joint Research Project on Rail Defect Management, U.S. Department of Transportation, Research and Special Programs Administration, Volpe National Transportation Sections Center, Cambridge, MA 02142, 2003.
[19] Clark R. Rail flaw detection: overview and needs for future developments. NDT&E International 37 (2004), 2003; 111–118.
[20] Sawley K, Reiff R. An assessment of Railtrack's methods for managing broken and defective rail. Rail failure assessment for the Office of the Rail Regulator, 2000; October 25.
[21] Rausand M, Høyland A. Section reliability theory. Models and statistical methods. Wiley-Interscience, New York, 2004.
[22] Ebersohn W, Ruppert CJ. Implementing a railway infrastructure maintenance section. Proceedings of Conference on Railway Engineering (CORE'98), Rockhampton, Queensland, Sept. 7–9, 1998.
[23] Budai G, Huisman D, Dekker R. Scheduling preventive railway maintenance activities. Journal of the Operational Research Society 2005; 1–10.
[24] Corshammar P. Perfect track. ISBN 91-631-8150-9, 2005.
[25] Zoeteman, A Railway design and maintenance from a life-cycle cost perspective:A Decision Support Approach. Dissertation, TRAIL Thesis Sries, Delft, The Netherlands; 2004: ISBN 90-5584-058-0.
[26] Hokstad P, Langseth H, Lindqvist BH, Vatn P. Failure modelling and maintenance optimization for a railway line. International Journal of Performability Engineering July 2005; 1(1):51–64.
[27] Podofillini L, Zio E, Vatn J. Modelling the degrading failure of a rail section under periodic inspection. In: Probabilistic Safety Assessment and Management, PSAM 7 / ESREL. Springer, Berlin, 2004; 2570–2575.
[28] Ascher H., Feingold H. Repairable systems modeling. Marcel Dekker, New York, 1984.
[29] Carretero J, Pe´rez JM, Garcı´a-Carballeira F, Caldero´n A, Ferna´ndez J, Garcı´a JD, *et al.,* Applying RCM. in large scale systems: A case study with railway networks. Reliability Engineering and System Safety 2003; 82:257–73.
[30] Cronau H. Die Breitschwelle: Eine neue Schwellenform der Heinrich Cronau. Eisenbahn-ingenieur 1998;49:70–72.

[31] Riessberger K. Frame-sleeper track promises a longer life. Railway Gazette International, July, West Sussex, 2002.
[32] Bogdanski S, Stupnicki J, Brown M, Cannon DF. A two-dimensional analysis of mixed-mode rolling contact fatigue crack growth rates in rails. Fifth International Conference on Biaxial/ Multiaxial Fatigue and Fracture, Krakow, Poland, Sept. 1997; 2: 189–206.
[33] Bower AF, Johnson KL, Plastic flow and shake-down of the rail surface in repeated wheel-rail contact. Wear 1991; 144(1–2):1–18.
[34] Vatn J. A life cycle cost model for prioritization of track maintenance and renewal. Innovations for a cost effective Railway Track, Promain 2002; 2 November.
[35] Zoeteman A. Railway design and maintenance from a life-cycle cost perspective. ISBN 90-5584-058-0. TRAIL Research School, 2004.

69

Cost–Benefit Optimization Including Maintenance for Structures by a Renewal Model

Rüdiger Rackwitz and Andreas Joanni,

Technical University Munich, Munich, Germany

Abstract: This chapter develops tools for optimizing design and maintenance strategies of aging structural components. It first reviews suitable formulations for failure models in structural engineering and the basics of renewal theory. It then introduces a repair model with or without preceding (imperfect) inspections. The inspection model introduces some increasing damage indicator function. Repairs are required if it exceeds some given threshold. Objective functions are derived for systematic reconstruction after failure or maintenance by periodic repairs alone, and by periodic inspections and possibly ensuing repairs (renewals). Finite repair times with given distribution function are considered. Initial formulations for independent repair and failure events are extended to dependent no-repair/repair and failure events.

69.1 Introduction

Most civil engineering structures age because of wear, corrosion, fatigue, and other phenomena. At a certain age they need to be inspected and, possibly, repaired or replaced. Many aging phenomena are rather complex and all but fully understood in their physical and chemical context. For concrete structures the most important aging phenomena in temperate climates are corrosion due to carbonation and/or chloride attack; for steel structures it is rusting and fatigue. In general, aging phenomena are uncertain. They involve a number of random variables or random processes. Failure is defined as a first passage time failure. More specifically, failure is defined when a more or less complicated function of those variables reaches a limiting state for the first time. Failure time distributions must be determined numerically. This makes analyses rather complex and rather different from analyses where analytical failure time models based on rich data can be used.

Another area of great interest is the optimization of the cost spent in maintaining civil engineering facilities. The enormous cost required for maintaining public infrastructures, for example, call for careful cost-benefit optimization of design rules and maintenance. It should be clear that only a rigorous life-cycle consideration can fully account for all cost involved. Moreover, it should be clear that design rules and maintenance procedures strongly interact.

In the following, classical renewal theory is applied in order to set up suitable objective functions for cost–benefit optimization of maintained structures. It turns out that almost all concepts developed earlier for electronic and machine components can also be employed in

structural engineering. In the civil engineering field some basic concepts have already been developed in [1] and later in [2] for stationary failure processes without deterioration. In agreement with standard cost–benefit analyses all benefits and cost are discounted. Rigorous integration of maintenance cost of inspection and repairs for structural components was started in [3] and [4] based on the work by Cox [5], Barlow and Proschan in [6], [7] but especially by Fox [8]. This continued in [9] by extending the considerations to existing structures. Age-dependent and block repairs as well as condition-based repairs were considered. In [4] and other references successful attempts have been made to cover also series systems. In all this work it was assumed that no-repair/repair events and failure events are independent, and repair times are negligible as compared to the failure times. However, this is rarely realistic since, on the one hand, inspection results and consecutive repair decisions and failure events most often depend on the same physical deterioration processes and, therefore, become highly dependent. On the other hand, infinitely short renewal times as assumed so far are generally only a simplification. The formulations are extended to cover also finite renewal times. These limitations have recently been removed in [10], which is also the basis of this contribution.

After presenting some failure models suitable for aging structural components, reviewing renewal theory to the extent needed for the further developments, and introducing appropriate inspection and repair models, the chapter first reviews the concepts for cost benefit optimization based on the renewal model. This is then extended to include preventive and corrective maintenance including independent and dependent no-repair/repair and failure events. Thereafter, new results are derived for the case of finite renewal times. An example illustrates the main findings.

69.2 Preliminaries

69.2.1 Failure Models for Deteriorating Components

There are very few exact, time-variant failure models available. One such model with many potential applications is the so-called random disturbance model. As a special case, stationary random Poissonian disturbances (earthquakes, storms, explosions, fires, *etc.*) with occurrence rate are considered. If a disturbance hits the system, failure will occur with probability $P_f(\mathbf{p})$. $\mathbf{p}$ is a vector of suitable design parameters. The failure process will again be Poissonian with rate $\lambda P_f(\mathbf{p})$. Deterioration cannot be accounted for. It is presented here only for completeness.

For aging structures a closed-form failure time (first passage time) distribution is hardly available except for some special, usually oversimplifying cases. The log-normal, inverse Gaussian or Weibull distribution function with a suitable deterioration mechanism for the mean (and/or other parameters) have been used. However, sufficient data to support those models are rarely available in the structures area. Realistic failure models must be derived from physical multi-variable deterioration models (cumulative wear, corrosion, fatigue, *etc.*). For deteriorating structures a widely used failure model is when the deterioration function is monotonically and continuously in(de)creasing. Then, let $G(\mathbf{X},t) = g(\mathbf{U},t)$ be the (differentiable), continuously decreasing structural state function of a structural component with $G(\mathbf{X},t) = g(\mathbf{U},t) \le 0$ the failure domain. $G(\mathbf{X},t) = g(\mathbf{U},t) = 0$ is denoted as limit state. $\mathbf{X}$ is a vector of random variables with continuous distribution function and time t is a parameter. Transition from $\mathbf{X}$ to $\mathbf{U}$ denotes the usual probability transformation from the original into the standard space of variables [11]. Within FORM/SORM the probability of the time to failure is [12], [13]

$$\begin{aligned} F(t) &= P(T \le t) \\ &= P(g(\mathbf{U},t) \le 0) \approx \Phi(-\beta(t))C(t) \end{aligned} \tag{69.1}$$

for $t \ge 0$, and the corresponding failure density is

$$\begin{aligned} f(t) &= \frac{\partial F(t)}{\partial t} \\ &\approx -\varphi(\beta(t))\frac{\partial \beta(t)}{\partial t}C(t) + \Phi(-\beta(t))\frac{\partial C(t)}{\partial t} \\ &= -\varphi(\beta(t))\left(\frac{-\frac{\partial}{\partial t}g(\mathbf{u}^*,t)}{\|\nabla_{\mathbf{u}}g(\mathbf{u}^*,t)\|}\right)C(t) \\ &\qquad + \Phi(-\beta(t))\frac{\partial C(t)}{\partial t}. \end{aligned} \tag{69.2}$$

T is the time to first entrance into a failure state. $\Phi(\cdot)$ and $\varphi(\cdot)$ denote the univariate standard normal distribution function and corresponding density, respectively. $\beta(t)$ is the (geometrical) reliability index $\beta(t) = \min\{\|\mathbf{u}\|\}$ for $\{\mathbf{u} : g(\mathbf{u},t) \le 0\}$. $C(t)$ is a correction factor evaluated according to SORM (and/or importance sampling) which can be neglected in many cases. In (69.2) it frequently can be assumed that $C(t)$ does not vary with t. Throughout the paper only FORM/SORM techniques will be applied.

In some cases consideration of (stationary or non-stationary) time-variant actions and a time-variant structural state function is necessary. Let $G(\mathbf{X}(t),t)$ be the (differentiable) structural state function such that $G(\mathbf{X}(t),t) \le 0$ denotes failure states and $\mathbf{X}(t)$ a random process. Then, the failure time distribution can be computed numerically by the outcrossing approach. A well-known upper bound is [14]

$$F(t) \le \int_0^t \nu(\tau)d\tau \le 1 \tag{69.3}$$

with the outcrossing rate (more specifically, the downcrossing rate)

$$\begin{aligned} \nu(\tau) = \lim_{\Delta\to 0}\frac{1}{\Delta}P(&\{G(\mathbf{X}(t),t) > 0\} \\ &\cap \{G(\mathbf{X}(t+\Delta),t+\Delta) \le 0\}) \end{aligned} \tag{69.4}$$

with Δ some small time interval. Most frequently, however, an asymptotic result is used

$$F(t) = 1 - \exp\left[-\int_0^t \nu(\tau)d\tau\right]. \tag{69.5}$$

Equation (69.5) implies a non-homogeneous Poisson process of failure events with intensity $\nu(t)$. For stationary failure processes (69.5) reduces to a homogeneous Poisson process and simplifies somewhat. Under suitable conditions both formulae can also be evaluated using FORM/SORM provided that the dependence structure of the two events $\{G(\mathbf{X}(t),t) > 0\}$ and $\{G(\mathbf{X}(t+\Delta),t+\Delta) \le 0\}$ can be determined in terms of correlation coefficients. However, the relevant conditions must be fulfilled, *i.e.*, the outcrossing events must become independent and rare asymptotically. For example, the independence property is lost if $\mathbf{X}(t)$ contains not only (mixing) random processes but also simple random variables. Therefore, in many cases this approach yields only crude approximations.

A numerical computation scheme for first-passage time distributions under less restrictive conditions can also be given. It is based on the following lower bound formula:

$$\begin{aligned} F(t) = P(T \le t) &= 1 - P(G(\mathbf{X}(\theta),\theta) > 0 \\ &\qquad \text{for all } \theta \text{ in } [0,t]) \\ &\ge P\left(\bigcup_{i=1}^{n} P(G(\mathbf{X}(t_i),t_i) \le 0)\right) \end{aligned} \tag{69.6}$$

with $t = t_n$ and $t_i < t$ denoting a narrow not necessarily regular time spacing of the interval $[0,t]$. As demonstrated by examples, *e.g.*, in [15], the lower bound to the first-passage time distribution turns out to be surprisingly accurate for all values of $F(t)$, if the time-spacing $\tau = \theta_i - \theta_{i-1}$ is chosen sufficiently close and where $\theta_i = i\tau$ and $t = \theta_n$. Within FORM/SORM it is

$$F(t) = P(T \le t) \ge P(\bigcup_{i=0}^{n} \{g(\mathbf{U}(\theta_i), \theta_i) \le 0\})$$
$$\approx P(\bigcup_{i=0}^{n} \{\alpha(\theta_i)^T \mathbf{U}(\theta_i)) + \beta(\theta_i) \le 0\}$$
$$= 1 - P(\bigcap_{i=0}^{n} \{Z_i \le \beta(\theta_i)\}) = 1 - \Phi_{n+1}(\mathbf{b}; \mathbf{R}) \tag{69.7}$$

Here again, a probability distribution transformation from the original space into the standard space is performed and the boundaries of each failure domain are linearized. The last line represents a first order approximation where $\Phi_n(\cdot;\cdot)$ is the n-dimensional standard normal integral with $\mathbf{b} = \{\beta(\theta_i)\}$ the vector of reliability indices of the various components (elements, individual events) in the union and the dependence structure of the events is determined in terms of correlation coefficients $\mathbf{R} = \{\rho_{ij} = \alpha(\theta_i)^T \alpha(\theta_j)\}$. Suitable computation schemes for the multinormal integral for high dimensions and arbitrary probability levels have been proposed, for example, in [16], [17], [18] and [19]. This computation scheme is approximate but quite general if the correlation structure of the state functions in the different points in time can be established.

Deterioration of structural resistance is frequently preceded by an initiation phase. In this phase failure is dominated by normal (extreme-value) failure. Structural resistance is virtually unaffected. Only in the succeeding phase do resistances degrade. Examples are crack initiation and crack propagation or chloride penetration into concrete up to the reinforcement and subsequent reduction of the reinforcement cross-section by corrosion, and, similarly, for initial carbonation and subsequent corrosion. In many cases the initiation phase is much longer than the actual degradation phase. Let T_i denote the random time of initiation, T_e the random time to normal (first-passage extreme-value) failure and T_d the random time from the end of the initiation phase to deterioration failure with degraded resistance. Note, extreme-value failure during the initiation phase and failure in the deterioration phase are mutually exclusive. If the variables and T_d can be assumed independent, the following formula can be used:

$$F(t) = F_e(t)\bar{F}_i(t) + \int_0^t f_i(\tau)\left[F_e(\tau) + (1 - F_e(\tau))F_d(t-\tau)\right] d\tau . \tag{69.8}$$

69.2.2 A Review of Renewal Theory

Assume that the structure fails at a random time in the future. After failure or serious deterioration it is systematically renewed by reconstruction or retrofit/repair. Reconstruction or retrofit/repair reestablish all (stochastic) structural properties. The times between failure (renewal) events have identical distribution functions $F(t),\ t \ge 0,$ with probability densities $f(t)$ and are independent (see [3] for details). Those are precisely the conditions under which classical renewal theory holds. Renewal theory allows for the first failure time distribution being different from the others. For simplicity, this modification is not considered herein (see, however, [5]). The independence assumption needs to be verified carefully. In particular, one has to assume that loads and resistances in the system are independent for consecutive renewal periods and there is no change in the design rules after the first and all subsequent failures (renewals). Even if designs change failure time distributions must remain the same.

The renewal function based on these assumptions and which will be used extensively later on is

$$M(t) = E[N(t)] = \sum_{n=1}^{\infty} np(N(t) = n)$$
$$= \sum_{n=1}^{\infty} n[F_n(t) - F_{n+1}(t)] = \sum_{n=1}^{\infty} F_n(t)$$
$$= \sum_{n=1}^{\infty} \int_0^t F_n(t-u)dF(u) = F(t) + \int_0^t M(t-u)dF(u) \tag{69.9}$$

with $N(t)$ the random number of renewals and $p(N(t) = n)$ the probability mass function. The

last expression in (69.9) is called the "renewal equation"'. Unfortunately, (69.9) has closed-form solutions for only very few special failure models. In general, (69.9) has to be determined numerically. A particularly suitable method is proposed in [20]. It starts from the renewal equation (69.9) and solves it numerically by simply making use of the upper and lower sum in Riemann–Stieltjes integration. Because $M(t)$ is non-decreasing we have the following bounds:

$$\begin{aligned} M_L(k\tau) &= F(k\tau)+\sum_{i=1}^{k} M_L((k-i)\tau)\Delta F(i\tau) \le \\ &\le M(k\tau) \le \\ &\le F(k\tau)+\sum_{i=1}^{k} M_U((k-i+1)\tau)\Delta F(i\tau) = M_U(k\tau) \end{aligned} \tag{69.10}$$

for equal partitions of length τ in $[0,t]$ with $\Delta F(i\tau) = F(i\tau) - F((i-1)\tau)$ and $n\tau = t$. This linear equation system is solved numerically.

Another related quantity of interest is the availability of a system, *i.e.*, its probability of being in a functional state. This is particularly interesting if, as discussed later, repairs take a finite time. Let $F(t)$ be the life time distribution with density $f(t)$ and $G(t)$ the repair-time distribution with density $g(t)$ of a component so that $H(t) = \int_0^t F(t-u)g(u)du$ is the distribution of $T_F + T_G$ for independent failure and repair times. Then, an important characteristic is the (point-in-time) availability of the component

$$A(t) = 1 - F(t) + \int_0^t (1 - F(t-u))dM_H(u), \tag{69.11}$$

where $M_H(t) = \sum_{i=1}^{\infty} H_i(t)$ is the renewal function for $H(t)$. The asymptotic availability is defined as

$$A(\infty) = \frac{E[T_F]}{E[T_F] + E[T_G]}, \tag{69.12}$$

which is easily interpreted as the ratio of the fraction of working time to the total time of a renewal cycle. Usually, $A(t)$ rapidly approaches $A(\infty)$. It is also possible to compute bounds on availability by the same method as for (69.3). Since

$$\begin{aligned} A_{U,L}(k\tau) &\lessgtr 1 - F(k\tau) + \\ &+ \sum_{j=1}^{k} (1 - F((k-j)\tau))(M_{U,L}(j\tau) - M_{U,L}((j-1)\tau)) \end{aligned} \tag{69.13}$$

one may use (69.10) in (69.13) for $k\tau < t$ and $A(0) = 1$. Unfortunately, as time t becomes large the numerical bounds widen.

The renewal intensity (or, if applied to failure processes, the unconditional failure intensity)

$$\begin{aligned} m(t) &= \lim_{dt \to 0} \frac{P(\text{one renewal in}[t, t+dt])}{dt} \\ &= \frac{dM(t)}{dt} = \sum_{n=1}^{\infty} f_n(t) \end{aligned} \tag{69.14}$$

can be obtained by differentiating the renewal function. As pointed out in [5] $m(t)$ has a limit

$$m(t \to \infty) = \lim_{t \to \infty} m(t) = \frac{1}{E[T]} \tag{69.15}$$

for $f(t) \to 0$ if $t \to \infty$. In approaching the limit it can be strictly increasing, strictly decreasing or oscillate in a damped manner around $1/E[T]$. For most failure models with increasing risk function the renewal intensity is increasing. The renewal intensity (failure rate) can be used to set acceptability limits, which is not done herein.

69.2.3 Inspection and Repair

Inspections should determine the actual state of a component in order to decide whether to carry out on repair or to leave it as is. However, inspections can rarely be perfect. A decision about repair can only be reached with certain probability depending

on the inspection method used. The repair probability depends on the magnitude of one (or more) suitable damage indicators (chloride penetration depth, crack length, abrasion depth, *etc.*) measured during inspection. For cumulative damage phenomena the repair probability $P_R(t)$ increases with the time t elapsed since the beginning of the deterioration process. For example, the repair probability may be presented as

$$P_R(t) = P(S(t,\mathbf{X}) > s_c) = P(s_c - S(t,\mathbf{X}) \le 0) \tag{69.16}$$

with $S(t,\mathbf{X})$ a suitable, monotonically increasing damage indicator, $\mathbf{X}$ a random vector taking into account all uncertainties during inspection and s_c a given threshold level. The vector $\mathbf{X}$ usually also includes a random variable modeling the measurement error. Frequently, the damage indicator function $S(t,\mathbf{X})$ has a similar form as the failure function and involves, at least in part, the same random variables. In this case failure and repair events become dependent events. Generalizations of (69.16) to multiple damage indicators and more complicated decision rules are straightforward. A discussion of the details of the efficiency of various inspection methods and the corresponding repair probabilities is beyond the scope of this paper.

After failure of a system or component it is repaired unless it is given up after failure. The term "repair" is used synonymously for repair, renewal, replacement, or reconstruction. Repairs, if undertaken, restore the properties of a component to its original (stochastic) state, *i.e.*, repairs are equivalent to renewals (AGAN= as good as new), so that the life time distribution of the repaired component is again $F(t)$. The repair times can either be assumed negligibly short or have finite length.

The proposed model is a somewhat idealized model capturing the most important aspects of the decision problem. It rests on a number of assumptions the most important of which is probably that repairs fully restore the initial (stochastic) properties of the component. Imperfect repairs cannot be handled because the renewal argument repeatedly used in the following breaks down. In the literature several models for imperfect repairs are discussed, which only partially reflect the situations met in the structures area. An important case is when so-called minimal repairs not essentially changing the initial lifetime are done right after an inspection. Such repairs leave a component "as bad as old"'. Renewal (perfect repair) occurs with probability π but minimal repair with probability $1-\pi$. This model, in fact, resembles the one studied herein with $\pi = P_R(t)$. A review of other and especially imperfect repair models is given in [22].

Inspection/repair at strictly regular time intervals as assumed below is also not very realistic. However, as will be shown in the example, the objective function is rather flat in the vicinity of the optimal value so that small variations will not noticeably change the results.

Repair operations necessarily lead to discontinuities (drops) in the risk function as well as in the (unconditional) failure rate. They can substantially reduce the number of failures and, thus, corrective renewals.

69.3 Cost–Benefit Optimization

69.3.1 General

For technical facilities the following objective has been proposed by Rosenblueth and Mendoza [1] based on earlier proposals for cost–benefit analysis:

$$Z(\mathbf{p}) = B(\mathbf{p}) - C(\mathbf{p}) - D(\mathbf{p})\,. \tag{69.17}$$

A facility is financially optimal if (69.17) is maximized. It is assumed that all quantities in (69.17) can be measured in monetary units. $\mathbf{p}$ is the vector of all safety relevant parameters. $B(\mathbf{p})$ is the benefit derived from the existence of the facility, $C(\mathbf{p})$ is the cost of planning, design, and construction and $D(\mathbf{p})$ is the cost in case of failure. Statistical decision theory dictates that expected values are to be taken [23]. In the

following it is assumed that $B(\mathbf{p}), C(\mathbf{p})$ and $D(\mathbf{p})$ are differentiable in each component of **p.** This makes optimization of (69.17) easy because gradient-based optimizers can be used. The cost may differ, for the different parties involved have different economic objectives, *e.g.*, the owner, the builder, the user, and society. A facility makes sense only if $Z(\mathbf{p})$ is positive within certain parameter ranges for all parties involved.

The facility has to be optimized during design and construction at the decision point. Therefore, all costs need to be discounted. A continuous discounting function is assumed for analytical convenience, which is accurate enough for all practical purposes,

$$\delta(t) = \exp\left[-\gamma t\right],$$

Where γ is a time-independent, time-averaged interest rate. In most cost–benefit analyses a tax-free and inflation-free discount rate should be taken. If a discrete discount rate γ' is given, one converts with $\gamma = \ln(1+\gamma')$.

In contrast to strategies that do a cost–benefit analysis only for given service times or, possibly, for the time to failure after which the structure is given up it is assumed that structures will be systematically reconstructed after failure or obsolescence and/or are properly maintained by perfect repairs. This rebuilding strategy is in agreement with the principles of life-cycle engineering and also fulfills the demand for sustainability [24]. Clearly, it rests on the assumption that future preferences are the same as the present preferences. It follows that sustainable life-cycle costing not only includes the cost of one replacement but of all cost that might emerge from future failures and renewals (repairs, replacements, *etc.*). Another aspect of sustainability is that only moderate discount rates should be chosen.

69.3.2 The Standard Case

The benefit $B(\mathbf{p})$ is discounted down to the decision point. For a benefit rate $b(t)$ unaffected by possible renewals one find

$$B = \int_0^\infty b(t)\exp\left[-\gamma t\right] A(t)dt \tag{69.18}$$

assuming convergence of the integral. If the benefit rate $b = b(t)$ is constant, and repair times are negligibly short one can integrate to obtain

$$B = \int_0^\infty b\exp\left[-\gamma t\right]dt = \frac{b}{\gamma}. \tag{69.19}$$

The upper integration limit is extended to infinity because the full sequence of life-cycle benefits is considered. A more refined benefit model has been introduced in [25], which is not considered herein (see, however, [9]).

The construction costs $C(\mathbf{p})$ are generally easy to assess. If they have to be financed, the cost of financing reduces the benefit. For example, the yearly cost for full financing (as a constant annuity) are $dC_\gamma(\mathbf{p}) = C(\mathbf{p})\dfrac{\exp\left[\gamma\right]-1}{1-\exp\left[-\gamma t_f\right]}$, where t_f is the financing time. These yearly costs can be taken into account in the benefit term.

The determination of damage cost is more involved. Consider the case of systematic reconstruction (or repair). Let Y_n be the time to the n th renewal

$$Y_n = \sum_{r=1}^{n} U_r, \tag{69.20}$$

and denote by $K(U_n)$ the cost of the interval U_n. $K(U_n)$ can contain failure cost, reconstruction cost or repair cost and it can be a function of time. The total discounted cost K for an infinite length of time is the sum of all renewal cost discounted down to time 0. This gives

$$K = \sum_{n=1}^{\infty} K(U_n) e^{\left(-\gamma\sum_{r=1}^{n} U_r\right)}. \tag{69.21}$$

The expected damage costs D are computed from:

$$\begin{aligned} D &= E\left[\sum_{n=1}^{\infty} K(U_n) e^{\left(-\gamma \sum_{r=1}^{n} U_r\right)}\right] \\ &= \sum_{n=1}^{\infty} E\left[\left(\prod_{r=1}^{n-1} e^{-\gamma U_r}\right) K(U_n) e^{-\gamma U_n}\right] \\ &= \sum_{n=1}^{\infty} E\left(e^{-\gamma U}\right)^{n-1} E\left(K(U) e^{-\gamma U}\right) = \frac{E\left(K(U) e^{-\gamma U}\right)}{1 - E\left(e^{-\gamma U}\right)} \end{aligned} \tag{69.22}$$

where we used formulations proposed in [26]. The renewal model ensures that all times U_r are identically distributed and independent. In the last line the well-known relation $\sum_{n=1}^{\infty} a q^{n-1} = \frac{a}{1-q}$ is used. $E\left(e^{-\gamma U}\right) = \int_0^{\infty} \exp[-\gamma u] f_U(u) du = f^*(\gamma)$ is also denoted by the Laplace transform of $f_U(u)$. Equation (69.22) is the key result for cost benefit optimization based on the renewal model. It should be mentioned that parallel but less rich results can be obtained for discrete failure models and discrete discounting [27].

69.4 Preventive Maintenance

69.4.1 Cost Benefit Optimization for Systematic Age-dependent Repair

First it should be emphasized that preventive maintenance only makes sense for increasing risk functions $r(t) = \frac{f(t)}{1 - F(t)}$ of the failure model. If the risk function is not increasing (but is constant or even decreasing) it is more cost–benefit optimal to wait until failure.

The general case of replacements (repairs, renewals) at random times T_R with distribution $F_R(t)$ or after failure at random times T_F with distribution $F_F(t, \mathbf{p})$ is best derived as follows. The renewal time is the minimum of these times with distribution function

$$\begin{aligned} F(t, \mathbf{p}) &= 1 - (1 - F_F(t, \mathbf{p}))(1 - F_R(t)) \\ &= 1 - \bar{F}_F(t, \mathbf{p}) \bar{F}_R(t) \end{aligned} \tag{69.23}$$

for independent times T_F and T_R with density

$$f(t, \mathbf{p}) = f_F(t, \mathbf{p}) \bar{F}_R(t) + f_R(t) \bar{F}_F(t, \mathbf{p}), \tag{69.24}$$

where the notation $\bar{F}(x) = 1 - F(x)$ is used. Application of (69.22) then gives for the damage term of an ordinary renewal process

$$\begin{aligned} D(\mathbf{p}) &= \frac{E\left(K(U) e^{-\gamma U}\right)}{1 - E\left(e^{-\gamma U}\right)} \\ &= \frac{(C(\mathbf{p}) + L) f^*_{\bar{F}_R}(\gamma, \mathbf{p}) + R(\mathbf{p}) f^*_{\bar{F}_F}(\gamma, \mathbf{p})}{1 - (f^*_{\bar{F}_F}(\gamma, \mathbf{p}) + f^*_{\bar{F}_R}(\gamma, \mathbf{p}))} \end{aligned} \tag{69.25}$$

where $f^*_{\bar{F}_R}(\gamma, \mathbf{p}) = \int_0^{\infty} \exp[-\gamma t] f_F(t, \mathbf{p}) \bar{F}_R(t) dt$ and $f^*_{\bar{F}_F}(\gamma, \mathbf{p}) = \int_0^{\infty} \exp[-\gamma t] f_R(t) \bar{F}_F(t, \mathbf{p}) dt$ are the modified complete Laplace transforms of $f_F(t, \mathbf{p}) \bar{F}_R(t)$ and $f_R(t) \bar{F}_F(t, \mathbf{p})$, respectively. L is the direct loss of failure, $C(\mathbf{p})$ the reconstruction cost after failure, and $R(\mathbf{p})$ the cost of repair.

At first sight, the case of random maintenance actions has hardly any practical application. However, if there is continuous monitoring of the structural state, the times T_R can be interpreted as the times when the monitoring measurements reach a critical value for the first time and, therefore, indicate the necessity of repair actions. This case is not studied further. Alternatively, assume maintenance actions with probability one at (almost) fixed intervals $a, 2a, 3a, \ldots$ so that $f_R(t) = \delta_e(a)$ and $F_R(t) = H_e(a)$ ($\delta_e(x) =$ Dirac's delta function, and $H_e(a) =$ Heavyside's unit step function). Equation (69.25) then becomes:

$$D_M(\mathbf{p},a) = \frac{(C(\mathbf{p})+L)f^{**}(\gamma,\mathbf{p},a)+R(\mathbf{p})\exp[-\gamma a]\bar{F}(\mathbf{p},a)}{1-(f^{**}(\gamma,\mathbf{p},a)+\exp[-\gamma a]\bar{F}(\mathbf{p},a))} \tag{69.26}$$

where $f^{**}(\gamma,\mathbf{p},a)=\int_0^a \exp[-\gamma t] f_F(t,\mathbf{p})dt$ is the incomplete Laplace transform of $f_F(t,\mathbf{p})$. The derivations for (69.25) and (69.26) clearly show that systematic repairs should be interpreted as one of the two renewal modes. Equation (69.26) goes back to some early work in [5] and [6], and especially to Fox [8]. It is still the basis for further developments in cost–benefit optimization for maintained structures with discounting, as will be seen below. Optimization can be carried out with respect to the design parameter $\mathbf{p}$ and/or the maintenance interval a. Already Fox [8] pointed out that an optimum in a only exists if the risk function of the failure model is increasing. Also, the repair cost $R(\mathbf{p})$ should be substantially smaller than $C(\mathbf{p})+L$ so that it is worth making preventive repairs and, thus, avoiding large failure and reconstruction cost in the case of failure.

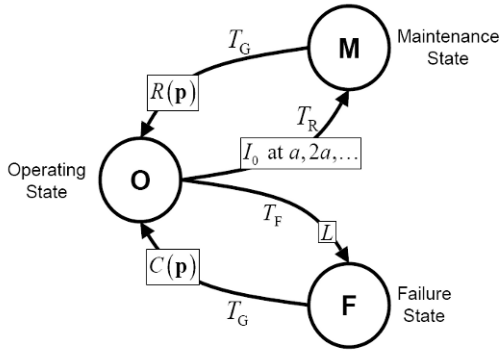


Figure 69.1. Finite repair times after failure or planned repair

Finite renewal times require only small modifications. The component behavior is modeled as shown in Figure 69.1. All repair times are identically distributed and independent of failure times. At failure costs L are involved while reconstruction cost $C(\mathbf{p})$ is incurred at the end of the repair time for each renewal cycle. It is further assumed that no failure occurs during repair. We consider first the first term in the damage function without repair actions.

The damage cost consists of two parts. Applying the reasoning for (69.22) of systematic reconstruction gives

$$D_H(\mathbf{p}) = \frac{Lf^*(\gamma,\mathbf{p})}{1-f^*(\gamma,\mathbf{p})g^*(\gamma)} + \frac{C(\mathbf{p})f^*(\gamma,\mathbf{p})g^*(\gamma)}{1-f^*(\gamma,\mathbf{p})g^*(\gamma)} = \frac{Lf^*(\gamma,\mathbf{p})+C(\mathbf{p})h^*(\gamma,\mathbf{p})}{1-h^*(\gamma,\mathbf{p})} \tag{69.27}$$

The renewal cycle now has length T_F+T_G. T_F and T_G are assumed independent. Clearly, $h^*(\gamma,\mathbf{p})=f^*(\gamma,\mathbf{p})g^*(\gamma)$ is the Laplace transform of the density $h(t,\mathbf{p})=\int_0^\infty f(t-\tau,\mathbf{p})g(\tau)d\tau$ of this alternating two-phase renewal process. Also, $g(t)$ is the density of the repair times. Deterministic renewal times of length s are included because $g^*(\gamma)=\exp[-\gamma s]$ is the Laplace transform of the density $g(t)=\delta(s)$.

With renewals after failure or systematic repairs at age a, (69.26) has to be modified

$$D_{HR}(\mathbf{p},a) = \frac{\left(\begin{array}{c} Lf^{**}(\gamma,\mathbf{p},a)+C(\mathbf{p})k^{**}(\gamma,\mathbf{p},a)+ \\ +R(\mathbf{p})g^{**}(\gamma,a)\bar{F}(\mathbf{p},a) \end{array}\right)}{1-(k^{**}(\gamma,\mathbf{p},a)+g^{**}(\gamma,a)\bar{F}(\mathbf{p},a))} \tag{69.28}$$

where

$$f^{**}(\gamma,\mathbf{p},a)=\int_0^a \exp[-\gamma t] f(t,\mathbf{p})dt,$$

$$k^{**}(\gamma,\mathbf{p},a)=\int_0^a\int_0^\infty \exp[-\gamma(t+\tau)]g(\tau)d\tau f(t,\mathbf{p})dt = f^{**}(\gamma,\mathbf{p},a)g^*(\gamma) \le h^{**}(\gamma,\mathbf{p},a)$$

$$g^{**}(\gamma,a)=\int_0^\infty \exp[-\gamma(t+a)]g(t)dt = \exp[-\gamma a]g^*(\gamma).$$

$k^{**}(\gamma,\mathbf{p},a)$ expresses the (discounted) time until the end of this renewal cycle where $C(\mathbf{p})$ becomes due and which can be larger than a. The upper bound $h^{**}(\gamma,\mathbf{p},a)$ for $k^{**}(\gamma,\mathbf{p},a)$ implies that the

reconstruction cost $C(\mathbf{p})$ fall always at a. $g^{**}(\gamma,a)$ takes account of the finite time of repair after a because, as assumed, the repair costs are only due at the end of the repair period. For many models of repair time distributions, *e.g.*, deterministic, exponential or Rayleigh, the inner integral in $k^{**}(\gamma,\mathbf{p},a)$ and the integral in $g^{**}(\gamma,a)$ are analytic. The first two terms in (69.28) represent the corrective renewal mode while the last term is the preventive renewal mode. In general, the influence of finite repair times is expected to be small, having in mind that mean repair times usually do not exceed a few percent of the failure times.

69.4.2 Cost–Benefit Optimization Including Inspections and Repair

In structures and many other areas any expensive maintenance operation is preceded by inspections involving cost I_0 if damage progression and/or changes in system performance are observable. We understand that the inspections are essential inspections eventually leading to decisions about repair or no repair. This maintenance strategy is sometimes called condition-based maintenance. If there are inspections at times $a, 2a, 3a, \ldots$ there is not necessarily a repair because aging processes and inspections are uncertain or the signs of deterioration are vague. Repairs occur only with probability $P_R(t)$ (see (69.16)). Then, inspection and repair cost must also be included in the damage term.

The objective function for independent no-repair/repair and failure events is now:

$$Z_{IM}(\mathbf{p},a) = B - C_R(\mathbf{p}) - J(a) - D_{IM}(\mathbf{p},a)\,. \tag{69.29}$$

Application of (69.22) to the inspection cost term yields

$$J(a) = \frac{I_0(\exp[-\gamma a]\bar{F}(\mathbf{p},a))}{1-(\exp[-\gamma a]\bar{F}(\mathbf{p},a))}\,. \tag{69.30}$$

The damage term is written as

$$D_{IM}(\mathbf{p},a) = \frac{N_{IM}}{D_{IM}} \tag{69.31}$$

with

$$\begin{aligned} N_{IM} \;=\; & L\left(\sum_{n=1}^{\infty}\prod_{j=0}^{n-1}\bar{P}_R(ja)f^{***}(\gamma,\mathbf{p},(n-1)a\le t\le na)\right)+ \\ & +C(\mathbf{p})\left(\sum_{n=1}^{\infty}\prod_{j=0}^{n-1}\bar{P}_R(ja)k^{***}(\gamma,\mathbf{p},(n-1)a\le t\le na)\right)+ \\ & +R(\mathbf{p})\sum_{n=1}^{\infty}g^{**}(\gamma,na)\prod_{j=0}^{n-1}P_R(na)\bar{P}_R(ja)\bar{F}(\mathbf{p},na) \end{aligned} \tag{69.32}$$

and, similarly, for the denominator

$$D_{IM} = 1-\left(\begin{array}{l}\displaystyle\sum_{n=1}^{\infty}\prod_{j=0}^{n-1}\bar{P}_R(ja)k^{***}(\gamma,\mathbf{p},(n-1)a\le t\le na) \\ \displaystyle+\sum_{n=1}^{\infty}g^{**}(\gamma,na)\prod_{j=0}^{n-1}P_R(na)\bar{P}_R(ja)\bar{F}(\mathbf{p},na)\end{array}\right) \tag{69.33}$$

Here, $P_R(0)=0$ and

$$\begin{aligned} & k^{***}(\gamma,\mathbf{p},(n-1)a\le t\le na) = \\ & = \int_{(n-1)a}^{na}\int_0^{\infty}\exp\left[-\gamma(t+\tau)\right]g(\tau)d\tau f(t,\mathbf{p})dt \\ & = f^{***}(\gamma,\mathbf{p},(n-1)a\le t\le na)g^{*}(\gamma,na) \\ & g^{**}(\gamma,na) = \int_0^{\infty}\exp\left[-\gamma(t+na)\right]g(t)dt \\ & \quad = \exp\left[-\gamma na\right]g^{*}(\gamma). \end{aligned}$$

In principle, the repair duration density $g(t)$ can be different after failure and for preventive repair.

If dependent no-repair/repair and failure events must be assumed the inspection cost remain as in (69.30). In analogy to the independent case it is

$$\begin{aligned} & f^{****}(\gamma,\mathbf{p},(n-1)a\le t\le na) = \\ & = \int_{(n-1)a}^{na}\exp\left[-\gamma t\right]\times \\ & \quad \frac{d}{d\vartheta}P\Big(\bigcap_{j=0}^{n-1}\left\{\bar{R}(ja)\right\}\cap\left\{T_F\le\vartheta\right\}\Big)_{|\vartheta=t}dt \end{aligned} \tag{69.34}$$

$$h^{****}(\gamma,\mathbf{p},(n-1)a\le t\le na)=$$
$$=\int_{(n-1)a}^{na}\exp[-\gamma t]\times \quad (69.35)$$
$$\frac{d}{d\vartheta}P(\bigcap_{j=0}^{n-1}\{\bar{R}(ja)\}\cap\{T_F+T_G\le\vartheta\})_{|\vartheta=t}\,dt$$

in

$$Z_{IMF}(\mathbf{p},a)=B-C_R(\mathbf{p})-J(a)-D_{IMD}(\mathbf{p},a)\,. \quad (69.36)$$

We further have

$$\begin{aligned}N_{IMD} &= L\left(\sum_{n=1}^{\infty}f^{****}(\gamma,\mathbf{p},(n-1)a\le t\le na)\right)\\ &+C(\mathbf{p})\left(\sum_{n=1}^{\infty}h^{****}(\gamma,\mathbf{p},(n-1)a\le t\le na)\right)\\ &+R(\mathbf{p})\sum_{n=1}^{\infty}g^{**}(\gamma,na)\times\\ &\times P(\{R(na)\}\cap\bigcap_{j=0}^{n-1}\{\bar{R}(ja)\}\cap\{T_F>na\})\end{aligned} \quad (69.37)$$

$$D_{IMD}=1-\left(\begin{aligned}&\sum_{n=1}^{\infty}h^{****}(\gamma,\mathbf{p},(n-1)a\le t\le na)\\ &+\sum_{n=1}^{\infty}g^{**}(\gamma,na)\times\\ &\times P(\{R(na)\}\cap\bigcap_{j=0}^{n-1}\{\bar{R}(ja)\}\cap\{T_F>na\})\end{aligned}\right) \quad (69.38)$$

in

$$D_{IMD}=\frac{N_{IMD}}{D_{IMD}}\quad . \quad (69.39)$$

$R(ja)$ is the repair event at ja, which takes some random time with density $g(t)$. The probabilities of the intersection events in those equations can be determined approximately by applying the FOR/SOR-methodology. Remember that a typical intersection event $\left\{\bigcap_{j=0}^{n-1}\bar{R}(ja)\cap\{T_F\le t\}\right\}$ after the probability distribution transformation is given by $\left\{\bigcap_{j=0}^{n-1}\{s_c-S(ja,\mathbf{U}_{R,j})>0\}\cap\{T_F\le t\}\right\}$ with $\{T_F\le t\}=\{g(\mathbf{U}_F,t)\le 0\}$ according to (69.1), for example. $\mathbf{U}_{R,j}$ and $\mathbf{U}_F$ denote the variables in the random vector defining the damage indicator (including measurement errors) and the variables defining failure, respectively. Because $\mathbf{U}_{R,j}$ and $\mathbf{U}_F$ have some components in common the events are dependent. These dependencies can be taken into account by linearizing the event boundaries individually or, better, in the joint β-point, if it exists, computing the correlation coefficients of the scalar event functions and evaluating the corresponding multivariate normal integrals by the methods presented in [16]–[19]. The densities required in (69.34) and (69.35) are obtained by numerical differentiation of the corresponding probabilities.

Here, we allow the cost for first construction $C_R(\mathbf{p})$ to be different from the reconstruction cost $C(\mathbf{p})$. At an inspection time ja, the inspection either remains the only action taken with probability $\bar{P}_R(ja)$ and associated cost I_0 which need to be discounted, or the inspection is followed by (immediate) repair with probability $P_R(ja)$ involving cost $R(\mathbf{p})$, again to be discounted. The first terms in the respective sums correspond to (69.25) or to (69.28). All higher order summation terms correct for the possibilities of having repair intervals longer than a. The sums are expected to converge because no-repair probabilities decrease according to (69.16). In general, only the first few terms in the infinite sums must be considered.

The effect of dependencies between no-repair/repair and failure events on optimal repair intervals can be significant. This will be demonstrated in the example. As mentioned before, a repair causes the risk function to drop at the repair time. The minimal repair model considered in (69.29) or (69.36) lets the risk function drop but not down to zero at an inspection time because there is a finite probability that there is no repair. It produces a saw tooth type behavior of the risk function or the unconditional failure rate, which ultimately approach zero, *i.e.*, no more preventive renewals occur. Some calculations of these functions are illustrated in [9].

69.5 Example

The following example from [9] with different parameters shows several interesting features and provides an appropriate test case. Chloride attack due to salting and subsequent corrosion, for example, in the entrance area of a parking house or a concrete bridge is considered. A simplified and approximate model for chloride concentration in concrete is $C(x,t) = C_s(1 - erf(\frac{x}{2\sqrt{Dt}}))$, where C_s = surface (extrapolated from measurements 0.5 to 1 cm below surface) chloride content, x = depth and D = diffusion parameter. A suitable criterion for the time to the start of chloride corrosion of the reinforcement, if the parameters are properly adjusted, is:

$$C_{cr} - C_s(1 - erf\left(\frac{c}{2\sqrt{Dt}}\right)) \le 0\,, \qquad (69.40)$$

where, C_{cr} = critical chloride content, c = concrete cover and $erf(.)$ the error function. The stochastic model is as follows:

Variable	[unit]	Distr. function	Parameters
C_{cr}	%	Uniform	0.4, 0.6
C_s	%	Uniform	0.8, 1.2
c	cm	Log-normal	5,1
Dl	$\frac{cm^2}{year}$	Uniform	0.5, 1.2

The uniform distributions reflect the large uncertainty in the variables. If C_{cr} and C_s are measured as percentages of cement content, the initiation time can be written as:

$$T_i(C_{cr}, C_s, D, c) = \frac{c^2}{4D}\left(erf^{-1}\left[1 - \frac{C_{cr}}{C_s}\right]\right)^{-2}\,, \qquad (69.41)$$

and the initiation event can be written as:

$$G_i(t) = T_i(C_{cr}, C_s, D, c) - t > 0\ . \qquad (69.42)$$

The units are such that $T_i(.)$ is in years.

During the initiation time the structure can fail due to time-variant, stationary extreme loading. It is assumed that each year there is an independent extreme realization of the load. Load effects are normally distributed with coefficient of variation of 25%. Structural resistance is also distributed normally with a mean six times as large as the mean load effect and a coefficient of variation of 25%, implying a central safety factor of 6. Once corrosion has started the mean resistance deteriorates with rate $d(t) = 1 - 0.07t + 0.00002t^2$. The distribution function of the time to first failure is computed using (69.8) with the failure time distributions in the initiation phase and in the deterioration phase determined by (69.7). The structural states in two arbitrary time steps have constant correlation coefficient of $\rho = \rho_{ij} = 0.973$. The failure time distributions and failure time densities are computed using FORM in (69.8) because the dependence between failure in the initiation phase and the deterioration phase can be neglected. Here and in all subsequent calculations curvature corrections according to SORM are small to negligible. For the given parameters one determines a mean initiation time of $E[T_i] = 41.5$ and a mean time to failure of $E[T_d] = 12.3$ so that the total mean time to failure is $E[T_i + T_d] = 53.8$ with coefficient of variation $CoV = 0.57$.

The structure is in a condition where repair is deemed necessary if, at inspection by chemical analyses of the drill dust from small bore holes, the chloride concentration in a depth of $c = 3.0$ cm exceeds the value of C_{cr} = 0.5. Therefore, the repair event at the time of inspection t corresponds to

$$G_R(t) = t - T_i(0.5(1 + 0.05U_\varepsilon(t)), C_s, D, c) \le 0 \qquad (69.43)$$

where a normally distributed measurement error $U_\varepsilon(t)$ with $m_\varepsilon = 1.0$ and $\sigma_\varepsilon = 0.05$ has been added. The measurement errors at different times are independent. Because there can be additional errors in the measurement depth it is assumed that c varies lognormally with mean $m_c = 3.0$ and standard deviation $\sigma_c = 1$. It should be noted from comparison of (69.26) and (69.28) that no-repair/repair events at the time of inspections and the failure events are closely related, because both are realizations of the same underlying physical process. Their probabilities differ because of different times and random independent measurement errors. Repair times are modeled by a Rayleigh distribution.

For demonstration purposes the erection costs are $C(m_c, m_r) = C_0 + C_1 m_c^2 + C_2 m_r$, the inspection costs are $I_0 = 0.02C_0$, and we have $C_0 = 10^6$, $C_1 = C_2 = 10^4$, $L = 10C_0$, $\gamma = 0.03$. For preventive repairs the cost are $R(m_c, m_r) = 0.6C(m_c, m_r)$. m_r is the safety factor separating the means of load effect and resistance. All costs are in appropriate currency units. The physical and cost parameters are somewhat extreme but not yet unrealistic.

The technical realization of the models described before requires some effort in order to take proper account of the various dependencies. Independent no-repair/repair and failure events can be formulated as a special case of dependent no-repair/repair and failure events.

In the following cost optimization is first done with respect to the repair interval a keeping the design parameter, for example, the concrete cover, fixed at $m_c = 5$ cm.

Figure 69.2 shows the preventive repair times, the corrective repair times, and their sum cost for the cases defined by (69.26) and (69.28). Equation (69.28) is slightly lower because of longer discounting periods (time to failure or systematic repair + renewal time). In this figure, mean repair times are assumed to be only 5% of mean failure times.

Figure 69.3 shows the maintenance cost curves (inspection + repair + failure cost) for various means of repair times and dependent no repair/repair and failure events. As expected, the influence of realistic repair times (smaller than 5% to 10% of the mean failure times) is small.

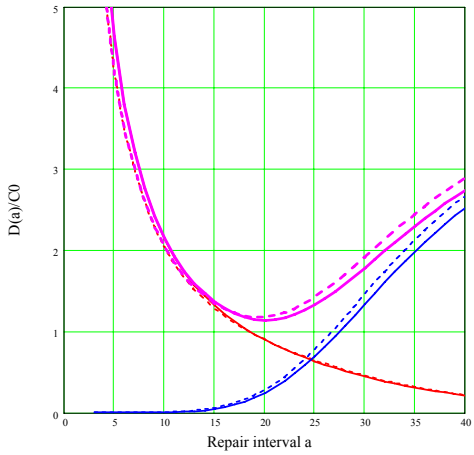


Figure 69.2. Damage costs for the model in (69.26) (*solid lines*) and. (69.28) (*dashed lines*)

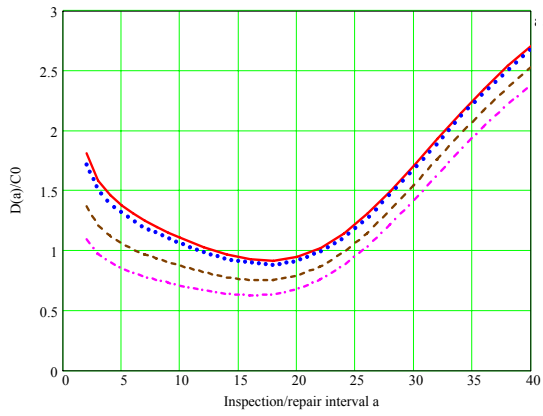


Figure 69.3. Maintenance costs for dependent no-repair/repair and failure events for different mean repair times (*solid line* = infinitely short, *dotted line* = m_R =0.5, *dashed line* = m_R =3.75, *dash-dotted line* m_R =7.2)

Figure 69.4 shows the total cost for independent no-repair/repair and failure events, for dependent no-repair/repair and failure events and for the case already discussed by Fox with finite repair times included. The mean repair time is 0.5. The optimum repair interval for the ideal case introduced by Fox and for the realistic dependent no repair/repair and failure events is 18 to 22 years,

but the total costs of maintenance are about 15% lower in the last case. For independent no repair/repair and failure events the minimum cost are for repair intervals of about 10 years but little difference is observed for repair intervals between 10 and 22 years. The total costs are about 50% higher. This illustrates that a realistic modeling is important.

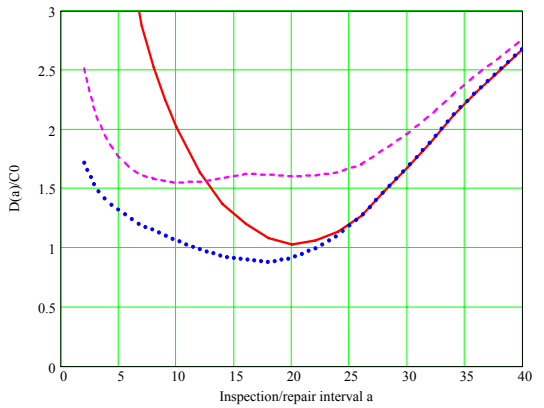


Figure 69.4. Maintenance costs for the model in (69.28) (*solid line*), (69.31) (*dashed line*) and. (69.39) (*dotted line*)

It is interesting to optimize simultaneously with respect to the inspection/repair interval, and the mean concrete cover taken as an important design parameter. Any suitable optimizer can be used for this operation. However, the mean concrete cover should have an upper limit around 6 cm to 7 cm because large concrete covers diminish the crack distributing effect of the reinforcement. Whatever this upper limit the optimum concrete cover will be at this upper limit and the optimal inspection/repair interval increases accordingly. The total maintenance costs decrease slightly. The same effect is observed if the safety factor enlarging the time T_d is increased. This demonstrates a strong interaction between the rules for design and maintenance, which, however, cannot be studied in more detail herein.

The benefit is not explicitly considered in this example. It would require numerical computation of the renewal function and from it the availability.

69.6 Summary

This chapter develops tools for optimizing design and maintenance strategies of aging structural components based on classical renewal theory. It reviews suitable formulations for failure models in structural engineering, which usually are non-analytic, and the basics of renewal theory. It then introduces a repair model with or without preceding (imperfect) inspections suitable for structural components. The inspection model introduces an increasing damage indicator function. Repairs are required if it exceeds some given threshold. Objective functions are derived for systematic reconstruction after failure or maintenance by periodic repairs alone and by periodic inspections and possibly ensuing repairs (renewals). Independent repair and failure events as well as dependent no-repair/repair and failure events are introduced. Some suitable numerical tools are also presented.

Extensions of the theory are possible with respect to facilities whose first failure time distribution is different from the other failure time distributions. Also, generalization to series systems is straightforward. Imperfect repairs cannot be handled within classical renewal theory.

References

[1] Rosenblueth E, Mendoza E. Reliability optimization in isostatic structures. Journal of the Engineering Mechanics, Division, ASCE, 97, EM6 1971; 1625–1642.

[2] Rackwitz R. Optimization – The basis of code making and reliability verification. Structural Safety 2000; 22(1):27–60.

[3] Streicher H, Rackwitz R. Renewal models for optimal life-cycle cost of aging civil infrastructures. IABMAS Workshop on Life-Cycle Cost Analysis and Design of Civil Infrastructure Systems and JCSS Workshop on Probabilistic Modeling of Deterioration Processes in Concrete Structures, Lausanne, 24.–26.3.2003 (eds. Frangopol DM, *et al*.,) ASCE, 2004; 401–412.

[4] Streicher H, Rackwitz R. Time-variant reliability-oriented structural optimization and a renewal model for life-cycle costing. Probabilistic Engineering Mechanics 2004; 19(1–2): 171–183.

[5] Cox DR. Renewal theory, London, Methuen, 1962.
[6] Barlow RE, Proschan F. Mathematical theory of reliability, Wiley, New York, 1965.
[7] Barlow RE, Proschan F. Statistical theory of reliability and life testing, Holt, Rinehart and Winston, New York, 1975
[8] Fox B. Age replacement with discounting, Operations Research 1966; 14: 533–537.
[9] Streicher H, Joanni A, Rackwitz R. Cost–benefit optimization and risk acceptability for existing, aging but maintained structures. Structural Safety 2008; 30: 375–393.
[10] Joanni A, Rackwitz R. Cost–benefit optimization for maintained structures by a renewal model. Reliability Engineering and Systems Safety. 2006; 93: 489–499.
[11] Hohenbichler M, Rackwitz R. Non-normal dependent vectors in structural safety. Journal of Engineering Mechancis, ASCE, 1981; 107(6):1227–1249.
[12] Hohenbichler M, Gollwitzer S, Kruse W, Rackwitz R. New light on first- and second-order reliability methods, Structural Safety, 1987; 4(4): 267–284.
[13] Rackwitz R. Reliability analysis – A review and some perspectives. Structural Safety 2001; 23(4): 365–395.
[14] Madsen HO, Krenk S, Lind NC. Methods of structural safety. Prentice-Hall, Englewood Cliffs, NJ, 1986
[15] Au S-K, Beck JL. First excursion probabilities for linear systems by very efficient importance sampling. Probabilistic Engineering Mechanics 2001; 16(3):193–207.
[16] Hohenbichler M, Rackwitz R. First-order concepts in system reliability. Structural Safety 1983; 1(3): 177–188.
[17] Gollwitzer S, Rackwitz R. An efficient numerical solution to the multinormal integral. Probabilistic Engineering Mechanics 1988; 3(2):98–101.
[18] Pandey MD. An effective approximation to evaluate multinormal integrals. Structural Safety 1998; 20(1): 51–67.
[19] Genz A. Numerical computation of multivariate normal probabilities. Computational and Graphical Statistics 1992; 1:141–149.
[20] Ayhan H, Limon-Robles J, Wortman MA. An approach for computing tight numerical bounds on renewal function. IEEE Transactions on Reliability 1999; 48(2): 182–188.
[21] Brown M, Proschan F. Imperfect Repair. Journal of Applied Probability 1983; 20: 851–859.
[22] Pham H, Wang H. Imperfect maintenance. European Journal of Operational Research 1996; 94: 425–438.
[23] von Neumann J, Morgenstern A. Theory of games and economical behavior. Princeton University Press, 1943.
[24] Rackwitz R, Lentz A, Faber M. Socio-economically sustainable civil engineering infrastructures by optimization. Structural Safety 2005; 27(3): 187–229.
[25] Hasofer AM, Rackwitz R. Time-dependent models for code optimization. Proceedings of ICASP8 Conference, Sydney, 12–15 Dec., 1999, (ed. Melchers RE, Stewart MG), Balkema, Rotterdam 2000; 1:151–158.
[26] Ran A, Rosenlund SI. Age replacement with discounting for a continuous maintenance cost model. Technometrics 1976; 18(4): 459–465.
[27] Van Noortwijk JM. Cost-based criteria for obtaining optimal design decisions. In: Corotis *et al*., (eds.) Proceedings ICOSSAR 01, Newport Beach 23–25 June, Structural Safety and Reliability, Sweets and Zeitlinger, Lisse, 2001.

Reliability and Price Assessment and the Associated Risk Control for Restructured Power Systems

Yi Ding[1], Ming J. Zuo[1], and Peng Wang[2]

[1]Department of Mechanical Engineering, University of Alberta, Canada
[2]Power Division, School of EEE, Nanyang Technological University, Singapore

Abstract: Electric utilities are experiencing restructuring throughout the world. The reliability techniques used for conventional power systems cannot be directly applied in the new environment. Moreover, electricity pricing in a restructured power system has become a major problem due to the changes in market structure. This chapter addresses reliability and price issues in restructured power systems. A technique to evaluate nodal prices and nodal reliabilities considering the correlation between price and reliability in a restructured power system with the Poolco market model is developed. The reliability network equivalent and the improved optimal power flow model for evaluation of reliabilities and prices in a restructured power system with the hybrid market structure are presented. Moreover, a penalty schema for reducing electricity price volatility and improving customer reliabilities is also discussed.

70.1 Introduction

The conventional electric power industry has been controlled and managed by large owners for nearly 100 years. In a relatively large geographical area, all the electric power facilities are usually owned by a single owner, who has a monopoly of electricity generation, transmission, and distribution systems. Electric energy and other ancillary services such as spinning reserve, frequency control, and reactive power generation are closely coordinated under the umbrella of one or more control centers. Electricity prices are usually determined by the administration and fixed for the same type of customers at different locations. Customers cannot select their suppliers and are obliged to receive services from monopoly utilities. Such power systems are called vertically integrated power systems.

Since the last decade, the restructuring of the traditional vertically integrated electric power system has been going on all over the world. The main objective of power system deregulation is to introduce competition in the power industry, where incumbent utilities have become inefficient [1], and provide more choices to market participants in the way they trade electricity and ancillary services. One traditional utility is separated into different generation companies (gencos), transmission companies (transcos) and distribution companies (discos), and retail companies [2]. Generally speaking, the market models can be classified into Poolco, bilateral contracts, and hybrid models [23].

Electric power system deregulation has occurred not only in industrialized counties but also in developing countries. South America was seen as the pioneer in the process of power industry restructuring [2], [3]. Chile was the first country to start the restructuring process in 1982 and other Latin American countries such as Argentina (1992), Peru (1993), Bolivia (1994), Colombia (1994), and Brazil (1996) followed [4]. It was shown that the power system restructuring in South America was very successful: in Chile the power losses in the transmission and distribution networks came down from 21% in 1986 to 8.6%; in Argentina the average electricity price was reduced from 39$/MWh in 1994 to 32$/MWh in 1996, and the availability of thermal generation units increased from below 47% in 1992 to 75% in 1996 [4] [5] [6].

The UK was the first developed country to start power industry deregulation. The electric power industry was the last major state-owned industry to be deregulated, and the process of privatization began in 1988 [7],[8] with the implementation of the Electricity Act. The Central Generating Board (CEGB), which owned nearly 60,000 MW of capacity and all high voltage transmission lines in Britain, was broken down into four independent companies [6], [7]: National Power, Power Gen, Nuclear Electric and the National Grid Company (NGC), with Nuclear Electric and NGC being state-owned companies. NGC operates the centralized power pool and assumes the role of the independent system operator (ISO) with the responsibility of promoting competition and managing the activities of the market [9]. The electricity distribution companies emerged from the former privatized regional area boards [7].

The USA has the largest number of electricity markets in the world. Unlike most other countries, the individual states in the USA have the right to develop their own market structures and implement the restructuring of the power industry. However, they must be directed by the Federal Energy Regulatory Authority (FERC) Acts [2]. The California power market was the first deregulated power market in USA, which opened in 1998. The PJM interconnection has the largest electric power market in the world.

Reliability is the main concern of power system planning and operation. In a conventional system, reliability is centrally controlled and managed by system operators. Most techniques focus on system reliability. System operators concentrate more on system reliability than customer reliability. Therefore generation re-dispatching and load shedding after a contingency are usually determined by a system operator based on their experience and judgment with little concern for customer requirements. The main objective of contingency management is to solve system voltage, line overloading, frequency, and power balance problems.

Restructuring and deregulation result in the functional segregation of a vertically integrated utility into distinct utilities in which each performs a single function. Economic segregation and service unbundling have changed the conventional mechanism of reliability management and system operation. One of the most important changes for the restructured power systems was the introduction of the ancillary market and customer participation in reliability management.

In the new environment, a customer can select the power and reserve providers who can satisfy his price and reliability expectations. This has changed the fundamentals of system reliability management and introduced new issues regarding electricity price. Electricity pricing has become an important issue in the restructured system due to the different usages of transmission and distribution facilities, reserve requirements, and customer choices regarding price and reliability. The system-oriented reliability assessment and management techniques developed for conventional vertically integrated systems need to be revised and improved for application in restructured power systems.

Due to the different market structures in the existing restructured power systems, the reliability and price problems for various market models are different. Therefore, the corresponding aspects considered in reliability and price assessment for various market models are different. The Poolco model and the hybrid model are the most important and popular market models in restructured power systems.

In the Poolco model, the market participants trade electricity through a centralized power pool. The electricity prices are uncertain due to the random nature of system failures and demand. Inadequate generation and transmission congestions caused by random failures may result in extreme price volatility, called "price spikes". The demand in the Poolco model is elastic. Customer response to price and reliability has changed the mechanism of load shedding from the supply side to the demand side. Therefore, the electricity price and supply point reliability are correlated due to customer participation of market trading. These aspects should be considered in the nodal price and nodal reliability evaluation of restructured power systems with the Poolco model. The techniques for evaluating reliabilities and prices for the Poolco model are discussed in Section 70.2. Part of this section has been published in [24].

In restructured power systems with hybrid market structure, generation companies (or customers) can sell (or buy) electricity either from a centralized power pool or directly through bilateral contracts. Due to market price uncertainties, risk-averse customers (or suppliers) can engage in long-term and firm bilateral contracts that guarantee supply (or selling) of power and reserve at relatively stable prices. Risk-prone customers (or suppliers) will respond to the spot market to buy (or sell) the same power and reserve for a possibly lower (or higher) price. A generation company can also sell their reserve capacity to the reserve market for system reliability requirements. In addition to reserve capacity payment, a genco will also receive the payment when its reserve capacity is utilized in contingency states. These flexible choices on reliability and prices for market participants have changed the mechanism of price and reliability managements, and have also created many new problems regarding reliability and price modeling and assessment. On the other hand, prices and reliabilities are also correlated. High reliability requirements from some customers will cause the increase of prices and higher prices will result in the decrease in demands from customers with low reliability requirements. Corresponding techniques to evaluate reliabilities, prices, and the associated risks for different participants are required to incorporate these changes. The methods for evaluating reliabilities and prices for hybrid model are discussed in Section 70.3; some parts of which have been published in [25].

The market participants in restructured power systems with Poolco or hybrid market structures may receive high price volatilities or even "price spikes" during contingency states. How to control electricity prices and mitigate high price volatilities is one of the most important problems that system operators face and are required to solve in the new environment. In restructured power systems, system operators usually do not have the power to directly control the electricity prices by setting some regulated values. In these cases, gencos may implement their market powers to raise market electricity prices to make more profit. Therefore, it is important to develop some mechanism for system operators to be able to indirectly control electricity prices and price risks in the new environment. A schema for controlling electricity price volatilities and improving system reliabilities is proposed in Section 70.4, some parts of which have been reported in [26].

Notation

j_0	normal system state index
j	contingency system state index
i,k	bus index
c	component index
g	generating unit index
s	customer sector index
N_c	number of components
N_g	number of generating buses
N_L	number of load buses
N	total number of buses
CDF	customer damage function
A_c	availability of a component
U_c	unavailability of a component
λ_c	failure rate of a component
μ_c	repair rate of a component
SN	the number of states considered

For state j_0, bus i and customer sector s of Poolco model:

p_0 state probability

P_{is}^{j0} real power demand

Q_{is}^{j0} reactive power demand

ρ_{pi}^{j0} nodal price of real power

ρ_{qi}^{j0} nodal price of reactive power

For state j, bus i ,unit g and customer sector s of Poolco model:

p_j state probability

D_j departure rate of system leaving state

d_j mean failure duration

NG_i^j number of generating units

NL_i^j number of customer sectors

C_{ig}^j cost function of a generating unit

OC_{is}^j outage cost of the customer sector

$CDF_s(d_j)$ *CDF* of customer sector s for d_j

θ_i^j voltage angle

$Y_{ik}^j = \left|Y_{ik}^j\right| \angle \delta_{ik}^j$ element of the admittance matrix

P_i^j real power injection

Q_i^j reactive power injection

P_{ig}^j real power generation of the unit

$P_{ig}^{j,\min}$ minimum real power generation of the unit

$P_{ig}^{j,\max}$ maximum real power generation of the unit

$\Delta P_{ig}^{j,low}$ lower limit on real power generation of the unit that can be changed from the normal state

$\Delta P_{ig}^{j,upp}$ upper limit on real power generation of the unit that can be changed from the normal state

Q_{ig}^j reactive power generation of the unit

$Q_{ig}^{j,\min}$ minimum reactive power output of the unit

$Q_{ig}^{j,\max}$ maximum reactive power output of the unit

LC_{pis}^j real power curtailment of the customer sector

$LC_{pis}^{j,\max}$ maximum real power curtailment of the customer sector

$V_i^j = \left|V_i^j\right| \angle \theta_i^j$ bus voltage

$\left|V_i^j\right|^{\max}$ upper limit of bus voltage

$\left|V_i^j\right|^{\min}$ lower limit of bus voltage

S_{ik}^j apparent power on line *i*-*k*

$S_{ik}^{j,\max}$ limits of apparent power transfer on line *i*-*k*

For state j and bus i of the hybrid model:

$V_i^j = \left|V_i^j\right| \angle \theta_i^j$ bus voltage

$Y_{ik}^j = \left|Y_{ik}^j\right| \angle \delta_{ik}^j$ element of the admittance matrix

NG_i^{pj} set of pool generating units

NL_i^{pj} set of pool customer sectors

C_{ig}^{pj} cost function of pool generating unit g

CC_{is}^{pj} curtailment cost of pool customer sector s

P_{ig}^j real power generation of unit g

Q_{ig}^j reactive power generation of unit g

ΔP_{ig}^j $= P_{ig}^0 - P_{ig}^j$

$\Delta P_{ig}^{j,low}$ lower limit of ΔP_{ig}^j

$\Delta P_{ig}^{j,up}$ upper limit of ΔP_{ig}^j

P_{is}^{pj} real power demand of pool customer sector s

Q_{is}^{pj} reactive power demand of pool customer sector s

CP_{is}^{pj} real power curtailment of pool customer sector s

CQ_{is}^{pj} reactive power curtailment of pool customer sector s

P_i^j nodal real power injection

RG_i^j set of reserve generating units

C_{ig}^{rj} cost function of reserve generating unit g

P_{ig}^{rj} real power provided to the pool by reserve unit g

Q_{ig}^{rj} reactive power provided to the pool by reserve unit g

$P_{ig}^{rj,\max}$ maximum real power reserve of unit g

$Q_{ig}^{rj,\max}$ maximum reactive power reserve of unit g

NL_i^{bj} set of bilateral customer sectors

For state j, and bilateral contract between bus i and k of hybrid model:

P_{ik}^{bj} real power contract

Q_{ik}^{bj} reactive power contract

CP_{iks}^{bj} real power curtailment of bilateral customer sector s

CQ_{iks}^{bj} reactive power curtailment of bilateral customer sector s

$CP_{iks}^{b,\max}$ maximum real power curtailment of bilateral customer sector s

CC_{iks}^{bj} curtailment cost function of bilateral customer sector s

70.2 Reliability and Price Assessment of Restructured Power Systems with the Poolco Market Model

In the Poolco market model, the market participants trade electricity through a centralized power pool. The real time (spot) pricing systems developed by Vickerry [10] and Schweppe, *et al.* [11] have been implemented to determine electricity prices.

There are three spot pricing systems prevalent in the present power markets [12]: the uniform marginal pricing system, the zonal marginal pricing system, and the nodal pricing system. In the first pricing system there is only one price, which is called the uniform marginal price. The electricity market in the U.K. [6] and the Alberta market have implemented such a pricing system. In the second one there are several prices in the market but only one price in a given zone, which can be named the zonal marginal price. The Norwegian market is a typical example of this model [12]. The last one is the nodal pricing system, in which different nodes have different prices. Typical examples of power markets implementing the nodal pricing system are the current California market, the Pennsylvania-New Jersey-Maryland market (PJM) [13], the New Zealand market [6] [12], and the New York market [14]. Currently the nodal pricing system is being adopted by more and more power markets because of its economical efficiency and fairness. Therefore, the techniques for nodal reliability and nodal price assessment are comprehensively discussed below.

Nodal prices in a Poolco market depend on generating unit locations, available generation capacity, and demand at each node, transmission limits, and customer response to price. Nodal price and nodal reliability are correlated. It is a complicated optimization problem to obtain the balance point between demand and price. In the following paragraphs of this section, the characteristics of customer demand response to nodal price are investigated. Nodal price and nodal reliability problems are formulated using optimal power flow and reliability evaluation techniques. Price volatilities due to random failures are investigated. The expected nodal price and associated deviation are introduced to represent the volatility of nodal prices caused by random failures. The IEEE-RTS [15] test system has been analyzed to illustrate the technique.

70.2.1 Customer Response to Price Changes

When a power system transfers from the normal operating state to a contingency state due to random failures, nodal prices may change with the system operating condition. Some customers may reduce their demands when nodal prices increase dramatically. The demand that a customer is willing to reduce is designated as the self-load curtailment in this chapter. The objective of self-load curtailment for a customer is to maximize its benefit. For state *j*, the self-load curtailment for customer i can be determined by solving the following optimization problem:

$$Max\ \Phi = B(P_{di}^0) - OC(P_{di}^0 - P_{di}^j) - \rho^j \times P_{di}^j \quad , \quad (70.1)$$

where P_{di}^0 is the equilibrium demand for the normal operating state, P_{di}^j is the demand for contingency state *j*, ($P_{di}^0 - P_{di}^j$) is the demand that a customer is willing to reduce, $B(P_{di}^0)$ is the customer benefit for the normal operating state, $OC(P_{di}^0 - P_{di}^j)$ is the cost due to load reduction, and ρ^j is the price of electricity for state *j*.

The necessary condition to maximize the welfare is:

$$\frac{\partial(OC(P_{di}^0 - P_{di}^j))}{\partial(P_{di}^0 - P_{di}^j)} = \rho^j . \quad (70.2)$$

Equation (70.2) shows that a customer will reduce his demand when the price of electricity is higher than the customer marginal cost at state *j*. This means that when a system transfers from the normal operating state to a contingency state, customer response can be indirectly measured by the customer interruption cost, which represents the customer's willingness to pay to avoid service interruption. The interruption cost is a function of customer and interruption characteristics [16], which include the diversity of customers, the nature of customer activities, and the size of the operation, *etc*. A Standard Industrial Classification (*SIC*) [16] has been used to divide customers into large user, industrial, commercial, agriculture, residential, government and institutions, and office and buildings categories. The survey data have been analyzed to give the sector customer damage functions (CDF_s).

70.2.2 Formulation of the Nodal Price and the Nodal Reliability Problem

The basic problem is to solve the nodal price and nodal reliability for each system state considering their correlation. The basic reliability technique is used to determine the state probability, departure the rate, and duration [17]. Contingency enumeration and state selection techniques have been used to determine the contingency states. Optimal power flow (OPF) techniques have been used to obtain the economical information regarding the system operation. The Lagrange multipliers evaluated by the solutions of OPF can be explained as the derivatives of the objective function with respect to the respective constraints [7]. Therefore, the Lagrangian multipliers corresponding to the power flow equations are interpreted as the marginal costs of electric power injected from the system to the corresponding nodes (nodal prices). In the proposed model customer damage functions and generation cost functions are used in the OPF problems to determine nodal price, load curtailed, and generation re-dispatched for each state. The probabilistic method is used to determine the expected values and the associated risk of nodal prices and nodal reliabilities. Considering a power system with N_c independent components, the reliability parameters for contingency state *j* with exactly *b* failed components can be determined using the following equations:

$$p^j = \prod_{c=1}^{b} U_c \prod_{c=b+1}^{N_c} A_c , \quad (70.3)$$

$$D^j = \sum_{c=1}^{b} \mu_c + \sum_{c=b+1}^{N_c} \lambda_c , \quad (70.4)$$

$$d^j = 1 \Big/ D_j . \quad (70.5)$$

For a contingency state, the objective of the optimization is to minimize the total system cost including the generation cost and customer interruption cost due to load curtailment. For system state *j*, the nodal prices, the generation re-

dispatched, and load shed considering customer requirements can be determined by solving the following optimization problem:

$$Min\ f^j = \sum_{i\in N_g}\sum_{g\in NG_i^j} C_{ig}^j(P_{ig}^j, Q_{ig}^j) + \sum_{i\in N_L}\sum_{s\in NL_i^j} OC_{is}^j(LC_{pis}^j, LC_{qis}^j) \quad (70.6)$$

where

$$OC_{is}^j(LC_{pis}^j, LC_{qis}^j) = LC_{pis}^j \times CDF_s(d_j)\ , \quad (70.7)$$

subject to the following constraints:

Load flow equations:

$$\sum_{g\in NG_i^j} P_{ig}^j - \sum_{s\in NL_i^j} P_{is}^{j_0} + \sum_{s\in NL_i^j} LC_{pis}^j = \sum_{i=1}^{N} V_i^j V_k^j \left|Y_{ik}^j\right| \cos(\theta_i^j - \theta_k^j - \delta_{ik}^j) \quad (70.8)$$

$$\sum_{g\in NG_i^j} Q_{ig}^j - \sum_{s\in NL_i^j} Q_{is}^{j_0} + \sum_{s\in NL_i^j} LC_{qis}^j = \sum_{i=1}^{N} V_i^j V_k^j \left|Y_{ik}^j\right| \sin(\theta_i^j - \theta_k^j - \delta_{ik}^j) \quad (70.9)$$

Generating unit limits:

$$P_{ig}^{j,\min} \le P_{ig}^j \le P_{ig}^{j,\max}\ , \quad (70.10)$$

$$Q_{ig}^{j,\min} \le Q_{ig}^j \le Q_{ig}^{j,\max}\ , \quad (70.11)$$

$$\Delta P_{ig}^{j,low} \le P_{ig}^j - P_{ig}^{j_0} \le \Delta P_{ig}^{j,upp}\ . \quad (70.12)$$

Load curtailment limits:

$$0 \le LC_{pis}^j \le LC_{pis}^{j,\max}\ . \quad (70.13)$$

Voltage limits:

$$\left|V_i^j\right|^{\min} \le \left|V_i^j\right| \le \left|V_i^j\right|^{\max}\ . \quad (70.14)$$

Line flow constraints:

$$\left|S_{ik}^j\right| \le S_{ik}^{j,\max}\ . \quad (70.15)$$

The nonlinear optimization problem can be solved by using various Newton methods with the second order convergence properties. However, additional algorithms have to be supplemented to search for active inequality constraints, which usually affect convergence properties of Newton methods [18].

The sequential quadratic programming (SQP) algorithm [19], which combines the Newton method with quadratic programming has been used to solve this problem. The Lagrangian function L^j of the problem (70.6)–(70.15) for state j is formed. The optimal generating unit outputs (P_{ig}^j, Q_{ig}^j), and the optimal load curtailments for customer sector (LC_{pis}^j, LC_{qis}^j) can be obtained using SQP. The nodal prices of active power and reactive power at bus i under the optimum solution are the following, respectively:

$$\rho_{pi}^j = \frac{\partial L_j}{\partial P_i^j}\ , \quad (70.16)$$

$$\rho_{qi}^j = \frac{\partial L_j}{\partial Q_i^j}\ . \quad (70.17)$$

In a Poolco market, the expected values, the standard deviation of nodal prices, and nodal reliabilities are important information for the risk analysis of market trading, planning, and operation. The expected nodal price is a weighted average of the prices for different states. Unlike many other commodities, electricity cannot be stored in a large amount and needs the continuous balance between the supply and demand at any time. The price for a contingency state might be quite different from the expected price. Inadequate generation and congestions in some contingency states result in extreme price volatility or "price spikes". The random nature of failures results in a great price uncertainty. Standard deviation of nodal prices can be used to evaluate the extent of price fluctuating around its expected value.

Considering all possible system states, the expected nodal prices, and nodal reliability indices can be determined using following equations.

The expected nodal price of real power:

$$\overline{\rho}_{pi} = \sum_{j=1}^{SN} p^j \rho_{pi}^j\ . \quad (70.18)$$

The standard deviation of $\overline{\rho}_{pi}$:

$$\sigma_{pi} = \sqrt{\sum_{j=1}^{SN} (\rho_{pi}^j - \overline{\rho}_{pi})^2 p^j}\ . \quad (70.19)$$

The expected nodal energy not supplied:

$$ENENS_i = \sum_{j=1}^{SN} D^j \times p^j \times NENS_i^j\ . \quad (70.20)$$

The expected interruption cost for the bus i :

$$ENCOST_i = \sum_{j=1}^{SN} D^j \times p^j \times NCOST_i^j \ . \quad (70.21)$$

70.2.3 System Studies

The technique has also been used to analyze a more complex system IEEE-RTS. IEEE-RTS has 10 generating (PV) buses, 17 load (PQ) buses, 33 transmission lines, 5 transformers, and 32 generating units. The total installed generating capacity for this system is 3405 MW with a system peak load of 2850 MW. System failures up to the second order have been considered in the evaluation. The nodal reliability indices, nodal prices, and the corresponding risks of the nodal prices have been calculated for each bus. The nodal prices for a representative bus (bus 3) are shown in Figures 70.1 and 70.2. The nodal prices of real power are presented therein. There are no price spikes and load shedding for the first order failures.

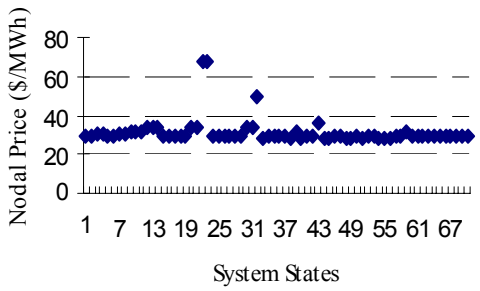


Figure 70.1. Nodal prices at bus 3 for the first order generation and transmission outages

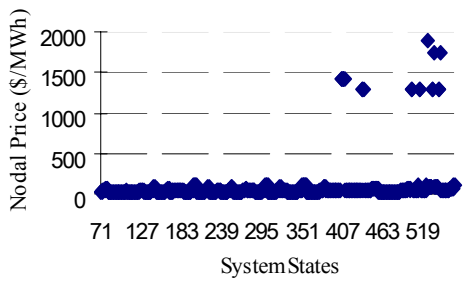


Figure 70.2. Nodal prices at bus 3 for the second order generation outages

70.3 Reliability and Price Assessment of Restructured Power Systems with the Hybrid Market Model

In restructured power systems with hybrid market structure, market participants can trade electricity either from a centralized power pool or directly through bilateral contracts. Therefore, the hybrid market model is a more flexible and complicated market structure than the Poolco model. This section reports techniques for evaluating both reliabilities and prices for the pool and bilateral customers in a hybrid power market. The reliability network equivalent techniques are extended to represent different generation suppliers in a hybrid market and to incorporate the complicated agreements or contracts among gencos in the reliability and price evaluation. The reliability and price problem for hybrid market models is formulated simultaneously using an improved OPF technique considering the correlation between reliability and price.

70.3.1 Reliability and Cost Models for Market Participants

Most power markets in the world are hybrid market models such as PJM [13], due to their flexibility to incorporate customer choices. In a hybrid power market customers can buy electricity either from the centralized power pool or directly from gencos through bilateral contracts. Different market rules and agreements are also present in this type of market. In order to clearly present the complicated relationship among these rules and agreements, and to evaluate generation and transmission reliabilities and prices, reliability and price models of market participants are introduced. There are two generation providers of the power pool and bilateral contract in a hybrid power market. All the gencos scheduled in power pool can be represented as an equivalent multi-state pool generation provider (EMPGP). A genco with bilateral contracts can be represented as an equivalent multi-state bilateral generation provider (EMBGP) as shown in Figure 70.3.

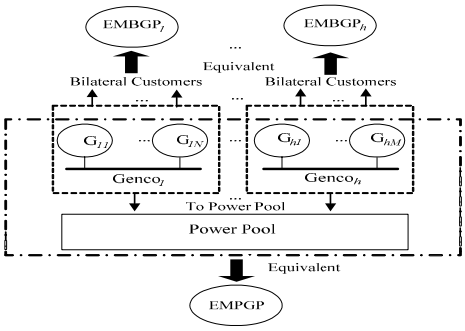


Figure 70.3. Generation system equivalent

The reliability parameters of an EMPGP or an EMBGP are represented using the state probability, departure rate and frequency. For an EMPGP with H gencos, the probability p^j, the departure rate D^j, and the frequency f^j for state j can be determined by the following equations, assuming that genco h in the pool has N_h units and M_h^j of these are out of service:

$$p^j = \prod_{h=1}^{H} \left(\prod_{g_h=1}^{M_h^j} U_{g_h} \prod_{g_h=M_h^j+1}^{N_h} A_{g_h} \right) , \tag{70.22}$$

$$D^j = \sum_{h=1}^{H} \left(\sum_{g_h=1}^{M_h^j} \mu_{g_h} + \sum_{g_h=M_h^j+1}^{N_h} \lambda_{g_h} \right) , \tag{70.23}$$

$$f^j = p^j D^j , \tag{70.24}$$

where A_{g_h}, U_{g_h}, λ_{g_h}, and μ_{g_h} are the availability, unavailability, failure rate, and repair rate of unit g in genco h, respectively. The reliability parameters of an EMBGP can be determined using similar equations. The unit operating cost is usually the function of unit output and is represented by a quadratic equation. The cost model of an EMPGP or an EMBGP is the aggregation of the cost functions of all the units in it, which changes correspondingly with the system state.

EMPGPs and EMBGPs can share their reserves to increase supply reliabilities and to reduce price risks. An EMPGP, which has reserve agreements (RA) with other EMBGPs, can be represented using an equivalent multi-state pool generation provider with reserve agreement (EMPGPWR) and an EMBGP, which has reserve agreements with other EMBGPs or the EMPGP, can be represented using an equivalent multi-state bilateral generation provider with reserve agreements (EMBGPWR).

The reliability parameters of EMPGPWR and EMBGPWR can be calculated using the reserve assisting method [17]. If the EMPGP and M EMBGPs share their reserve, the reliability parameters of the EMPGPWR or an EMBGPWR can be calculated as:

$$p_{h+l}^j = p_{h+l-1}^j p_l^k , \tag{70.25}$$

$$D_{h+l}^j = D_{h+l-1}^j + D_l^k , \tag{70.26}$$

$$f_{h+l}^j = p_{h+l}^j D_{h+l}^j , \tag{70.27}$$

where p_{h+l-1}^j and D_{h+l-1}^j are the probability and the departure rate of the assisted EMPGP (or EMBGP h) before adding the assisting EMBGP l (or EMPGP), respectively, and p_l^k and D_l^k are the probability and the departure rate of state k for EMBGP l.

The effect of the transmission network on load point reliabilities and prices can be represented using nodal reliabilities and prices. The transmission system between the EMPGP and a bulk load point (BLP) can be represented by an equivalent multi-state transmission provider for pool customers (EMTPP). The transmission system between an EMBGP and a BLP can be represented by an equivalent multi-state transmission provider for bilateral customers (EMTPB). The EMTPP (or EMTPB) considering reserve agreements is designated as EMTPPWR (or EMTPBWR), respectively. These equivalents are shown in Figure 70.4.

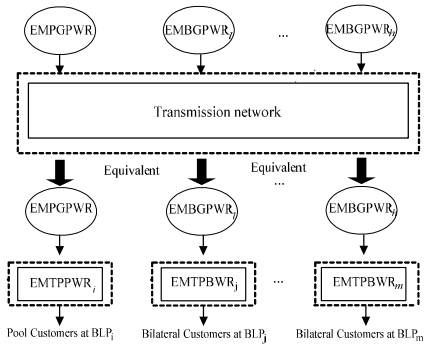


Figure 70.4. Transmission system equivalent

70.3.2 A Model of Customer Responses

If a power system transfers from the normal operating state to a contingency state due to random failures, prices may change with the system operating condition. When demand cannot be met by a power pool, the pool customers will either buy electricity from EMBGPs if there are reserve agreements or compete for the insufficient electricity. Therefore, the customer damage function (CDF_s) [16], is used to model pool customer response to load curtailment.

When generation failures in an EMBGP result in inadequate generation, bilateral customers may buy electricity from the pool or shed the load if the spot price is too high. The power transfer price may also increase due to transmission failures. If the power transfer cost is higher than the customer willingness to pay for it, the power transferred may be reduced. The bilateral sector customer damage function (BCF_s) is used to reflect the bilateral customer sector willingness to pay for the power transfer to avoid curtailing.

70.3.3 Formulations of Reliability and Price Problems

The objective of the problem is to determine customer load curtailment and nodal price through minimizing the total system cost using the OPF technique for each inadequacy state. The problems for two structures are formulated using the OPF technique based on the proposed reliability, price, cost, and response models.

Firstly the hybrid market model without reserve agreements is considered. In this model, electricity is traded through the pool and bilateral contracts, and there are no reserve agreements among market participants.

In this case, a new item is added to (70.6) to include the curtailment costs of bilateral contracts. New constraints are introduced for the bilateral contracts. The objective function becomes:

$$\begin{aligned} Min\ f^j = & \sum_{i\in N_g}\sum_{g\in NG_i^{pj}} C_{ig}^{pj}(P_{ig}^j, Q_{ig}^j) + \\ & \sum_{i\in N_L}\sum_{s\in NL_i^{pj}} CC_{is}^{pj}(CP_{is}^{pj}, CQ_{is}^{pj}) + \\ & \sum_{i\in BC_i}\sum_{\substack{k\in BC_i \\ k<i}}\sum_{s\in NL_i^{bj}} CC_{iks}^{bj}(CP_{iks}^{bj}, CQ_{iks}^{bj}) \end{aligned} \tag{70.28}$$

where the interruption costs of the pool customer are:

$$CC_{is}^{pj}(CP_{is}^{pj}, CQ_{is}^{pj}) = CP_{is}^{pj} \times CDF_s(1/D^j). \tag{70.29}$$

The curtailment cost of bilateral contract is:

$$CC_{iks}^{bj}(CP_{iks}^{bj}, CQ_{iks}^{bj}) = CP_{iks}^{bj} \times BCF_s(1/D^j) \tag{70.30}$$

subject to the following constraints.

Modified power flow constraints:

$$\begin{aligned} & \sum_{g\in NG_i^{pj}} P_{ig}^j - \sum_{s\in NL_i^{pj}}(P_{is}^{p0} - CP_{is}^{pj}) - \sum_{k\in BC_i}(-1)^{\beta}(P_{ik}^{bj} - \sum_{s\in NL_i^{bj}} CP_{iks}^{bj}) \\ & = \sum_{k=1}^{N} |V_i^j||V_k^j||Y_{ik}^j|\cos(\theta_i^j - \theta_k^j - \delta_{ik}^j) \end{aligned} \tag{70.31}$$

$$\begin{aligned} & \sum_{g\in NG_i^{pj}} Q_{ig}^j - \sum_{s\in NL_i^{pj}}(Q_{is}^{p0} - CQ_{is}^{pj}) - \sum_{k\in BC_i}(-1)^{\beta}(Q_{ik}^{bj} - \sum_{s\in NL_i^{bj}} CQ_{iks}^{bj}) \\ & = \sum_{k=1}^{N} |V_i^j||V_k^j||Y_{ik}^j|\sin(\theta_i^j - \theta_k^j - \delta_{ik}^j) \end{aligned} \tag{70.32}$$

where control variable $\beta = 0$ if i is a sink bus of bilateral contract, and $\beta = 1$ if i is a source bus for bilateral contract. The re-scheduled bilateral contracts P_{ik}^{bj} and Q_{ik}^{bj} in (70.31) and (70.32) are determined from the EMBGP using reliability equivalent techniques.

Generating unit limits:

$$P_{ig}^{\min} \le P_{ig}^j \le P_{ig}^{\max}, \tag{70.33}$$

$$Q_{ig}^{\min} \le Q_{ig}^j \le Q_{ig}^{\max}, \tag{70.34}$$

$$\Delta P_{ig}^{j,low} \le P_{ig}^j - P_{ig}^0 \le \Delta P_{ig}^{j,up}. \tag{70.35}$$

Curtailment limits of pool customer sectors:

$$0 \le CP_{is}^{pj} \le CP_{is}^{\max}. \tag{70.36}$$

Curtailment limits of bilateral customer sectors:

$$0 \le CP_{iks}^{bj} \le CP_{iks}^{b,\max}. \tag{70.37}$$

Voltage limits:

$$|V_i|^{\min} \le |V_i^j| \le |V_i|^{\max}. \tag{70.38}$$

Line flow constraints:

$$\left|S_{ik}^{j}\right| \le \left|S_{ik}^{j}\right|^{\max} . \tag{70.39}$$

The Lagrangian function L^j of the problem (70.28)–(70.39) for state j is formed and solved to provide the optimal generating unit outputs (P_{ig}^{j}, Q_{ig}^{j}), the curtailments for pool customer sector ($CP_{is}^{pj}, CQ_{is}^{pj}$), and the curtailment of bilateral contract ($CP_{iks}^{bj}, CQ_{iks}^{bj}$). The nodal prices of active power for the pool customers at bus i under the optimum solution can be obtained using the following equation:

$$\rho_i^j = \frac{\partial L^j}{\partial P_i^j} . \tag{70.40}$$

The price for a bilateral contract customer can be determined using the following equation based on the contractual price π_{ik} and the transfer price T_{ik}^{j}, which is calculated as the difference in nodal prices between bus *i* and *m:*

$$\rho_i^j = \pi_{ik} + T_{ik}^{j} . \tag{70.41}$$

Secondly the hybrid market model with reserve agreements is considered. Compared with (70.28), a new item is added to the objective function to represent the cost of the committed reserve to the pool from bilateral contracts. The reserve constraints are also introduced correspondingly. The power flow constraints (70.31) and (70.32) are modified to include the effect of reserve agreements on power flow. The objective function becomes:

$$\begin{aligned} Min\ f^j = &\sum_{i\in N_g}\sum_{g\in NG_i^{pj}} C_{ig}^{pj}(P_{ig}^{j}, Q_{ig}^{j}) + \sum_{i\in N_L}\sum_{s\in NL_i^{pj}} CC_{is}^{pj}(CP_{is}^{pj}, CQ_{is}^{pj}) \\ &+ \sum_{i\in BC_i}\sum_{\substack{k\in BC_i \\ k<i}}\sum_{s\in NL_i^{bj}} CC_{iks}^{bj}(CP_{iks}^{bj}, CQ_{iks}^{bj}) + \sum_{i\in N_g}\sum_{g\in RG_i^{rj}} C_{ig}^{rj}(P_{ig}^{rj}, Q_{ig}^{rj}) \end{aligned} \tag{70.42}$$

subject to constraints (70.33)–(70.39) and modified power flow constraints

$$\begin{aligned} &\sum_{g\in NG_i^{pj}} P_{ig}^{j} + \sum_{g\in RG_i^{j}} P_{ig}^{rj} - \sum_{k\in BC_i}(-1)^{\beta}(P_{ik}^{bj} - \sum_{s\in NL_i^{bj}} CP_{iks}^{bj}) \\ &- \sum_{s\in NL_i^{pj}}(P_{is}^{pj} - CP_{is}^{pj}) = \sum_{k=1}^{N}\left|V_i^j\right|\left|V_k^j\right|\left|Y_{ik}^j\right|\cos(\theta_i^j - \theta_k^j - \delta_{ik}^j) \end{aligned} \tag{70.43}$$

$$\begin{aligned} &\sum_{g\in NG_i^{pj}} Q_{ig}^{j} + \sum_{g\in RG_i^{j}} Q_{ig}^{rj} - \sum_{k\in BC_i}(-1)^{\beta}(Q_{ik}^{bj} - \sum_{s\in NL_i^{bj}} CQ_{iks}^{bj}) \\ &- \sum_{s\in NL_i^{pj}}(Q_{is}^{pj} - CQ_{is}^{pj}) = \sum_{k=1}^{N}\left|V_i^j\right|\left|V_k^j\right|\left|Y_{ik}^j\right|\sin(\theta_i^j - \theta_k^j - \delta_{ik}^j) \end{aligned} \tag{70.44}$$

Reserve constraints:

$$0 \le P_{ig}^{rj} \le P_{ig}^{rj,\max} , \tag{70.45}$$

$$0 \le Q_{ig}^{rj} \le Q_{ig}^{rj,\max} . \tag{70.46}$$

The pool demands change from P_{is}^{p0} and Q_{is}^{p0} to P_{is}^{pj} and Q_{is}^{pj} as some bilateral customers may buy the electricity from the pool due to inadequate generation from their EMBGPWR. The P_{is}^{pj} and Q_{is}^{pj} are determined by the states of the EMBGPWR and associated reserve agreements with the power pool.

The solution of the above optimization problem yields the pool generation outputs (P_{ig}^{j}, Q_{ig}^{j}), the pool load curtailments for customer sectors ($CP_{is}^{pj}, CQ_{is}^{pj}$), the sector curtailments of bilateral contracts ($CP_{iks}^{bj}, CQ_{iks}^{bj}$), and the reserve ($P_{ig}^{rj}, Q_{ig}^{rj}$) used.

70.3.4 System Studies

The proposed techniques, the improved OPF technique for the Poolco model (Tech1), for the hybrid model without reserve agreement (Tech2), and for the hybrid model with reserve agreement (Tech3), have been used to analyze the IEEE-RTS. The results obtained using these techniques have been compared with those obtained using the reported technique, the OPF based spot pricing technique [11], [20], [21] for the Poolco model (ETech). The generating system of the RTS is divided into five gencos. The RTS is analyzed as different market models: the Poolco model in which all gencos and customers sell and buy energy from the power pool. In the hybrid model without reserve agreements (Hymodel1), the power pool (EMPGP) consists of gencos 1, 2 and 5. Genco3 and Genco4 are represented as EMBGP1 and EMBGP2, respectively. The bilateral

customers at buses 3, 9 and 19 directly purchase electricity from Genco3 (EMBGP1) at 72 $/MWh and the customers at buses 10 and 13 from Genco4 (EMBGP2) at 75 $/MWh. Other customers buy electricity from the EMPGP at nodal prices. In the hybrid model with reserve agreements (Hymodel2), EMBGP1 and EMBGP2 share their reserve with EMPGP.

Table 70.1 lists the prices ($/MWh) and price deviations ($/MWh) of different models and techniques for the representative nodes. The table shows that the nodal prices obtained using Tech1 are higher than those obtained using ETech. The nodal prices obtained using Tech3 are higher than those obtained using ETech6. This means that system reliability has to be considered in pricing techniques. The higher expected prices and the standard deviations are due to the price spikes and the associated high probability caused by inadequate generation and line congestions.

Table 70.1. Prices and associated risk indices

BLP	ETech	Tech1		Tech3		Tech2	
	ρ_i	$\overline{\rho}_i$	σ_i	$\overline{\rho}_i$	σ_i	$\overline{\rho}_i$	σ_i
1	28.41	78.24	253.5	80.6	250.5	276.8	607.0
2	28.41	78.24	253.4	80.6	250.6	276.7	606.7
3	28.75	80.30	261.2	91.9	157.4	85.0	32.6
4	29.20	80.62	261.3	83.0	258.0	285.0	625.0
5	29.09	80.30	260.5	82.8	257.5	284.8	624.8

70.4 A Schema for Controlling Price Volatilities Based on Price Decomposition Techniques

Because of the low elasticity of system demand, inadequate generation, and line congestion due to system failures may result in price spikes. The electricity prices in a restructured power system can be highly volatile during contingency states. As discussed before, the high prices in a restructured power system have resulted in significant impact on customers. In the new environment, the system operator usually cannot directly control the electricity prices by setting regulated values. Therefore, how to the control price risk caused by system random failures can be a major problem faced by the system operator.

In this section, a schema for controlling electricity price volatility based on the price decomposition technique [22] is proposed. In this schema, generation companies (gencos) or transmission companies (transcos) will be penalized if the failures of their components result in unexpected price change. The penalty is calculated based on the difference of electricity price components between the normal state and contingency states. The motivation of the proposed penalty schema is to: 1) penalize those resulting in price volatility and hurting system reliability; 2) encourage gencos and transcos to improve their reliabilities through maintenance action, replacement of old equipments, and reserve agreements among market participants; 3) compensate the increase of customer cost caused by price volatility and load interruption; 4) provide the system operator a flexible tool to control price and reliability risk.

70.4.1 Price Decomposition Techniques

OPF is used to evaluate nodal prices. The general form of the OPF formulations for system state *j* can be formulated as [22]:

$$Min\, f^j(\mathrm{X}^j) \text{ for } \mathrm{X}^j \,. \tag{70.47}$$

Subject to:

$$\mathrm{G}^j(\mathrm{X}^j,\eta^j) = 0\,, \tag{70.48}$$

$$\mathrm{H}^j(\mathrm{X}^j,\eta^j) \le 0\,, \tag{70.49}$$

where $\boldsymbol{X^j} = (x_1^j,...x_n^j)$ represents a vector of control variables in the system operation such as real and reactive power generations, and load sheddings. $\eta^j = (\eta_1^j,...,\eta_m^j)$ represents a parameter vector in the system operation. $f(\mathrm{X})$ is the system operation cost. $\mathrm{G}^j(\mathrm{X}^j,\eta^j)$ is the vector of equality constraints such as power flow equations, and $\mathrm{H}^j(\mathrm{X}^j,\eta^j)$ is the vector of inequality constraints such as voltage limits, generation output limit, *etc*.

According to the Karush–Kuhn–Tucker (KKT) condition, the optimal solution to the OPF problem (70.47)–(70.49) must satisfy:

$$\frac{\partial f^j}{\partial \mathrm{X}^j}+\lambda^j\frac{\partial \mathrm{G}^j}{\partial \mathrm{X}^j}+\bar{\rho}^j\frac{\partial \bar{\mathrm{H}}^j}{\partial \mathrm{X}^j}=0\,, \tag{70.50}$$

$$\boldsymbol{G^j}(\boldsymbol{X^j},\boldsymbol{\eta^j})=0\,, \tag{70.51}$$

$$\bar{\mathrm{H}}^j(\mathrm{X}^j,\eta^j)=0\ , \tag{70.52}$$

where $\bar{\mathrm{H}}^j$ and $\bar{\rho}^j$ are column vectors that have active inequalities among H^j and the associated Lagrangian multipliers, respectively, and λ^j is the vector of the Lagrangian multipliers associated with equality constraints.

The Lagrangian function of (70.47)–(70.49) is defined as:

$$L^j(\mathrm{X}^j,\eta^j,\lambda^j,\rho^j)=f^j(\mathrm{X}^j)+\lambda^j G^j(\mathrm{X}^j,\eta^j)+\bar{\rho}^j\bar{H}^j(\mathrm{X}^j,\eta^j). \tag{70.53}$$

At an optimal solution, the nodal prices of real power are given as follows:

$$\pi_{pi}^j=\frac{\partial L^j}{\partial P_i^j}\,. \tag{70.54}$$

To break down the nodal prices into a more detail expression, the components we are interested in among $(\mathrm{G}^j,\bar{\mathrm{H}}^j)$ have to be provided. Let M^j be the non-tradable constraints among $(\mathrm{G}^j,\bar{\mathrm{H}}^j)$, which we are not interested in, and N^j be the tradable constraints among $(\mathrm{G}^j,\bar{\mathrm{H}}^j)$, which we are interested in. Equations (70.50)–(70.52) can be rewritten as:

$$\frac{\partial f^j}{\partial \mathrm{X}^j}+\mathrm{U}^j(\mathrm{X}^j,\eta^j,\alpha^j)=0\,, \tag{70.55}$$

$$\boldsymbol{M^j}(\boldsymbol{X^j},\boldsymbol{\eta^j})=0\,, \tag{70.56}$$

where

$$\mathrm{U}^j(\mathrm{X}^j,\eta^j,\alpha^j)=\lambda^j\frac{\partial \mathrm{G}^j}{\partial \mathrm{X}^j}+\bar{\rho}^j\frac{\partial \bar{\mathrm{H}}^j}{\partial \mathrm{X}^j}=\alpha^j\frac{\partial \mathrm{M}^j}{\partial \mathrm{X}^j}+\beta^j\frac{\partial \mathrm{N}^j}{\partial \mathrm{X}^j} \tag{70.57}$$

$\boldsymbol{\alpha^j}$ is the row vector of the Lagrangian multipliers corresponding to the constraints $\boldsymbol{M^j}$ and $\boldsymbol{\beta^j}$ is the row vector of the Lagrangian multipliers corresponding to the constraints $\boldsymbol{N^j}$.

Differentiating (70.55) and (70.56) with respect to P_i^j, the equations can be rewritten as follows:

$$\begin{bmatrix}\dfrac{\partial (f^j)^2}{\partial^2(\mathrm{X}^j)}+\dfrac{\partial \mathrm{U}^j}{\partial \mathrm{X}^j} & \dfrac{\partial \mathrm{U}^j}{\partial \alpha^j}\\ \dfrac{\partial \mathrm{M}^j}{\partial \mathrm{X}^j} & 0\end{bmatrix}\cdot\begin{bmatrix}\dfrac{\partial \mathrm{X}^j}{\partial P_i^j}\\ \dfrac{\partial \alpha^j}{\partial P_i^j}\end{bmatrix}=\begin{bmatrix}-\dfrac{\partial \mathrm{U}^j}{\partial \eta^j}\cdot\dfrac{\partial \eta^j}{\partial P_i^j}\\ -\dfrac{\partial \mathrm{M}^j}{\partial \eta^j}\cdot\dfrac{\partial \eta^j}{\partial P_i^j}\end{bmatrix}. \tag{70.58}$$

Therefore $\dfrac{\partial \boldsymbol{X^j}}{\partial P_i^j}$ and $\dfrac{\partial \boldsymbol{\alpha^j}}{\partial P_i^j}$ can be obtained.

The nodal prices of real power can be decomposed as:

$$\begin{aligned}\pi_{pi}^j&=\frac{\partial f^j}{\partial \boldsymbol{X^j}}\frac{\partial \boldsymbol{X^j}}{\partial P_i^j}+\boldsymbol{\beta^j}\left(\frac{\partial \boldsymbol{N^j}}{\partial \boldsymbol{X^j}}\frac{\partial \boldsymbol{X^j}}{\partial P_i^j}+\frac{\partial \boldsymbol{N^j}}{\partial \boldsymbol{\eta^j}}\frac{\partial \boldsymbol{\eta^j}}{\partial P_i^j}\right)\\&=\sum_{k=1}^{n1}\left(\frac{\partial f_k^j}{\partial \boldsymbol{X^j}}\frac{\partial \boldsymbol{X^j}}{\partial P_i^j}\right)+\sum_{k=1}^{m}\boldsymbol{\beta^j}\left(\frac{\partial N_k^j}{\partial \boldsymbol{X^j}}\frac{\partial \boldsymbol{X^j}}{\partial P_i^j}+\frac{\partial N_k^j}{\partial \boldsymbol{\eta^j}}\frac{\partial \boldsymbol{\eta^j}}{\partial P_i^j}\right)\end{aligned} \tag{70.59}$$

where $\dfrac{\partial f^j}{\partial \mathrm{X}^j}\dfrac{\partial \mathrm{X}^j}{\partial P_i^j}$ is the nodal price component representing the cost from generator units and $\beta^j\left(\dfrac{\partial \mathrm{N}^j}{\partial \mathrm{X}^j}\dfrac{\partial \mathrm{X}^j}{\partial P_i^j}+\dfrac{\partial \mathrm{N}^j}{\partial \eta^j}\dfrac{\partial \eta^j}{\partial P_i^j}\right)$ is the nodal price component representing the cost from constraints for the state *j*.

70.4.2 The Proposed Schema

The random nature of failures creates great price uncertainty. The nodal price components for contingency states can be significantly different from the components in the normal state. Consider a simple example as shown in Figure 70.5.

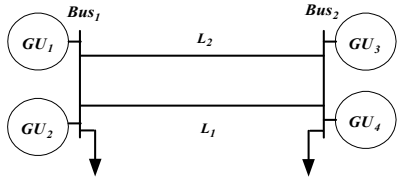


Figure 70.5. The two-bus test system

In this example, the system consists of four units belonging to two generation companies (gencos). Genco 1 owns unit 1 (250MW) at bus 1 and unit 4 (50MW) at bus 2. Genco 2 owns unit 2 (200MW) at bus 2 and unit 3 (76MW) at bus 2. There are two states considered in this example: the normal state and state 4 (unit 4 out of service).

By using the nodal price decomposition technique the nodal price can be expressed in the following form:

Nodal price at bus i = charge for power generation of GU1
+ compensation for power generation upper limit of GU1
+ charge for power generation of GU2
+ compensation for power generation upper limit of GU2
+ charge for power generation of GU3
+ compensation for power generation upper limit of GU3
+ charge for power generation of GU4
+ compensation for power generation upper limit of GU4
+ compensation for voltage lower or upper limit at bus 1
+ compensation for voltage lower or upper limit at bus 2
+ congestion charge for line 1
+ congestion charge for line 2

In the first case, it is assumed that the system is in the normal state. The nodal prices at bus 1 and at bus 2 include four non-zero terms corresponding to the charge for power generation of units and can be decomposed as:

$$\pi_{p1}^{0} = 20.313 + 0 + 12.926 + 0 + 0.11415 + 0 + 0.065229 + 0 + 0 + 0 + 0 + 0 = 33.4\$/MWh$$

$$\pi_{p2}^{0} = 0.32461 + 0 + 0.20657 + 0 + 21.029 + 0 + 12.016 + 0 + 0 + 0 + 0 + 0 = 33.6\$/MWh$$

In the normal state the profits of Genco 1 and Genco 2 are 1779.7$/h and 1154.2$/h, respectively. The customer payment for power at bus 1 and bus 2 is 1336.7$/h and 8729.8$/h, respectively.

In the second case, it is assumed that unit 4 is out of service. The nodal prices at bus 1 and at bus 2 include three non-zero terms, which can be decomposed as:

$$\pi_{p1}^{4} = 21.207 + 0 + 13.497 + 0 + 0.17797 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 34.9\$/MWh$$

$$\pi_{p2}^{4} = 0.50586 + 0 + 0.32194 + 0 + 34.234 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 35.1\$/MWh$$

In this state, the profits of Genco 1 and Genco 2 are 1860.3 $/h and 1348.9$/h, respectively. The customer payment for power at bus 1 and bus 2 is 1395.3$/h and 9116.1$/h, respectively.

Comparing the results in case 1 with the results in case 2, it can be seen that the failure of the system component results in the uncertainty of the nodal price, and the variations of nodal price components, the customer payment, and the genco's profit. The outage of a generation unit usually causes a relatively large profit increase of other generating units. In case 2 though unit 4 failed, the profit of the responsible Genco 1 still increases from 1779.7$/h in the normal state to 1860.3 $/h because of the increased nodal price at bus 1 and the output of unit 1. Obviously, the corresponding genco can use this strategy to earn more profit.

The proposed schema is to evaluate a penalty cost to the corresponding genco or transco if the failures of its components result in electricity price volatility. Two major factors are considered in the schema to evaluate the penalty cost. The first factor is the differences in the nodal price components between the normal state and the corresponding contingency state. The second factor is the responsibility of the corresponding genco or transco for the variation of nodal price components. For the variations of different components in the nodal prices, the responsibilities of genco or transco are different. Some market rules will be set up by the system operator to determine the responsibilities of a genco or a transco for the variation of nodal price components.

If contingency state j is caused by the failure in Genco or Transco z, the penalty can be defined as:

$$\text{Penalty}_{z}^{j} = \sum_{i \in N_L} \left\{ \gamma_0 \cdot (v_{i,0}^{j} - v_{i,0}^{j_0}) + \gamma_1 \cdot (v_{i,1}^{j} - v_{i,1}^{j_0}) \right\} \cdot D_i^j + \gamma_2 \cdot \left\{ \sum_{i \in N_L} \sum_{s \in NI_i^j} OC_{is}^{j} (LC_{pis}^{j}) \right\} \tag{70.60}$$

where $v_{i,0}^{j}$ and $v_{i,0}^{j_0}$ are price components at bus i related to z for the contingency state j and the normal state, respectively,

$$\nu_{i,0}^{j}=\sum_{\substack{k=1\\k\notin GS}}^{z1}\left(\frac{\partial f_k^j}{\partial \boldsymbol{X}^{\boldsymbol{j}}}\frac{\partial \boldsymbol{X}^{\boldsymbol{j}}}{\partial P_i^j}\right)+\sum_{\substack{k=1\\k\notin CS}}^{z2}\beta^j\left(\frac{\partial N_k^j}{\partial \boldsymbol{X}^{\boldsymbol{j}}}\frac{\partial \boldsymbol{X}^{\boldsymbol{j}}}{\partial P_i^j}+\frac{\partial N_k^j}{\partial \boldsymbol{\eta}^{\boldsymbol{j}}}\frac{\partial \boldsymbol{\eta}^{\boldsymbol{j}}}{\partial P_i^j}\right) \quad (70.61)$$

$$\nu_{i,0}^{j_0}=\sum_{\substack{k=1\\k\notin GS}}^{z1}\left(\frac{\partial f_k^{j_0}}{\partial X^{j_0}}\frac{\partial X^{j_0}}{\partial P_i^{j_0}}\right)+\sum_{\substack{k=1\\k\notin CS}}^{z2}\beta^{j_0}\left(\frac{\partial N_k^{j_0}}{\partial X^{j_0}}\frac{\partial X^{j_0}}{\partial P_i^{j_0}}+\frac{\partial N_k^{j_0}}{\partial \eta^{j_0}}\frac{\partial \eta^{j_0}}{\partial P_i^{j_0}}\right) \quad (70.62)$$

It can be seen from (70.61) and (70.62) that $\nu_{i,0}^{j}$ and $\nu_{i,0}^{j_0}$ have two items. The first item represents price components for power generation of units of Genco *z*. The second item represents price components for the tradable constraints related to Genco *z* or Transco *z, e.g.,* power generation limit of units of Genco *z* or congestion charge of Transco *z*.

$\nu_{i,1}^{j}$ and $\nu_{i,1}^{j_0}$ are price components not related to *z* for contingency state *j* and the normal state, respectively,

$$\nu_{i,1}^{j}=\sum_{k=z1+1}^{n1}\left(\frac{\partial f_k^j}{\partial \boldsymbol{X}^{\boldsymbol{j}}}\frac{\partial \boldsymbol{X}^{\boldsymbol{j}}}{\partial P_i^j}\right)+\sum_{k=z2+1}^{m}\beta^j\left(\frac{\partial N_k^j}{\partial \boldsymbol{X}^{\boldsymbol{j}}}\frac{\partial \boldsymbol{X}^{\boldsymbol{j}}}{\partial P_i^j}+\frac{\partial N_k^j}{\partial \boldsymbol{\eta}^{\boldsymbol{j}}}\frac{\partial \boldsymbol{\eta}^{\boldsymbol{j}}}{\partial P_i^j}\right) \quad (70.63)$$

$$\nu_{i,1}^{j_0}=\sum_{k=z1+1}^{n1}\left(\frac{\partial f_k^{j_0}}{\partial \boldsymbol{X}^{\boldsymbol{j_0}}}\frac{\partial \boldsymbol{X}^{\boldsymbol{j_0}}}{\partial P_i^{j_0}}\right)+\sum_{k=z2+1}^{m}\beta^{j_0}\left(\frac{\partial N_k^{j_0}}{\partial \boldsymbol{X}^{\boldsymbol{j_0}}}\frac{\partial \boldsymbol{X}^{\boldsymbol{j_0}}}{\partial P_i^{j_0}}+\frac{\partial N_k^{j_0}}{\partial \boldsymbol{\eta}^{\boldsymbol{j_0}}}\frac{\partial \boldsymbol{\eta}^{\boldsymbol{j_0}}}{\partial P_i^{j_0}}\right) \quad (70.64)$$

The first item in (70.63) and (70.64) represents price components for units' power generation of other gencos and load shedding of customers. The second item in (70.63) and (70.64) represents price components for all other tradable constraints not related to Genco *z* or Transco *z, e.g.*, voltage limits and power generation limit of units of other Gencos.

γ_0 is the proportion that the Genco or Transco *z* is responsible for the increase of price components related to *z*. Usually $0\le\gamma_0\le 1$.

γ_1 is the proportion that the Genco or Transco z is responsible for the increase of price components not related to z. Usually $0\le\gamma_0\le 1$ and $\gamma_1\le\gamma_0$.

γ_2 is the proportion that the Genco or Transco z is responsible for the interruption cost of customers if there is load shedding for state j. Usually $0\le\gamma_2\le 1$.

The demand at bus *i* for state *j* can be calculated as:

$$D_i^j=\sum_{s\in NL_i^j}P_{is}^{j_0}-\sum_{s\in NL_i^j}LC_{pis}^j\ . \quad (70.65)$$

The second case is reconsidered now. For the normal state the first item of $\nu_{1,0}^{j_0}$ related to Genco 1 can be represented as $20.313+0$, where 20.313 is the price component for power generation of unit 1 at bus 1, and 0 is the price component for power generation of unit 4 at bus 1. The compensation of power generation upper limit of unit 1 is zero. In the contingency state 4 (unit 4 out of service) the first item of $\nu_{1,0}^{4}$ related to Genco 1 can be represented as $21.207+0$, where 21.207 is the price component for power generation of unit 1 at bus 1, and the price component related to the unit 4 is also zero because this unit is out of service. The compensation of power generation upper limit of unit 1 is also zero.

In the normal state the first item of $\nu_{1,1}^{j_0}$ related to unit 2 and unit 3 can be represented as $12.926+0.11415+0+0$, where 12.926 and 0.11415 are price components for power generation of units 2 and 3 at bus 1, respectively . The compensation of power generation upper limit of units 2 and 3 is zero. In the contingency state 4 the first item of $\nu_{1,1}^{4}$ related to units 2 and 3 can be represented as $13.497+0.17797+0+0$, where 13.497 and 0.17797 are price components for power generation of units 2 and 3 at bus 1, respectively. The compensation of power generation upper limit of unit 2 and unit 3 is also zero.

It is supposed that γ_0 and γ_1 are set by the system operator as 0.3 and 0.2, respectively. The penalty of Genco 1 for state 4 can be calculated as:

$$\begin{aligned}\text{Penalty}_1^4 &= \left\{\begin{matrix}0.3\times(21.207-20.313)+\\0.2\times(13.497+0.17797-12.926-0.11415)\end{matrix}\right\}\times 40\\ &+\left\{\begin{matrix}0.3\times(0.50586-0.32461)+\\0.2\times(0.32194+34.234-0.20657-21.029)\end{matrix}\right\}\times 260\\ &=722.6\$/h\end{aligned}$$

In this case the profit of Genco 1 goes from 1860.3$/h to 1860.3−722.6=1137.7$/h, which is much less than the profit in the normal state.

The system operator of the power pool will set γ_0, γ_1 and γ_2 to reflect the responsibilities of the genco or transco and to influence the price volatility. The penalty will stimulate gencos and transcos to improve their reliabilities and therefore reduce price volatilities.

Acknowledgment

This work was partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

[1] Hunt S, Shuttleworth G. Competition and choice in electricity, Wiley, New York, 1996.
[2] Song K. Aspects of strategic bidding in deregulated electricity markets. Ph.D Thesis, Nanyang Tech. University, 2001.
[3] Philipson L, Willis HL. Understanding electric utilities and de-regulation. Marcel Dekker, New York, 1999.
[4] Rudnick H. Pioneering electricity reform in South America. IEEE Spectrum, 1996; 33 (8): 38–44.
[5] Rudnick H. The electricity market restructuring in South America: Successes and failures on market design. Presented at the Plenary Session of Harvard Electricity Policy Group, California 1998 Jan.
[6] Bhattacharya K, Bollen M, Daalder JE. Operation of restructured power systems. Kluwer, Boston, 2001.
[7] Weber JD, Individual welfare maximization in electricity markets including consumer and full transmission system modeling. Ph.D Thesis, UIUC, 1999.
[8] Northup ME, Rasmussen JA. Electricity reform abroad and U.S. investment, Report from the United States Department of Energy – Energy Information Agency, 1997, http://www.eia. Doe.gov/emeu/pgem/electric.
[9] Tabors RD. Lessons from the UK and Norway. IEEE Spectrum, 1996; Aug.: 45–49.
[10] Vickery W. Responsive pricing and public utility services. Bell Journal of Electronics and Management Science 1971; 2: 337–346.
[11] Schweppe FC, Micheal TR, Bohn RE. Spot pricing of electricity. Kluwer, Boston, 1988.
[12] Ding F, Fuller JD, Nodal, uniform, or zonal pricing: distribution of economic surplus. IEEE Transactions on Power Systems 2005; May, 20(2): 875–882.
[13] The Pennsylvania-New Jersey-Maryland inter-connections http://www.pjm.com/
[14] ISO. New York, http://www.nyiso.com
[15] IEEE Task Force, IEEE Reliability Test System, IEEE Transactions on Power Apparatus and Systems, PAS-98: 2047–2054, 1979.
[16] Wacker G, Billinton R. Customer cost of electric service interruptions. Proceedings of the IEEE 1989; 77(6): 919–930.
[17] Billinton R, Allan RN. Reliability evaluation of power systems. Plenum Press, New York, 1996.
[18] Lehmköster C. Security constrained optimal power flow for an economical operation of FACTS-devices in liberalized energy markets. IEEE Transactions on Power Systems, 2002; April, 17(2): 603–608.
[19] Bertsekas DP. Nonlinear programming. Athena Scientific. Belmont, USA, 1999.
[20] Alvarado F, Hu Y, Ray D, Stevenson R, and Cashman E. Engineering foundations for determination of security costs. IEEE Transactions on Power Systems 1991; August, 6(3).
[21] Baughman ML, Siddiqi SN, Zarnikau JW. Advanced pricing in electrical systems Part I: Theory. IEEE Transactions on Power Systems 1997; 12 (1):489–501.
[22] Chen L, Suzuki H, Wachi T, Shimura Y. Components of nodal prices for electric power systems. IEEE Transactions on Power Systems 2002; 17 (1): 41–49.
[23] Shahidehpour M, Alomoush M. Restructured electrical power systems operation, trading and volatility. Marcel Dekker, New York, 2001.
[24] Wang P, Ding Y, Xiao Y. Technique to evaluate nodal reliability indices and nodal prices of restructured power systems. IEE Proceedings Generation, Transmission, And Distribution, 2005; May, 152(3): 390–396.
[25] Ding Y, Wang P. Reliability and price risk assessment of a restructured power system with hybrid market structure. IEEE Transactions on Power Systems. 2006; Feb., 21(1): 108–116.
[26] Ding Y. Nodal reliability and nodal price in deregulated power markets. Ph.D Thesis, Nanyang Technological University, 2006.

71

Probabilistic Risk Assessment for Nuclear Power Plants

Peter Kafka

Consultant, RelConsult, Grünwald, Germany

Abstract: Probabilistic risk assessment (PRA) is a systematic and comprehensive methodology to evaluate risks associated with a complex technological entity. PRAs for nuclear power plants have a more than 30 year old success story. The present chapter outlines in depth the PRA history, the essential elements of a PRA, today's challenges, an outlook, and last but not least, some rational comments to trigger supplementary developments and further improvements in the PRA methodology and the related risk management process.

71.1 Introduction

Electric power generation using nuclear energy and associated risk assessment is one of the major engineering areas that has been practised successfully for more than 60 years.

The electricity for the first time by a nuclear reactor was generated on December 20, 1951 at the EBR-I experimental station near Arco, Idaho, in the United States. On June 27, 1954, the world's first nuclear power plant to generate electricity for an electrical power grid started operations at Obninsk in the former USSR. The world's first commercial scale nuclear power station, Calder Hall in England, opened on October 17, 1956.

Today, there are 444 nuclear power plants (NPP) in operation world-wide (status on December 31, 2005). The installed capacity is 390.931 MWe (gross). These facilities generated 2.750 Mrd. kWh in the year 2005 (net). This amount of electricity represents about 15% of the electricity demand worldwide. Related to this huge industrial undertaking, the safety record, also considering the observed nuclear disasters, is remarkably good and it is a great engineering challenge to keep it at this excellent level.

In depth safety evaluations have been growing since 1956. At that time in USA the first commercial NPPs were switched to the grid. Thus, the licensing authority in the states (at that time: USAEC; US Atomic Energy Commission) asked the Brookhaven National Laboratory to estimate the consequences of a severe nuclear accident. The results of this estimation were published in 1957 by the USAEC in the report "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants" and coded with WASH 740 [1]. This so-called Brookhaven Report was not very helpful, because it concluded that if the containment functioned no damage to the surrounding population would occur, and if the containment failed only the upper bound of consequences could be estimated from the relief of the large quantities of fission products in the form of noble gases, radioiodine, and some fractions of

other fission products. The public impact would be enormous by such a scenario.

Realizing this overestimation the US Congress established the well known Price Anderson Act to provide the protection of public needed by the industry and in doing so it ignored the upper limit estimates of WASH 740.

A few years later it was suggested by engineers in many countries to estimate not only the consequences of severe accidents (the worst case) but also the inherent probabilities of severe scenarios and finally the consequences to a plant, the public, or the environment. As a successful promoter of this "risk-informed" approach using realistic assumptions for potential event scenarios Farmer [2] has to be honored.

This milestone for industrial safety engineering as a whole marks the beginning of probabilistic risk assessment (PRA).

In the course of these developments in the United States the Nuclear Regulatory Commission (US NRC) entrusted Norman Rasmussen from MIT to assess the risk associated with the operation of ten light water reactors in the U.S. The results of this challenging undertaking were published in 1975 in form of the "Rasmussen Report" and coded as WASH 1400 [3].

Typically for this first comprehensive and plant-wide risk study was the integrative application of event tree and fault tree methodology. Both methods were known but applied separately in system reliability studies in various technologies.

The report concluded that the risks to the individual posed by such NPPs were acceptably small, compared with other tolerated risks. Specifically, the report concluded that the probability of a complete core meltdown is about 1 in 20,000 *per* reactor *per* year.

The Rasmussen Report was peer-reviewed by the "Lewis Committee" in 1977, which broadly endorsed the methodology as the best available, but warned that the risk figures were subject to large uncertainties.

WASH 1400 steered the nuclear community, the NPP operators, and the licensing authorities around the globe to perform risk assessment for all the individual NPPs based on the PRA approach.

These worldwide plant specific PRA activities also triggered much R&D work for improving weaknesses in methodologies, to broaden the probabilistic/statistical data base, to complete the understanding of accident phenomena, and finally to reduce uncertainties in risk estimates.

Following that period of intensive and expensive R&D work in many countries, and inspired partly by the Three Mile Island Accident in 1991 WASH-1400 was replaced by NUREG-1150 [4]. In parallel in all the countries operating NPPs, PRAs for specific plants, or at least for families of similar plants, were initiated and finalized. At this time the term probabilistic risk assessment was modified into the synonym probabilistic safety assessment (PSA).

In 1995, the USNRC issued the PRA Policy Statement, which says: "The use of PRA in all regulatory requirements should be increased to the extent supported by the state-of-the-art PRA methods and data in a manner that compliments the defense-in-depth philosophy. PRA should be used to reduce unnecessary conservatism associated with current regulatory requirements." [5].

Today, there is consensus among NPP designers, operators, and licensing authorities that PRA/PSA:

- achieves a realistic description and quantification of risk;
- models performance of various safety measures;
- makes known and therefore allows weak points in system design, construction, and operation to be revealed;
- reflects the consequences of dependencies in systems, components, and man–machine in general;
- makes uncertainties explicitly visible;
- identifies the relative importance of specific accident sequences, safety features, and component failures;
- allows the assessment of operational and maintenance related aspects;
- considers and applies explicitly operational experience as a indispensable knowledge base; and
- allows monitoring the actual risk level throughout the life cycle of an NPP.

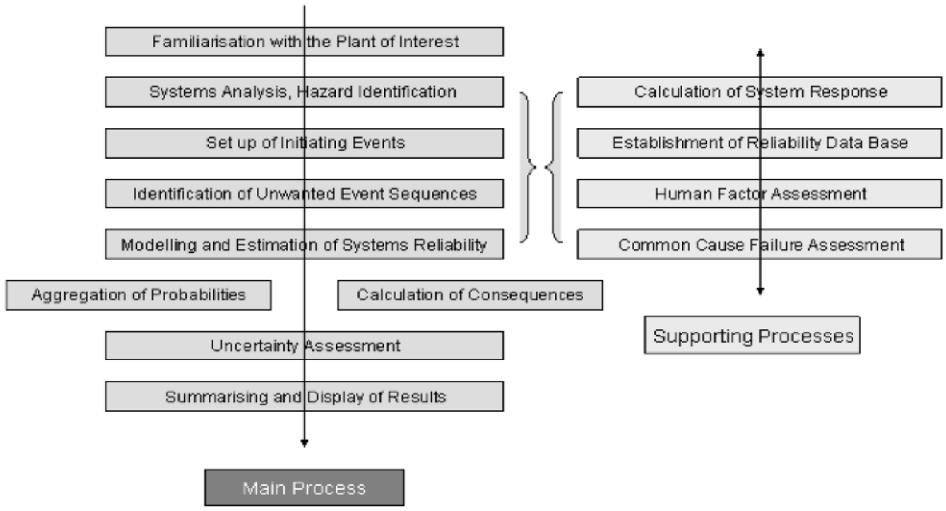


Figure 71.1. The main tasks required for a typical PRA

Remarkable for this condensed historical perspective are also the keen activities to harmonize the PRA procedure for easy review and comparisons of outcomes. Specifically, the IAEA in Vienna promoted activities and published a series of guidelines in form of: "How you should conduct a PSA…" [6].

Beyond these non-binding IAEA guidelines some countries endorsed "requirements" for doing the PRA and their utilization. As an example the "PSA Leitfaden" is referenced for Germany [7]. Additional information regarding the utilization of PRAs in licensing procedures is given in [8].

The standardization organization ASME (American Society for Mechanical Engineers) endorsed the "PRA Standard" in 2002 [9] aiming also at the use of "best practice" for PRA achievement.

Nowadays, other technologies in many countries, *e.g.*, the space industry, the oil and gas industry, dangerous goods transport, and process facilities are looking carefully at the PRA approach developed and used in nuclear industry, and are working at adopting the essence of that approach for their own safety questionnaire [10]. The NASA PRA Guideline, published in 2002 [25], is an example and a reference for that performed synergism.

In Figure 71.1, the main tasks performed in a PRA process are shown. However, the illustrated process can never be straightforward. Some iterative actions dependent on preliminary results in a given process step are always required [26].

Considering the enormous activities performed for PRA and the huge mass of publications in this field, the author is aware that this condensed historical perspective can only be a limited snapshot of the real world in PRA/PSA undertakings [27].

71.2 Essential Elements of PRA

PRA, often named PSA, is a systematic and comprehensive methodology to evaluate the risks associated with a complex technological entity [26].

Risk in a PRA is defined as a feasible adverse outcome of an event scenario triggered by a malfunction of a technical entity, a human interaction, or an environmental impact.

Risk is characterized by two quantities:

- the magnitude (severity) of the possible adverse consequence, and
- the likelihood (probability) of the occurrence of the adverse consequence.

Adverse consequences can be directed to the:

- entity itself and, therefore, to a financial loss;
- staff or the surrounding population and, therefore, to a health impact;
- environment and, therefore, to an ecological disaster, or
- entity, the humans, and the environment together.

Consequences are expressed by numbers (*e.g.*, in the form of physical parameters or number of potentially impacted people), and their likelihoods of occurrence are expressed as probabilities or frequencies (*i.e.*, the number of occurrences or the probability of occurrence *per* unit of time).

PRA usually answers three basic questions:

- What can go wrong within the entity?
- What are the adverse consequences?
- How likely are these adverse consequences?

For NPPs it is usual to perform PRAs for three different ranges [6], [28], [29]:

Level I: Risk assessment based on event scenarios that can lead to core damage.

Level II: Risk assessment based on event scenarios that can lead to core damage and consequently to a loss of containment.

Level III: Risk Assessment based on event scenarios that can lead to core damage, a loss of containment, and consequently to an impact on the surrounding public and the environment.

In Figure 71.2 a simplified PRA logic is shown. It is by rule a "cause–consequence logic" composed of fault trees and event trees. The trees are intermeshed to a global model. Normally, about 30 event trees and 100 fault trees are combined. The event trees describe a success/failure logic; the fault trees the undesired TOP events. In Figure 71.2 the summing up procedures *via* binning of similar outcomes of event trees, *etc.*, is not visualized.

The entire combination of event and fault trees represents a probabilistic model. This means all the causes (basic events), the logic gates (AND, OR, *etc.*) in the fault trees, the initiating event, the gates in the event trees (success or failure, respectively yes or no), the core damage, the containment failure, and all the various estimated consequences are characterized by quantified probabilities [9].

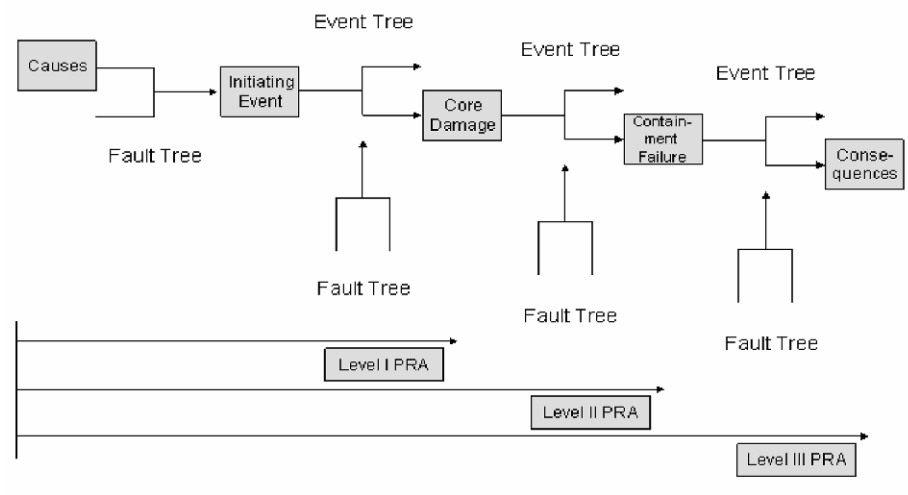


Figure 71.2. Simplified PRA logic (binning procedures are neglected)

71.2.1 Identification of Scenarios

The identification of scenarios that have be undergone for an in-depth analysis is focused on the hazards inherent in the NPP. The main hazards result from radioactive inventories of the reactor core and the fuel element storage pool. Thus, the PRA focusses on the identification of scenarios that can eventually lead to undesired consequences if some hazardous situations develop [26].

The process of identification is normally supported by a "master logic diagram" (MLD), which shows in a tree logic all the various sequences (causes) that can lead to the undesired release of radioactive products and, therefore, to unwanted consequences for the plant, the public, or the environment. This process is often not straightforward because an increase of insight perhaps leads to a re-consideration of possible event sequences.

MLG creates the so-called initiating events (IEs) triggering the unwanted sequence. These IEs are the starting point for identifying (probably the most complete) possible event scenarios, which can be modeled with the means of event tree logic. The undesired events, or end states, of the event trees are classified as plant damage states such as the un-cooled core or the core melt.

The granulation of the event trees is normally oriented on the system level. This means the event trees show what happens if a given system is functioning or if it fails.

In the real work out of PRAs the practitioners identify about 30 event trees manifesting all the identified scenarios that can lead to the unwanted release of radioactive products.

If the PRA is to answer a typical question of plant owners, *e.g.*, how can a particular plant damage be triggered, the identification process has to be focused backwards to identify the various causes for such an unwanted damage.

71.2.2 System Reliability

The assessment of system reliability is essential in the course of a PRA process. It answers main questions *e.g.*, what can go wrong and how frequent is it? Answers to these questions are not only of interest for the main task of risk assessment but also for plant availability estimations, maintenance optimizations, and life-cycle cost calculations [26],[30].

The methodology for reliability assessment is *per se* well developed and established, and has been in use for many years in various technologies, However, the number of systems and components, the complexity of interactions, and the implementation of new technologies, *e.g.*, digital control systems based on embedded software, are NPP specific and, therefore, challenging issues for reliability engineers.

Besides these facts one has to be aware that some component failures are so-called rare events and, therefore, the statistical data base for these components is associated with significant uncertainties. So far, ongoing activities to collect raw data in NPPs and to estimate the belonging reliability figures (*e.g.*, failure rates, CCF data, repair times) is of great importance.

The main approach applied for system reliability assessment is given by the fault tree methodology (FTA). Some PRA practitioners support FTA at the front end by failure mode and effect analysis (FMEA) to identify possible failure modes and their causes and consequences. However, it is surprising that this beneficial and fully formalized approach is not routinely utilized within the process of system reliability assessment for NPPs.

Some system behavior that is significantly time dependent is modeled by using the Markov approach. As is known, this approach allows for various time-dependent system stages (*e.g.*, operation, standby, repair), the explicit estimation of probabilities to be present in one of these stages.

71.2.3 System Response

For system design it is assumed every one of the installed components and system functions are working properly. Under this condition many different physical properties (*e.g.*, temperature, pressure, stress) are calculated. Accompanying sensitivity studies often illuminate often some deviation from the design purpose if a specific parameter is beyond the design value.

The PRA process raises many more questions regarding the physical behavior of the system be-

cause according to Murphy's law every component build in the system can fail and, therefore, the system response can be related to the design status very differently.

In practice it is not possible to repeat, case by case, the system response calculation for all the possible situations or combinations of component failures. Usually, event tree logic showing unwanted failure sequences creates the cases for system response calculations. However, this procedure is not a one way street because also the identification of the unwanted sequences in the event trees should take into account insight from system response calculations or system understanding. Thus, in other words, these two working steps, identification of the event sequences of interest and the calculation of system response, are usually prepared with close cooperation of reliability engineers and system designers.

Some simplifications in the form of pessimistic assumptions are regularly required if the system response is highly dynamic (time dependent) and the modeling of event sequences is quasi-static (snap shot) [26].

71.2.4 Common Cause Failure

The family of dependent failures are multiple failure events that can defeat the mechanical/ structural barriers, the diversity, and/or redundancy applied in the NPP to ensure highly reliable systems under operation or a sufficient availability of standby safety features [26].

Generally, the following major categories of dependent failures are considered within a PRA:

- Functional dependencies. This category includes dependence among systems or components due to sharing of common hardware (*e.g.*, pipe work, cables) or sharing a common process (*e.g.*, depressurization of a primary circuit for successful functioning of core cooling).
- Physical dependencies. This category couples multiple systems or components through a common environment (*e.g.*, steamy atmosphere, flooding, earthquake).
- Human interaction dependencies. This category includes dependencies caused by common procedures/actions applied for man–machine interactions (*e.g.*, misinterpretation of procedural steps).

These categories of dependencies are normally modeled explicitly in PRAs to the extent that is practicable related to the available historical information.

Besides these categories one has to be aware that similar or identical components would have a similar sensitiveness against specific environmental conditions, process parameters, stress conditions, *etc.*, named root causes. Therefore, it is known that similar or identical components can fail together if a common root cause takes place. Obviously, this type of dependent failure, named common cause failure (CCF) cannot explicitly be modeled in, *e.g.*, fault trees; one has to consult operational experience and relevant data bases to judge the probability for common failures.

For practical use in PRAs, a few similar models have been developed and the values for the associated parameters have been proposed and published. One of the simplest models is the so-called β-factor model. It says that the probability of a CCF (*i.e.*, common failure of redundant components) is a given fraction of the probability of a random failure of one of the components. It has been experienced that β-factors can be in the range of 10%.

As a consequence of this worth impact to the reliability of redundant systems great effort is being spent to estimate adequate β-factors, and *vice versa*, to improve engineering practice for reduction of CCF sensitiveness of redundant systems and components.

71.2.5 Human Factors

The PRA approach requires the quantification of system failures in the form of explicit probabilities. As a consequence, each part of the system (*i.e.*, man–machine) has to be considered as a potential source of an inadequate functional behavior. Thus, the human error probability (HEP) is *per se* a vital value of interest [33].

The HEP is defined as the number of erroneously performed tasks of type i divided by the number of all tasks of type i. However, it is indeed difficult to calculate the HEP value beforehand

because both values required for the HEP formula are fuzzy. Nevertheless, the evaluation the operational experience opens the door to estimating the HEP values retrospectively.

In PSA models normally three types of personnel actions are distinguished:

Type A: Personnel action during proper operation of the system that has led to a hidden error (example: wrong position of a standby valve).
Type B: Personnel action that has led to an initiating event (example: opening a valve and therefore creating a small leak in a primary circuit).
Type C: Personnel actions after initiating event in order to cope with it (example: switching on the emergency core cooling system).

Obviously, Type C actions have to be subdivided further because actions in this plant phase can be planned or unplanned and can mitigate or not mitigate the real accident sequence.

The most common quantification procedure for HEPs follows the THERP method published in Allan Swain's handbook. It requires a task analysis based on tree logic and the utilization of the performance shaping factors considering the environmental conditions, the training status of the operator, and the time span available for fulfilling the task. The task tree logic considers not only the success and failure path but also recovery actions to correct a wrong action into a successful one.

A significant number of other models have been published and applied to PRAs. These advanced models are summed up as second generation models (*e.g.*, ATHENA, CREAM, MERMOS, *etc.*) and are characterized as "knowledge-based models", different to the first generation of models (*e.g.*, THERP, HCR, Slim-Mod, *etc.*), characterized as skill and rule-based models.

Human reliability assessment in general has many problems to solve. For instance, the errors of commission have been for many decades been known to be important in the course of severe accidents. However, only in the last few years' has significant progress been made to cope with this type of errors by the development of the knowledge-based models of the second generation. The quantification of soft issues, like managerial aspects within the NPPs, will be a great challenge for the HRA researchers in the next years.

71.2.6 Software Reliability

In this century there has been a great turn from the utilization of hard-wired control systems to digital systems controlled by software running on computers or embedded in specific processors. Unfortunately, this movement toward digital systems has had great impact on the PRA process. It is no longer plausible and is not supported by sound operational experience that the implemented and tested software will not fail and, therefore, the reliability (risk) impact related to other failure possibilities and causes can be neglected [25].

Indeed, all the safety related control systems in NPPs are highly redundant (*e.g.*, two out of four) and, therefore, the failure of a single digital electronic device does not create a loss of function. However, common inadequacies in software specifications can easily jeopardize this precautionary principle.

Software is always in communication with sensor signals, data packages transmitting on bus systems, the computer hardware itself, and the actions required for, *e.g.*, software flashing and software maintenance actions. Thus, the question is, how reliable is the software *under the conditions of these interactions and communications*? However, for reliability engineering it is not only an open question in terms of "go and no go" (success/failure); it is also a question of "what would go wrong" (unwanted).

These shortly illuminated interactions are well under discussion and in practice often controlled, limited, or eliminated by very specific hardware or software features. Nevertheless, the complexity of highly dynamic interaction of accurate and probably erroneous (*i.e.*, failure case) signals or software functions should trigger many more warnings that the given resources for reliability assessment of digital control systems are not sufficient. Moreover, the excuse "software reliability assessment is too complex" can no longer be accepted.

In this context it is important to remember that also on the lower system level for digital control

systems does the PRA process require an answer to the three main questions for PRAs in general:

- What can go wrong within the system?
- What are the adverse consequences?
- How likely are these adverse consequen-ces?

71.2.7 Uncertainties

Engineering knowledge, judgment, mathematical modeling, and mechanistic formulations are ingredients of the PRA process and finally the results. For many years it has been tradition among physicists and engineers to perform an error analysis of both the measurements and the computations. The errors under consideration were mainly due to small fluctuations around nominal values and to, *e.g.*, rounding processes in functional relationships [9],[34].

In the case of PRA it is not only a matter of small fluctuations and of rounding, but there is also a need to simplify the real world due to a lack of knowledge. An extended error analysis or more adequately an uncertainty analysis of PRA results is, therefore, essential.

The result from the uncertainty analysis is a quantitative statement how well the answer to the PRA question can be given. However, this answer can only be given by considering the various epistemic uncertainties involved. This type of uncertainty includes the relevance of phenomena, the adequacy of the numerous models applied within the PRA, the suitability of the hundreds of parameter values used in these models, and the accuracy of the great number of reliability characteristics.

For the purposes of uncertainty analysis the state of knowledge of epistemic uncertainties is expressed by subjective probability distributions. The complex functional relationship in a PRA model makes it impossible to obtain the aggregated subjective probability distribution analytically. It is, however, possible by application of the Monte Carlo simulation technique to generate numerically the epistemic uncertainties associated with the PRA results.

In contrast to the epistemic uncertainties one has to be aware that everything that contributes to the variability within the population of considered NPPs is aleatory uncertainty. The aleatory uncertainty is that addressed when the occurrence of undesired events or phenomena with the plant are modeled in random or stochastic manner. The quantification of aleatory uncertainties is the actual purpose of the PRA itself. The measure for aleatory uncertainty is the probability in its frequentistic interpretation. The measure of the epistemic uncertainty is also probability but in its subjective interpretation as a degree of belief.

It should be stressed that the quantification process of epistemic uncertainties does not only generate the range and distribution of the numerical PRA results but also the information on how significantly a given parameter or parameter cluster contributes. In other words, the sensitivity of the various parameters can be estimated.

Today's challenges in this field are the further development of effective calculation processes, a realistic subjective judgment of parameter uncertainties, the estimation of model uncertainties, and the use of large computer/processor clusters to run simulation trials of complex mechanistic codes.

71.2.8 Probability Aggregation

Probability aggregation throughout the entire probabilistic model (*i.e.*, the coupled event and fault trees) is an ambitious task. At the beginning of PRA work the computerized support was very limited. Thus, often a linking procedure was performed by hand for the various fault trees and the corresponding event trees [9],[34].

Nowadays, the commercial software packages used for PRAs (*e.g.*,: Saphire®, Cafta®, RiskSpectrum®, Relex®, Isograph®) are ready the handle a significant number of event and fault trees and to perform the linking procedure, based on some inputted overhead, automatically. Nevertheless, the huge number of basic events involved (*e.g.*, 5000–8000 for a Level I PRA) requires that the practitioners perform, after calculations, some tricky plausibility test mostly executed by checking the Boolean cut sets responsible for the various TOP events in fault trees or the unwanted end states in event trees.

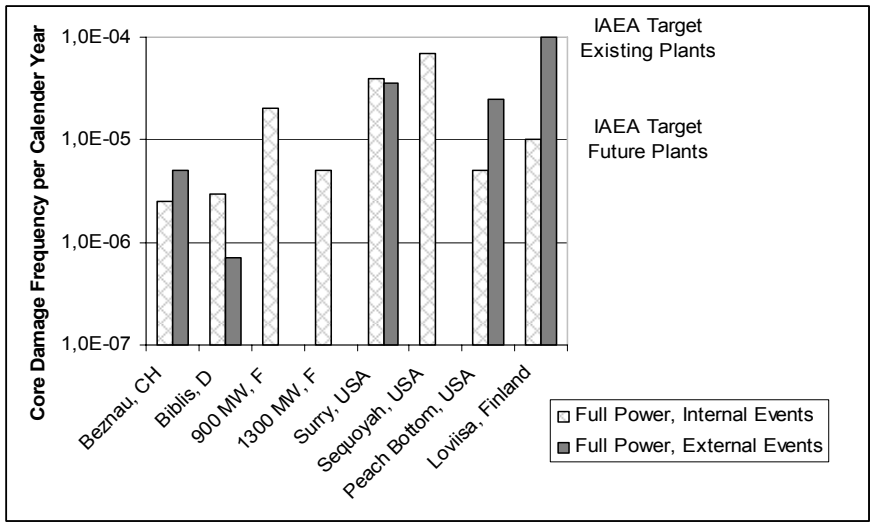


Figure 71.3. PRA Level I results in comparison for international NPPs [28]

In some cases if specific linkings and combinations of TOP events are of interest a combination of reliability software and an office spread sheet software may be a good choice.

The combinatorial explosion of different event sequences and end states in large PRA models forces a so-called binning procedure. This means the end states representing similar plant damage states (*e.g.,* loss of core cooling) are clustered together, and the resulting probability or frequency per plant year is summed up across this cluster.

Obviously, for a Level III PRA this probability aggregation is much more complex because the core melt model, the containment response, the environmental model, and the cause–consequence model for health effects come into the focus. The probability aggregation for these types of PSAs is normally performed by hand but is supported by computerized numerical procedures.

In Figure 71.3, typical results for Level I PRAs are shown. All the probabilities are aggregated to final results in form of frequencies *per* reactor year.

71.3 Today's Challenges

Existing analysis processes and approaches can never be perfect. State of knowledge is growing and PRA visionaries often create sophisticated ideas. Based on this one has to constantly look for useful improvements of the PRA methodology and the assessment process itself. In the following chapters three essential issues are picked up as main challenges for today's PRA practitioners and managers.

71.3.1 The Risk Management Process

As stated, risk is an inherent characteristic of all technical installations and processes. It has a dominant impact upon safe operation *and* economical effectiveness. It is, therefore, important that a satisfactory level of risk is achieved by an adequate risk management process [35– 42].

However, there is a worldwide discussion about the "satisfactory level" of risk and the question: "How safe is safe enough?" Nevertheless, for various industries in some countries [36, 37, 39] (or internationally) global risk goals have been established [43], [53].

To ensure that such a global risk level is achieved, realistic requirements must be set and an agreed risk management process should follow. This process must reflect continuous and evolutionary approaches to the achievement of safety and the management of all safety activities being an integral part of project activity, from the design phase throughout all phases of the life cycle of the entity.

At present, traditional engineering education teaches risk management only in a modest way. The plant engineer is trained to achieve the "function" of a product, an installation or a process. The safety engineer, on the other hand, must think about how this function can fail and, therefore, which safety measures are required and adequate to be installed for failure prevention and mitigation. To learn this way of thinking, we normally need "training on the job" and relevant publications such as lessons learned (*e.g.*, [64]). Only based on these conditions can safety engineers widen their know-how and knowledge base to keep pace with the ever more complex technical problems in NPPs.

A large volume of literature has been published related to "risk management" [36–42]. Financial risk, project risk, health risk, technical risk, and last but not least, gambling risk, have been evaluated and treated to a great extent. It is worth to mentioning that in the context of PRA the technical risk lies in the focus.

Considering advanced publications related to technical risk management one can observe that the ideal, classical, and prospective management process for *new* entities consists of four main steps:

- Risk goal setting.
- Apportionment of specific risk targets and transformation of these local risk targets into the considered entity.
- Proof of the compliance of the risk of the real entity with the goal settled.
- Controlling the risk of the real entity throughout the life cycle.

Obviously, much PRA work is performed related to *existing* entities, *e.g.*. the NPPs in operation, to assess the inherent risk. However, this retrospective process is not ideal for new NPPs.

Risk management should be a living mission at each technical entity. Therefore, it is continuously required to ask "what can go wrong?" and to adopt adequate safety measures to cope with the identified undesired events. This undertaking must be also in the interest of all the utilities to safeguard their investment.

In this context, the global term risk management should not be confused with specific project risk management (*i.e.*, investment costs and timescale risk). However, it should be noted that proper and timely application of risk management will also reduce the project risk for entities requiring a safety license prior to going into operation.

The risk management process can be subdivided into the following valuable documents and the respective managerial and technical activities required throughout the life cycle of an entity:

Document 1: The Global Risk Strategy.
Document 2: The Risk Management Program.
Document 3: The Risk Management Plan.

These three documents describe in the course of risk management the main goals, the required activities, and the results gained. They must be worked out by different parties within the establishment and can be characterized as documents followed by actions "starting from global aspects going towards detailed elements". (Remark: some Standards are calling Document 2 and Document 3 together "Program Plan" (*e.g.* [38].)

As it declares, Document 1 should be established and inaugurated by the top management of the establishment using all their competence and power. It can be generic, which means that the strategy would be binding for a given type (series) of entities. Document 2 should be established and implemented mainly by the project group for a given entity, and Document 3 should be established and the concurrent actions executed by the reliability and safety experts in the different working teams.

Document 1 must be available at least in the beginning of the life cycle (*e.g.*, the design phase); Documents 2 and 3 will be required over the life cycle, as it is dependent on the increasing information concerning the entity.

Thus, in other words, the three documents describe "what is why and how to do it" and are the results of the concurrent actions. In this sense, the documents demonstrate the qualification and the willingness of the establishment to be an organization of excellence related to the essential topic of "risk".

It must be concluded that such an ideal risk management process is really not existent within the nuclear technology and, therefore, it would be a great challenge for PRA practitioners, managers, and licensing authorities to steer developments resolving this vision.

71.3.2 Software Reliability

Conventionally, software, the related hardware, the sensors, the actuators, and the interconnection *via* a bus system are considered separately in safety assessments. This simplified approach does not model the real world adequately. Advanced insights of engineers and field experiences are pointing out that these elements should be considered as a "network" and that planned or unplanned interaction within this network should be studied.

However, such an undertaking would be an enormous step forward and can be seen as a new dimension of risk assessment. There is hope that sophisticated simulations on computer may illuminate the real world of digital control systems that is driven by software.

71.3.3 Test and Maintenance Induced Faults

It is common practice in reliability technology to perform various tests and maintenance work on real systems, thus achieving high confidence in reliability behavior throughout the life cycle. As a consequence, the reliability model for the estimation of system reliability should reflect the impact of these useful working procedures.

The classical hypothesis "as good as new after test and maintenance" is one of the related approaches to model system reliability analytically. When using this hypothesis, one has to be aware that more frequent tests and maintenance work (shorter time intervals) would improve, *e.g.*, for standby systems, the availability *per* demand, because recognized malfunctions would be immediately repaired. However, from field experience it is well known that tests and maintenance work can never be perfectly executed by the acting personnel. A given probability always exists that an additional and unforeseen fault be introduced into the system.

Thus, in other words, the "as good as new" hypothesis would not reflect the facts in the real world. Some modifications in all reliability calculation procedures would be the consequence. Therefore, it is a great challenge for PRA practitioners and managers to estimate the probability for test and maintenance induced faults based on specific field data acquisition. Some preliminary estimates for this type of introduced faults shows about a fraction of 20% of all the hidden faults.

71.4 Outlook

Risk is inherent in all the human undertakings and the man-made technological world. To assess it and to keep it under control is an essential task for sustainable welfare and successful industrial progress.

A new analytical tool based on engineering and operational experience named probabilistic risk/safety assessment has been under development for the last four decades. This methodology has found many applications and has reached a mature level of confidence, significantly expanding the insights gained by deterministic safety assessment [54]–[63]. It opens a window to see the real world of complex technologies not only in the case of perfect functioning but also in the case of malfunctions of man–machine in a given environment.

A PRA has been performed for most of the approximately 440 existing NPPs. Differences are given related to the extent (Level I, II, III) and the operational regimes considered (*e.g.*, full power, shut down stage). In so far there is a remarkable pool of PRA practitioners and related experience.

However, the ideal risk management process is largely missing for new NPPs. It should involve:

- risk goal setting,
- risk goal transformation into the plant under constriction,

- risk goal proof, and
- risk monitoring throughout the life cycle.

Obviously, this management process is interrelated with massive safety political and country specific questions, but the perception of the importance to close this significant break around the PRA process may steer fruitful developments.

It should be remembered that for various technologies, installations, or undertakings (*e.g.*, aviation, off-shore installations, ships, space modules, process plants, dangerous goods transport) national or international risk standards have been established for decision making in licensing procedures.

References

[1] USNRC: Theoretical possibilities and consequences in large nuclear power plants, WASH 740, 1957.

[2] Farmer FR. Siting criteria – A new approach. IAEA Symposium Vienna, IAEA SM-89/34. 1967; April.

[3] USNRC: Reactor safety study: An assessment of risks in US nuclear power plants. WASH 1400, NUREG -75/14, 1975.

[4] USNRC: Severe accident risk, an assessment for five U.S. nuclear power plants. NUREG-1150, 1991.

[5] US-NRC: Use of probabilistic risk assessment methods in nuclear activities, Final Policy Statement (FPS), Federal Register, 1995; August 16, 60: 42622.

[6] IEAE, Procedures for conducting probabilistic safety assessments for nuclear power plants (Level II). Safety Series No. 50-P-8, IAEA, Vienna, , ISBN 92-0-103195-X, June 1995.

[7] Bundesamt für Strahlenschutz (BfS): Grundlagen zur periodischen Sicherheitsüberprüfung für Kernkraftwerke, Dezember 1996.

[8] Berg H-P, Frömel T, Weil L. Updated requirements for safety reviews in Germany. ATW Journal, August September 2006; 526–531.

[9] ASME: Standard for probabilistic risk assessment for nuclear power plant application, ASME, 2002.

[10] US Congress: Risk assessment improvement act of 1994, Identifier: H. R. 4306, USA, 1994.

[11] Center for Risk Analysis, Harvard: Reform of risk regulation: Achieving more protection at less cost, Harvard School of Public Health, Boston, USA, 1995; March.

[12] Ale BJ, *et al*., Uijt de Haag, Zoning instruments for major accident prevention. Proceedings, ESREL'96-PSAM III, Crete, Springer, Berlin, 1996; 1911–1916.

[13] The Engineering Council: Guidelines on risk issues, The Engineering Council, U.K., 1993; ISBN 0-9516611-7-5.

[14] Kirchsteiger C.. (Editor). Risk assessment and management in the context of the Seveso II directive. Industrial Safety, Series 6, Elsevier, Amsterdam, 1998.

[15] Preyssl C. Safety risk assessment and management – The ESA approach. Reliability Engineering and System Safety 1995; 49:303–309.

[16] MHD: Besluit Risiko's Zware Ongevallen, Mayor Hazard Decree, Staatsblad 291, Staatsdrukkerij, The Netherlands, 1992.

[17] BUWAL: Handbuch 1 zur Störfallverordnung StFV, und Beurteilungskriterien zur Störfallverordnung, Bundesamt (BUWAL), Schweiz, Juni 1991, August 2001.

[18] Kirchsteiger, C.: On the use of probabilistic and deterministic methods in risk analysis, Journal of Loss Prevention 1999; 12:399–419.

[19] ESA: Proceedings of First IAASS Conference on Space Safety, a new beginning", 25-27 October 2005, Nice, France, ESA SP- 599, 2005; December.

[20] Mihm P. Acceptable risk level, 5th Framework Programme EC, SAMRAIL Project, WP 2.4, , 2004; June 23.

[21] EASA: Certification specifications for large aeroplanes. European Aviation Safety Agency, CS-25, Book-1, Airworthiness Code, 2004.

[22] Klein M, Schueller GI, Esnault P. Guidelines for factors of safety for aerospace structures. Proceedings, ESREL'96-PSAM III, Crete, Springer, Berlin, 1996:1696–1701.

[23] Kafka P. International perspectives on the use of probabilistic safety assessment (PSA) in Industry. Panel Discussion, PSAM7-ESREL'04 Conference, Berlin 2004; June 14–18.

[24] Spouge J. Risk acceptance criteria for ships, DNV Technica, C7458, 1999.

[25] NASA: Probabilistic risk assessment procedure guide for NASA managers and practitioners**,** Version 1.1. NASA Headquarters; August, 2002.

[26] Eurocourse PSARID: Probabilistic Safety and Risk-informed Decision Making, GRS, 2001; March 5–9.

[27] Baier M, Schäfer A. PSA-International Aspects, ATW Journal, January 2005; 25–31.

[28] Kröger W, Chang Sang-Lung. Reflexions on current and future nuclear safety. ATW Journal, 2006; July: 458–469.
[29] OECD, WGIP: Level II methodology and severe accident management. 1997, www.nea.fr/html/nsd/docs/1997/csni-r1997-11.pdf
[30] Shooman M. Probabilistic reliability: An engineering approach. 2nd Edition. Kreiger, Melbourne, FL, 1990.
[31] Blockley D. Editor. Engineering safety. McGraw-Hill, New York, 1992.
[32] Kafka P. Probabilistic safety assessment: Quantitative process to balance design, manufacturing and operation for safety of plant structures and systems. Nuclear Engineering and Design 1996; 165:333–350.
[33] Swain A, Guttmann H. Handbook of human reliability analysis with emphasis on nuclear power plant application. NUREG/CR-1278, 1983; August.
[34] Apostolakis G. The concept of probability in safety assessment of technological systems. Science 1990; 50:1359–1366.
[35] Ministry of Defense U.K.:Safety management requirements for defense systems. Standard 00-56, Part 1 and 2, 1996.
[36] Canadian Standards Association: Risk management guidelines for decision makers. CAN/CSA-Q 850-97, Ontario, Canada, 18. Jan. 2000.
[37] Standards Australia: Risk Management Standard AS.NZS 4360:1999, Homebush, Australia, 1999.
[38] British Standard Institution: Risk management standard, BS-6079-3:2000, London, 2000
[39] DNV: Structural reliability analysis of marine structures, Classification AS, N-1322, Horvic, June, 1992.
[40] Bonano E, PeiI K. Risk assessment: A defensible foundation for environmental management decision making. Proceedings, ESREL96-PSAM III, Crete, Springer, Berlin, 1996; 2117–2121.
[41] Kafka P. Risk management– An indispensable installation. Proceedings International Symposium on Safety Science and Technology, Shanghai, China. Science Press, Bejing, ISBN 7-03-014386-8, 2004; October 25–28: 2517–2527
[42] Kafka P, Spallek R. Risikomanagement über den Lebenszyklus eines Produkts. Risk-tech Tagung, TÜV Automotiv GmbH München, Nov. 11–12 2004.
[43] Kafka P. How safe is safe enough? – An unresolved issue for all technologies. Proceedings of ESREL'99, A.A. Balkema, Rotterdam 1999, ESREL'99, 1999; September 13–17: 385–390.
[44] Hessel PP. Toward risk based regulation. Proceedings, ESREL96-PSAM III, Crete, Springer, Berlin, 1996; 339–342.
[45] Recherche Transports Sécurité. Des principes de sécurité GAME, MEM, ALARP. 2000; July–Sept., 68: 48–65.
[46] US NRC: Safety goals for nuclear power plant operation. US NRC, NUREG-0880, Washington DC, 1996.
[47] Watson I. Developments in risk management, Paper, ESREL'93, Munich, VDI Verlag, Düsseldorf, 1993; 511–521.
[48] Kafka P, Sicherheit großtechnischer Anlagen. TÜ.VDI Verlag, Düsseldorf, 9/95; September: 354–357.
[49] Petersen K, Sieger K, Kongso H. Setting reliability targets for the great belt link tunnel equipment. European Safety, Reliability and Data Association (ESReDA) Seminar. Amsterdam, Holland, April 1992.
[50] Aven T, Nja O, Retteda W. On risk acceptance and risk interpretation. Proceedings ESREL'96-PSAM III, Crete, Springer, Berlin, 1996: 2191–2196.
[51] International Atomic Energy Agency. The safety of nuclear power. IAEA: INSAG-5, Safety Series No. 75-INSAG-5, Vienna 1992.
[52] CNSC, Draft regulatory standard – Probabilistic safety assessment (PSA) for nuclear power plants. Canadian Nuclear Safety Commission. 2004; June: S-294.
[53] Kafka P. The process of safety management and decision making. International Journal of Performability Engineering 2006; October,2(4):315–329.
[54] US-NRC: An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis. RG 1.175, RG 1.176, RG 1.177, RG 1.178, July 1998 (http://www.nrc.goc)
[55] US-NRC: Risk-informed implementation plan. RIRIP, 2001, (http://www.nrc.gov)
[56] US-NRC: Reactor oversight process, ROP, 2000l;July (http://www.nrc.gov)
[57] Murphy J. Risk-based regulation: Practical experience in using risk-related insights to salve regulatory issues. Proceedings, KAERI, PSN95, Seoul November 1995: 945–948.
[58] Kafka P. Screening of status of probabilistic safety evaluations for different advanced reactor concepts. EU Report for JRC Petten, December, 2004.
[59] Kafka P. Harmonisation in the field of safety of nuclear installations. Level 1 of Probabilistic

Safety Assessment (PSA), Report for EU DG XI, 1999.

[60] Fragola JR, Shooman ML Experience bounds a nuclear plant probabilistic safety assessment. Proceedings Annual IEEE Reliability and Maintainability Symposium (RAMS) Jan. 21-23, 1992: 157–165.

[61] Thadani A, Murphy J. Risk-informed regulation - issues and prospects for its use in reactor regulation in den USA. Proceedings, ESREL'96-PSAM III, Crete, Springer, Berlin, 1996; 2172–2177.

[62] Kafka P.The process of safety management and decision making. ESREL2005 Conference, Tri City, Proceedings, Balkema AA, Poland 2005; 27–30 June: 1003–1010.

[63] Kafka P. Risk monitoring systems. Proceedings PSAM7-ESREL'04 Conference, Springer, Berlin, 2004; June 14–18: 2635–2640.

[64] Misra KB, editor. Special issue on risk management and safety, International Journal of Performability Engineering, January 2007; 3(1); Parts I and II.

72

Software Reliability and Fault-tolerant Systems: An Overview and Perspectives

Hoang Pham

Rutgers University, USA

Abstract: This chapter outlines the basic concepts of software development process, reliability engineering, and data analysis. It also presents some of the existing NHPP software reliability models and their applications. Numerical examples are provided to illustrate the results. A generalized software reliability model considering environmental factors is presented and Sections 72.5 and 72.6 discuss briefly the software fault-tolerant concepts and software cost models, respectively.

72.1 Introduction

Today, almost everyone in the world is directly or indirectly affected by computer systems. Computers are used in diverse areas for various applications, including air traffic control, nuclear reactors, aircraft, real-time sensor networks, industrial process control, automotive mechanical and safety control, and hospital health care, affecting many millions of people. One application of computer systems to hospital health care is the monitoring of heart patients. In hospitals so equipped, sensors that detect electrical signals associated with heart activity are attached to the patient's heart area. The signals from these sensors are transmitted along wires to a computer programmed to analyze such data. If the incoming data indicate that the patient is doing well, the computer generates no output. If the data indicate the onset of serious conditions, the computer signals an alarm at the nursing station indicating which patient needs human care and the kind of help most apt to be useful.

As the functionality of computer operations becomes more essential and yet more complicated and critical applications increase in size and complexity, there is a great need for looking at ways to quantify and predict the reliability of computer systems in various complex operating environments. Faults, especially with logic, in software design thus become more subtle. Usually logic errors in the software are not hard to fix but diagnosing logic bugs is the most challenging for many reasons. The fault again is usually subtle. For example, a man wants to withdraw $50 at an automatic transfer machine (ATM) from a checking account held jointly with his wife. Almost simultaneously, at another machine, his wife also begins the deposit of $500. Both the husband's and the wife's ATM read the account balance of $100 from the memory at the bank's central computer. While the first ATM (husband's machine) subtracts the withdrawal, the second ATM adds the

deposit. Because withdrawals often take slightly longer to process than deposits, the wife's ATM records a new balance of $600 before her husband's transaction is complete. His ATM, obviously not knowing that the old balance has been changed and in fact increased, records a wrong balance of $50, instead of the new balance, which should be $550!

An error is a mental mistake made by the programmer or designer. A fault is the manifestation of that error in the code. A software failure is defined as the occurrence of an incorrect output as a result of an input value that is received with respect to the specification. Figure 72.1 demonstrates how a software fault triggered by a specific input leads to software failure.

In recent years, the cost of developing software and the penalty cost of software failure have become a major expense in the whole system [32]. Failure of the software may result in an unintended system state or course of action. A loss event could ensue in which property is damaged or destroyed, people are injured or killed, and/or monetary costs are incurred. A quantitative measure of loss is called the risk cost of failure [36]. In other words, risk cost is a quantitative measure of the severity of loss resulting from a software failure. A research study has shown that professional programmers average six software defects for every 1000 lines of code (LOC) written. At that rate, a typical commercial software application of 500,000 LOCs may contain about 3000 programming errors including memory-related errors, memory leaks, language-specific errors, extra compilation errors, standard library errors, *etc*.

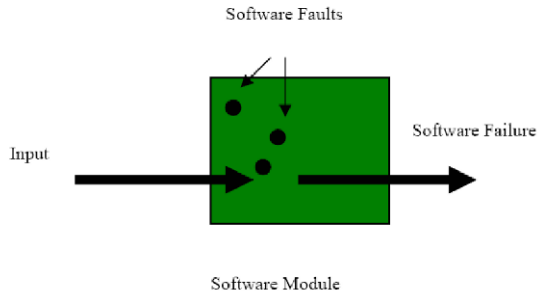


Figure 72.1. Relationship between software fault and software failure

As software projects become larger, the rate of software defects increases geometrically (see Figure 72.2). Table 72.1 shows the defect rates of several software applications *per* 100 LOC. Locating software faults is extremely difficult and costly. A study conducted by Microsoft showed that it takes about 12 programming hours to locate and correct a software defect. At this rate, it can take more than 24000 hours (or 11.4 man-years) to debug a program of 350000 LOC at a cost of over US$1 million [42].

Software errors have caused spectacular failures, some with dire consequences, such as the following examples. On 31 March 1986, a Mexicana Airlines Boeing 727 airliner crashed into a mountain because the software system did not correctly negotiate the mountain position. Between March and June 1986, the massive Therac-25 radiation therapy machines in Marietta, Georgia; Boston, Massachusetts; and Tyler, Texas overdosed cancer patients due to flaws in the computer program controlling the highly automated devices. On 26 June 1988, Air France's new A320 model, delivered just two days before, crashed into the trees at an air show near Mulhouse in France due to computer software failure while performing a low-level pass. Three passengers were killed.

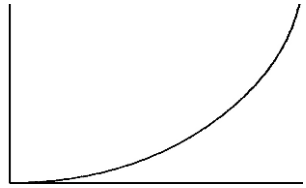


Figure 72.2. The rate of software defect changes

Table 72.1. Defect rates of several software applications

Application	Number of systems	Fault density (*per* 100 LOC)
Airborne	8	1.28
Strategic	18	0.66
Tactical	6	1.00
Process control	2	0.18
Production	9	1.30
Developmental	2	0.40

During the period 2–4 November 1988, a computer virus infected software at universities and defense research centers in the United States causing system failures. On 10 December 1990, Space Shuttle Columbia was forced to land early due to computer software problems. On 17 September 1991, a power outage at the AT&T switching facility in New York City interrupted service to 10 million telephone users for 9 hours. The problem was due to the deletion of three bits of code in a software upgrade and failure to test the software before its installation in the public network [48].

On 14 August 2003, a blackout that crippled most of the Northeast corridor of the United State and parts of Canada resulted from a software failure at First Energy Corporation, which may have contributed significantly to the outage. In 1992, the London Ambulance service switched to a voice and computer control system, which logged all its activities. However, when the traffic to the computer increased the software could not cope and slowed down; as a consequence it lost track of the ambulances. On 26 October 1992, the computer-aided dispatch system of the ambulance service in London, which handles more than 5000 requests daily in the transportation of patients in critical condition, failed after installation. This led to serious consequences for many critical patients.

A recent inquiry revealed that a software design error and insufficient software testing caused an explosion that ended the maiden flight of the European Space Agency's (ESA) Ariane 5 rocket, less than 40 seconds after lift-off on 4 June 1996. The problems occurred in the flight control system and were caused by a few lines of the Ada code containing three unprotected variables. The ESA estimates that corrective measures will amount to US$362 million [42].

Generally, software faults are more insidious and much more difficult to handle than physical defects. In theory, software can be error-free, and unlike hardware, does not degrade or wear out but deteriorates. The deterioration here, however, is not a function of time. Rather, it is a function of the results of changes made to the software during maintenance, through correcting latent defects, modifying the code to changing requirements and specifications, environments and applications, or improving software performance. All design faults are present from the time the software is installed on the computer. In principle, these faults could be removed completely, but in reality the goal of perfect software remains elusive [10]. Computer programs, which vary for fairly critical applications between hundreds and millions of lines of code, can make the wrong decision because the particular inputs that triggered the problem were not tested and corrected during the testing phase. Such inputs may even have been misunderstood or unanticipated by the designer who either correctly programmed the wrong interpretation or failed to identify the problem. These situations and other such events have made it apparent that we must determine the reliability of the software systems before putting them into operation.

72.2 The Software Development Process

As software becomes an increasingly important part of many different types of systems that perform complex and critical functions in many applications, such as military defense, nuclear reactors, *etc*., the risk and impacts of software-caused failures have increased dramatically. There is now general agreement on the need to increase software reliability by eliminating errors made during software development. Software is a collection of instructions or statements in a computer program. A program can be regarded as a function, mapping the input space to the output space, where the input space is the set of all input states, and the output space is the set of all output states. An input state can be defined as a combination of input variables or a typical transaction to the program. A software program is designed to perform specified functions. When the actual output deviates from the expected output, a failure occurs.

A software life cycle consists of five successive phases: analysis, design, coding, testing, and operation [42]. The *analysis phase* is the most important phase, the first step in the software development process and the foundation of building a successful software product. The

purpose of the analysis phase is to define the requirements and provide specifications for the subsequence phases and activities. The *design phase* is concerned with how to build the system to behave as described. The *coding phase* involves translating the design into code in a programming language. Coding can be decomposed into the following activities: identify reusable modules, code editing, code inspection, and final test plan. *The testing phase* is the verification and validation activity for the software product. Verification and validation (V&V) are the two ways to check if the design satisfies the user requirements. The *operation phase* is the final phase in the software life cycle. It involves the transfer of responsibility for the maintenance of the software from the developer to the user by installing the software product and it becomes the user's responsibility to establish a program to control and manage the software.

There are two commonly types of failure data: time-domain data and interval-domain data. Some existing software reliability models can handle both types of data. The time-domain data is characterized by recording the individual times at which the failure occurred. For example, in the real-time control system data [24], there are totally 136 faults reported and the time-between failures (TBF) in seconds are listed in Table 72.2. The interval-domain data is characterized by counting the number of failures occurring during a fixed period. The time-domain data always provides better accuracy in the parameter estimates with current existing software reliability models, but involves more data collection efforts than the interval domain approach.

72.3 Software Reliability Modeling

Since computers are being used increasingly to monitor and control both safety-critical and civilian systems, there is a great demand for high-quality software products. Reliability is a primary concern for both software developers and software users.

Research activities in software reliability engineering have been conducted, and a number of NHPP software reliability growth models [11], [26],[36],[37],[39],[40],[41],[45],[46],[47],[57], [58],[65] have been developed to assess the reliability of software. Software reliability models based on the NHPP have been quite successful tools in practical software reliability engineering. In this paper, we only discuss software reliability models based on NHPP. These models consider the debugging process as a counting process characterized by its mean value function. Software reliability, can be estimated once the mean value function is determined. Model parameters are usually estimated using either the maximum likelihood method or least squared estimate.

The following acronyms and notation will be used throughout the paper.

Acronyms

AIC	the Akaike information criterion
MLE	maximum likelihood estimate
NHPP	non-homogeneous Poisson process
SRGM	software reliability growth model
SSE	sum of squared errors

Notation

$a(t)$	time dependent fault content function
$b(t)$	time dependent fault detection-rate function *per* fault *per* unit time
$m(t)$	expected number of error detected by time t ("mean value function")
$R(x/t)$	software reliability function, *i.e.*, the conditional probability of no failure occurring during $(t, t+x)$ given that the last failure occurred at time t
^	estimates using the MLE method

72.3.1 A Generalized NHPP Model

Many existing NHPP models assume that failure intensity is proportional to the residual fault content. A general class of NHPP SRGMs can be obtained by solving the following differential equation [40]:

$$\frac{dm(t)}{dt} = b(t)[(a(t) - m(t)].$$

The general solution of the above differential equation is given by

Table 72.2. The real-time control system data for time domain approach

Fault	TBF	Cum. TBF	Fault	TBF	Cum. TBF	Fault	TBF	Cum. TBF	Fault	TBF	Cum. TBF
1	3	3	35	227	5324	69	529	15806	103	108	42296
2	30	33	36	65	5389	70	379	16185	104	0	42296
3	113	146	37	176	5565	71	44	16229	105	3110	45406
4	81	227	38	58	5623	72	129	16358	106	1247	46653
5	115	342	39	457	6080	73	810	17168	107	943	47596
6	9	351	40	300	6380	74	290	17458	108	700	48296
7	2	353	41	97	6477	75	300	17758	109	875	49171
8	91	444	42	263	6740	76	529	18287	110	245	49416
9	112	556	43	452	7192	77	281	18568	111	729	50145
10	15	571	44	255	7447	78	160	18728	112	1897	52042
11	138	709	45	197	7644	79	828	19556	113	447	52489
12	50	759	46	193	7837	80	1011	20567	114	386	52875
13	77	836	47	6	7843	81	445	21012	115	446	53321
14	24	860	48	79	7922	82	296	21308	116	122	53443
15	108	968	49	816	8738	83	1755	23063	117	990	54433
16	88	1056	50	1351	10089	84	1064	24127	118	948	55381
17	670	1726	51	148	10237	85	1783	25910	119	1082	56463
18	120	1846	52	21	10258	86	860	26770	120	22	56485
19	26	1872	53	233	10491	87	983	27753	121	75	56560
20	114	1986	54	134	10625	88	707	28460	122	482	57042
21	325	2311	55	357	10982	89	33	28493	123	5509	62551
22	55	2366	56	193	11175	90	868	29361	124	100	62651
23	242	2608	57	236	11411	91	724	30085	125	10	62661
24	68	2676	58	31	11442	92	2323	32408	126	1071	63732
25	422	3098	59	369	11811	93	2930	35338	127	371	64103
26	180	3278	60	748	12559	94	1461	36799	128	790	64893
27	10	3288	61	0	12559	95	843	37642	129	6150	71043
28	1146	4434	62	232	12791	96	12	37654	130	3321	74364
29	600	5034	63	330	13121	97	261	37915	131	1045	75409
30	15	5049	64	365	13486	98	1800	39715	132	648	76057
31	36	5085	65	1222	14708	99	865	40580	133	5485	81542
32	4	5089	66	543	15251	100	1435	42015	134	1160	82702
33	0	5089	67	10	15261	101	30	42045	135	1864	84566
34	8	5097	68	16	15277	102	143	42188	136	4116	88682

$$m(t) = e^{-B(t)}\left[m_0 + \int_{t_0}^{t} a(\tau)b(\tau)e^{B(\tau)}d\tau\right],$$

where $B(t) = \int_{t_0}^{t} b(\tau)d\tau$ and $m(t_0) = m_0$ is the marginal condition of the above differential equation with t_0 representing the starting time of the debugging process. The reliability function based on the NHPP is given by:

$$R(x/t) = e^{-\left[m(t+x)-m(t)\right]}.$$

Many existing NHPP models can be considered as a special case of the above general model.

An increasing function *a(t)* implies an increasing total number of faults (note that this includes those already detected and removed and those inserted during the debugging process) and reflects imperfect debugging. An increasing *b(t)* implies an increasing fault detection rate, which could be either attributed to a learning curve phenomenon, or to software process fluctuations, or a combination of both. Different *a(t)* and *b(t)* functions also reflect different assumptions of the software testing processes. A summary of the most NHPP existing models is presented in Table 72.3.

Table 72.3. Summary of the mean value functions [40]

Model name	Model type	m(t)	Comments
Goel–Okumoto (G-O)	Concave	$m(t) = a(1 - e^{-bt})$ $a(t) = a, b(t) = b$	Also called the exponential model
Delayed S-shaped	S-shaped	$m(t) = a(1 - (1 + bt)e^{-bt})$	Modification of the G-O model to make it S-shaped
Inflection S-shaped SRGM	S-shaped	$m(t) = \frac{a(1 - e^{-bt})}{1 + \beta e^{-bt}}$ $a(t) = a, b(t) = \frac{b}{1 + \beta e^{-bt}}$	Solves a technical condition with the G-O model. Becomes the same as G-O if $\beta = 0$
Yamada Exponential	S-shaped	$m(t) = a(1 - e^{-r\alpha(1 - e^{(-\beta t)})})$ $a(t) = a, b(t) = r\alpha\beta e^{-\beta t}$	Attempt to account for testing-effort
Yamada Rayleigh	S-shaped	$m(t) = a(1 - e^{-r\alpha(1 - e^{(-\beta t^2/2)})})$ $a(t) = a, b(t) = r\alpha\beta t e^{-\beta t^2/2}$	Attempt to account for testing-effort
Yamada exponential imperfect debugging model (Y-ExpI)	Concave	$m(t) = \frac{ab}{\alpha + b}(e^{\alpha t} - e^{-bt})$ $a(t) = ae^{\alpha t}, b(t) = b$	Assume exponential fault content function and constant fault detection rate
Yamada linear imperfect debugging model (Y-LinI)	Concave	$m(t) = a[1 - e^{-bt}][1 - \frac{\alpha}{b}] + \alpha a t$ $a(t) = a(1 + \alpha t), b(t) = b$	Assume constant introduction rate α and the fault detection rate
Pham–Nordmann–Zhang (P-N-Z) Model	S-shaped and concave	$m(t) = \frac{a[1 - e^{-bt}][1 - \frac{\alpha}{b}] + \alpha a t}{1 + \beta e^{-bt}}$ $a(t) = a(1 + \alpha t), b(t) = \frac{b}{1 + \beta e^{-bt}}$	Assume introduction rate is a linear function of testing time, and the fault detection rate function is non-decreasing with an inflexion S-shaped model.
Pham–Zhang (P-Z) Model	S-shaped and concave	$m(t) = \frac{1}{(1 + \beta e^{-bt})}[(c + a)(1 - e^{-bt}) - \frac{a}{b - \alpha}(e^{-\alpha t} - e^{-bt})]$ $a(t) = c + a(1 - e^{-\alpha t}), b(t) = \frac{b}{1 + \beta e^{-bt}}$	Assume introduction rate is exponential function of the testing time, and the fault detection rate is non-decreasing with an inflexion S-shaped model

72.3.2 Application 1: The Real-time Control System

We perform the model analysis using the real-time control system data given in Table 72.2. The first 122 data points are used for the goodness of fit test and the remaining data are used for the predictive power test. The results for fit and prediction are listed in Table 72.4. Although software reliability models based on the NHPP have been quite successful tools in practical software reliability engineering [42], there is a need to validate their validity with respect to other applications such as communications, manufacturing, medical monitoring, and defense systems.

72.4 Generalized Models with Environmental Factors

Most existing models, however, require considerable numbers of failure data in order to obtain an accurate reliability prediction. Information concerning the development of the software product, the method of failure detection, environmental factors, *etc*., however, are ignored to almost all the existing models. In order to develop a useful software reliability model and to make sound judgments when using the model, one needs to have an in-depth understanding of how software is produced; how errors are introduced, how software is tested, how errors occur, types of errors and environmental factors can help us in justifying the reasonableness of the assumptions, the usefulness of the model, and the applicability of the model under a given user environment [48]. In other words, these models would be valuable to software developers, users, and practitioners if they are capable of using information about the software development process, incorporating the environmental factors, and are able to give greater confidence in estimates based on small numbers of failure data.

This section discusses a generalized software reliability model with environmental factors.

Table 72.4. Parameter estimation and model comparison

Model name	SSE (fit)	SSE(Predict)	AIC	MLEs
G -O model	7615.1	704.82	426.05	$\hat{a} = \mathbf{125}$, $\hat{b} = \mathbf{0.00006}$
Delayed S-shaped	51729.23	257.67	546	$\hat{a} = \mathbf{140}$, $\hat{b} = \mathbf{0.00007}$
Inflexion S-shaped	15878.6	203.23	436.8	$\hat{a} = \mathbf{135.5}, \hat{b} = \mathbf{0.00007}, \hat{\beta} = \mathbf{1.2}$
Yamada exponential	6571.55	332.99	421.18	$\hat{a} = \mathbf{130}, \hat{\alpha} = \mathbf{10.5}, \hat{\beta} = \mathbf{5.4 \times 10^{-6}}$
Yamada Rayleigh	51759.23	258.45	548	$\hat{a} = \mathbf{130}, \hat{\alpha} = \mathbf{5 \times 10^{-10}}, \hat{\beta} = \mathbf{6.035}$
Y-ExpI model	5719.2	327.99	450	$\hat{a} = \mathbf{120}$, $\hat{b} = \mathbf{0.00006}$, $\hat{\alpha} = \mathbf{1 \times 10^{-5}}$
Y-LinI model	6819.83	482.7	416	$\hat{a} = \mathbf{120.3}, \hat{b} = \mathbf{0.00005}, \hat{\alpha} = \mathbf{3 \times 10^{-5}}$
P-N-Z Model	5755.93	106.81	415	$\hat{a} = \mathbf{121}, \hat{b} = \mathbf{0.00005}, \hat{\alpha} = \mathbf{2.5 \times 10^{-6}}, \hat{\beta} = \mathbf{0.002}$
P-Z model	14233.88	85.36	416	$\hat{a} = \mathbf{20}, \hat{b} = \mathbf{0.00007}, \hat{\alpha} = \mathbf{1.0 \times 10^{-5}}, \hat{\beta} = \mathbf{1.922}$ $\hat{c} = \mathbf{125}$

Additional Notation

$\tilde{z}$	Vector of environmental factors
$\tilde{\beta}$	Coefficient vector of environmental factors
$\Phi(\tilde{\beta}\ \tilde{z})$	Function of environmental factors
$\lambda_0(t)$	Failure intensity rate function without environmental factors
$\lambda(t,\tilde{z})$	Failure intensity rate function with environmental factors
$m_0(t)$	Mean value function without environmental factors
$m(t,\tilde{z})$	Mean value function with environmental factors
$R(x/t,\tilde{z})$	Reliability function with environmental factors

The proportional hazard model (PHM), which was first proposed in [7], has been successfully utilized to incorporate environmental factors in survival data analysis in medical field and in hardware system reliability area.

The basic assumption for PHM is that the hazard rates of any two items associated with the settings of environmental factors, say z_1 and z_2, respectively, will be proportional to each other. The environmental factors are also known as covariates in PHM. When the PHM applied to the non-homogeneous Poisson process, it becomes the proportional intensity model (PIM).

A general fault intensity rate function incorporating the environmental factors based on PIM can be constructed using the following assumptions:

(a). The new fault intensity rate function consists of two components: the fault intensity rate functions without environmental factors, $\lambda_0(t)$, and the environmental factor function, $\Phi(\tilde{\beta}\ \tilde{z})$.

(b). The fault intensity rate function $\lambda_0(t)$ and the function of the environmental factors are independent. The function $\lambda_0(t)$ is also called the baseline intensity function.

Let us assume that the fault intensity function $\lambda(t,\tilde{z})$ is given in the form:

$$\lambda(t,\tilde{z}) = \lambda_0(t)\cdot\Phi(\tilde{\beta}\ \tilde{z}),$$

where

$$\Phi(\tilde{\beta}\ \tilde{z}) = \exp(\beta_0 + \beta_1 z_1 + \beta_2 z_2 + \ldots).$$

The mean value function and reliability function with environmental factors can be obtained, respectively:

$$m(t,\tilde{z}) = \Phi(\tilde{\beta}\ \tilde{z}) m_0(t)$$

and

$$R(x/t,\tilde{z}) = [R_0(x/t)]^{\Phi(\tilde{\beta}\ \tilde{z})}$$

A widely used method, which is known as the partial likelihood estimate method, can be used to estimate the unknown parameters of the software reliability model with environmental factors. The partial likelihood method estimates the coefficients of covariates, the β_I's, separately from the parameters in the baseline intensity function. The likelihood function of the partial likelihood method is given by [7]:

$$L(\beta) = \prod_i \frac{\exp(\beta z_i)}{[\sum_{m\in R}\exp(\beta z_m)]^{d_i}},$$

where d_i represents the tie failure times.

72.4.1 Application 2: The Real-time Monitor Systems

In this section, we illustrate the software reliability model with environmental factors based on the PIM method using the software failure data collected from the real-time monitor systems [55]. The software consists of about 200 modules and each module has, on average, 1000 lines of a high-level language like FORTRAN. Total 481 software faults were detected during 111-day testing period. Both the information of testing team size and the software failure data are recorded.

The only environmental factor available in this application is the testing team size. Team size is one of the most useful measures in the software development process. It has close a relationship with the testing effort, testing efficiency and the development management issues. From the correlation analysis of the 32 environmental factors [65], team size is the only factor correlated to the

program complexity, which is the number one significant factor according to our environmental factor study. Intuitively, the more complex the software, the larger team is required. Since the testing team size ranges from 1 to 8, we first categorize the factor of team size into two levels. Let z_1 denote the factor of team size as follows:

$$z_1 = \begin{cases} 0 & \text{team size ranges from 1-4} \\ 1 & \text{team size ranges from 5-8} \end{cases}$$

After carefully examining the failure data, we find that after day 61, the software turns stable and the failures occur with a much slower frequency. Therefore, we use the first 61 data points for testing the goodness-of-fit and estimating the parameters, and use the remaining 50 data points (from day 62 to day 111) as real data for examining the predictive power of software reliability models.

In this application, we use the P-Z model listed in Table 72.3 as the baseline mean value function, that is,

$$m_0(t) = \frac{1}{(1+\beta\, e^{-bt})}[(c+a)(1-e^{-bt}) - \frac{ab}{b-\alpha}(e^{-\alpha t} - e^{-bt})]$$

and the corresponding baseline intensity function can be expressed as follows:

$$\lambda_0(t) = \frac{1}{(1+\beta\, e^{-bt})}[(c+a)(1-e^{-bt}) - \frac{ab}{b-\alpha}(e^{-\alpha t} - e^{-bt})] + \frac{-\beta b e^{-bt}}{(1+\beta e^{-bt})^2}[(c+a)(1-e^{-bt}) - \frac{ab(e^{-\alpha t} - e^{-bt})}{b-\alpha}]$$

Therefore, the intensity function with environmental factor is given by [62]:

$$\lambda(t) = \lambda_0(t) \cdot e^{\beta_1 z_1} = \left\{ \begin{array}{l} \frac{1}{(1+\beta\, e^{-bt})}[(c+a)(1-e^{-bt}) - \frac{ab}{b-\alpha}(e^{-\alpha t} - e^{-bt})] + \\ \frac{-\beta b e^{-bt}}{(1+\beta e^{-bt})^2}[(c+a)(1-e^{-bt}) - \frac{ab(e^{-\alpha t} - e^{-bt})}{b-\alpha}] \end{array} \right\} e^{\beta_1 z_1}$$

The estimate of β_1 using partial likelihood estimate method is $\hat{\beta}_1 = 0.0246$ which indicates that this factor is significant to consider. The estimates of parameters in the baseline failure intensity function above are as follows:

$\hat{a} = 40.0, \hat{b} = 0.09, \hat{\beta} = 8.0, \hat{\alpha} = 0.015, \hat{c} = 450$

The results of several existing NHPP models are also listed in Table 72.5.

The results show that incorporating the factor of team size into the P-Z model that explains the fault detection better and thus enhances the predictive power of this model. Further research is needed to incorporate application complexity, test effectiveness, test suite diversity, test coverage, code reused, and real application operational environments into the NHPP software reliability models and into the software reliability model in general [48].

72.5 Fault-tolerant Software Systems

Fault-tolerance has become one of the major concerns of computer designers. It is important to provide high reliability to critical applications such as aircraft controller and nuclear reactor controller software systems. No matter how thorough the testing, debugging, modularization, and verification of software are, design bugs still plague the software. After reaching a certain level of software refinement, any effort to increase the reliability, even by a small margin, will increase exponential cost. Over the last three decades, there has been considerable research in the area of fault-tolerant software.

Fault-tolerant software has been considered for use in a number of critical areas of application. For example, in traffic control systems, the computer aided traffic control system (COMTRAC) [20] is a fault-tolerant computer system designed to control the Japanese railways. It consists of three symmetrically interconnected computers. Two computers are synchronized at the program task level while the third acts as an active-standby. Each computer can be in one of the following states: on-line control, standby, or offline. The COMTRAC software has a symmetric configuration. The configuration system contains the configuration control program and the dual monitor system contains the state control program. When one of the computers under dual operation has a fault, the state control program switches the system to single operation and reports the completion of the system switching to the configuration control program. The configuration control program commands the state control program to switchover to dual operation with the standby computer. The latter program then executes the system switchover, transferring

Table 72.5. Model evaluation

Model name	***m*(*t*)**	**SSE(Prediction)**	**AIC**
G-O model	$m(t) = a(1 - e^{-bt}), a(t) = a, b(t) = b$	1052528	978.14
Delayed S-shaped	$m(t) = a(1 - (1 + bt)e^{-bt})$ $a(t) = a, b(t) = \frac{b^2 t}{1 + bt}$	83929.3	983.90
Inflexion S-shaped	$m(t) = \frac{a(1 - e^{-bt})}{1 + \beta e^{-bt}}, a(t) = a, b(t) = \frac{b}{1 + \beta e^{-bt}}$	1051714.7	980.14
Yamada Exponential	$m(t) = a(1 - e^{-r\alpha(1 - e^{(-\beta t)})}), a(t) = a$ $b(t) = r\alpha\beta e^{-\beta t}$	1085650.8	979.88
Yamada Rayleigh	$m(t) = a(1 - e^{-r\alpha(1 - e^{(-\beta t^2/2)})}), a(t) = a$ $b(t) = r\alpha\beta t e^{-\beta t^2/2}$	86472.3	967.92
Y-ExpI model	$m(t) = \frac{ab}{\alpha + b}(e^{\alpha t} - e^{-bt}), a(t) = ae^{\alpha t},$ $b(t) = b$	791941	981.44
Y-LinI model	$m(t) = a[1 - e^{-bt}][1 - \frac{\alpha}{b}] + \alpha a t,$ $a(t) = a(1 + \alpha t), b(t) = b$	238324	984.62
P-N-Z model	$m(t) = \frac{a}{1 + \beta e^{-bt}}[(1 - e^{-bt})(1 - \frac{\alpha}{b}) + \alpha t]$ $a(t) = a(1 + \alpha t), b(t) = \frac{b}{1 + \beta e^{-bt}}$	94112.2	965.37
P-Z model	$m(t) = \frac{1}{(1 + \beta e^{-bt})}[(c + a)(1 - e^{-bt}) - \frac{ab}{b - \alpha}(e^{-\alpha t} - e^{-bt})]$ $a(t) = c + a(1 - e^{-\alpha t}), b(t) = \frac{b}{1 + \beta e^{-bt}}$	86180.8	960.68
Environmental Factor model	$m(t) = \frac{1}{(1 + \beta e^{-bt})}[(c + a)(1 - e^{-bt}) - \frac{ab}{b - \alpha}(e^{-\alpha t} - e^{-bt})]e^{\beta_1 z_1}$ $a(t) = c + a(1 - e^{-\alpha t}), c(t) = 1 - \frac{(1 + \beta)}{(e^{bt} + \beta)}$	560.82	890.68

control to the configuration control program, which judges the accuracy of the report and indicates its own state to the other computers. COMTRAC shows that it failed seven times during a three-year period – once due to hardware failure, five times due to software failure, and once for unknown causes.

Software fault-tolerance is achieved through special programming techniques that enable the software to detect and recover from failure incidents. This section discusses a basic concept for fault-tolerant software techniques and some advanced techniques including self-checking systems.

Fault-tolerant software assures system reliability by using protective redundancy at the software level. There are two basic techniques for obtaining fault-tolerant software:

- The RB scheme
- NVP

Both schemes are based on software redundancy assuming that the events of coincidental software failures are rare.

72.5.1 The Recovery Block Scheme

The recovery block scheme, proposed by Randell [49], consists of three elements: primary module, acceptance tests, and alternate modules for a given task. The simplest scheme of the recovery block is as follows:

Ensure T
By P
Else by Q_1
Else by Q_2
.
.
.
Else by Q_{n-1}
Else Error

where T is an acceptance test condition that is expected to be met by successful execution of either the primary module P or the alternate modules $Q_1, Q_2, \ldots, Q_{n-1}$. The process begins when the output of the primary module is tested for acceptability. If the acceptance test determines that the output of the primary module is not acceptable, it recovers or rolls back the state of the system before the primary module is executed. It allows the second module Q_1, to execute. The acceptance test is repeated to check the successful execution of module Q_1. If it fails, then module Q_2 is executed, *etc*. The alternate modules are identified by the keywords "else by" When all alternate modules are exhausted, the recovery block itself is considered to have failed, and the final keywords "else error" declares the fact. In other words, when all modules execute and none produce acceptable outputs, then the system falls.

In a recovery block, a programming function is realized by n alternative programs, $P_1, P_2 \ldots, P_n$. The computational result generated by each alternative program is checked by an acceptance test, T. If the result is rejected, another alternative program is then executed. The program will be repeated until an acceptable result is generated by one of the n alternatives or until all the alternative programs fail. The probability of failure of the RB scheme, P_{rb}, is as follows [48]:

$$P_{rb} = \prod_{i=1}^{n}\left(e_i + t_{2i}\right) + \sum_{i=1}^{n} t_{1i}\ \mathrm{e_i}\left(\prod_{j=1}^{i-1}\left(e_j + t_{2j}\right)\right),$$

where

e_i = probability of failure for version P_i

t_{1i} = probability that acceptance test i judges an incorrect result as correct

t_{2i} = probability that acceptance test i judges a correct result as incorrect.

72.5.2 *N*-version Programming

The NVP was proposed by [6] for providing fault-tolerance in software. In concept, the NVP scheme is similar to the *N*-modular redundancy scheme used to provide tolerance against hardware faults [20]. The NVP is defined as the independent generation of $N \geq 2$ functionally equivalent programs, called *versions,* from the same initial specification.

Consider an NVP scheme consists of n programs and a voting mechanism, V. As opposed to the RB approach, all n alternative programs are usually executed simultaneously and their results are sent to a decision mechanism which selects the final result. The decision mechanism is normally a voter when there are more than two versions (or,

more than *k* versions, in general), and it is a comparator when there are only two versions *(k* versions). The syntactic structure of NVP is as follows:

seq
par
P_1 (version 1)
P_2 (version 2)
.
.
.
P_n (version n)
decision V

Assume that a correct result is expected where there are at least two correct results. The probability of failure of the NVP scheme, P_n, can be expressed as

$$P_{nv} = \prod_{i=1}^{n} e_i + \prod_{i=1}^{n} (1-e_i) e_i^{-1} \prod_{j=1}^{n} e_j + d \,.$$

The main difference between the recovery block scheme and the *N*-version programming is that the modules are executed sequentially in the former. The recovery block generally is not applicable to critical systems where real-time response is of great concern.

Another scheme that adopts intermediate voting is the *N*-program, self-checking scheme [59] where each version is subject to an acceptance test or checking by comparison. When $N = 2$, it is a two-version, self-checking scheme or self-checking duplex scheme. Whenever a particular version raises an exception, the correct result is obtained from the remaining versions and execution is continued. This method is similar to the CER approach, with the only difference being the on-line detection in the former by an acceptance test rather than a comparison.

72.6 Cost Modeling

It is important to determine when to stop testing based on the reliability and cost assessment. Several software cost models and optimal release policies have been studied in the past two decades. [28] discussed a simple cost model addressing linear developing cost during testing and operational period. [27] also discussed the optimum software-release time problem with a fault-detection phenomenon during operation. [22] discussed optimal software release time with consideration of a given cost budget. [8]studied the stop-testing problem for large software systems with changing code using graphical methods. They reported the details of a real time trial of a large software system that had a substantial amount of code added during testing. [36]developed a cost model with an imperfect debugging and random life cycle as well as a penalty cost to determine the optimal release policies for a software system. [39] developed the expected total net gain in reliability of the software development process, as the economical net gain in software reliability that exceeds the expected total cost of the software development, that uses to determine the optimal software release time which maximizes the expected total gain of the software system. [41] presented a generalized cost model addressing the fault removal cost, warranty cost and software risk cost due to software failures for the first time. Such model is given by:

$$E(T) = C_0 + C_1 T^{\alpha} + C_2 m(T)\mu_y + C_3 \mu_w [m(T+T_w) - m(T)] + C_R [1 - R(x/T)]$$

where

C_0	set-up cost for software testing
C_1	software test cost *per* unit time
C_2	cost of removing each fault *per* unit time during testing
C_3	cost to remove an fault detected during warranty period
CR	loss due to software failure
E(T)	expected total cost of a software system at time T
μ_y	expected time to remove a fault during the testing period
μ_w	expected time to remove a fault during the warranty period.

The detailed results to obtain the optimal software release time that minimizes the expected total cost can be obtained in [41].

72.6.1 The Gain Model with Random Field Environments

[53] recently developed a software gain model under random field environment [47] with consideration of not only time to remove faults during in-house testing, cost of removing faults

during beta testing, risk cost due to software failure, but also the benefits from reliable executions of the software during both beta testing and field operation. This model addresses both beta testing and operation phases in the software systems. During beta testing, not only can software faults still be removed from the software after failures occur, but they are also likely to be conducted in an environment that is the same as (or close to) the end-user environment. Note that the previous model in this section considers both the warranty cost and the penalty cost after releasing the software, which are overlapped with each other. The model in [53] is indeed slightly different, it does not consider a warranty cost, but instead considers a similar concept — the cost associated with the beta testing that is conducted in the field environment. The beta testing cost and the penalty cost after the software is released are not overlapped with each other. Details can be obtained in [54].

72.6.2 Other Cost Models

[43] presented a software cost model based on the quasi renewal processes. If the inter-arrival time represents the error-free time (time between errors), a quasi renewal process can be used to model reliability growth for software. For example, suppose that all faults of the software have the same chance of being detected. If the inter-arrival times of a quasi renewal process represent the error-free times of the software, the expected cumulative number of software faults in [0, t] can be described by the renewal function $M(t)$ with parameter $\alpha > 1$. Let $\overline{M}(t)$ be the number of remaining software faults at time t. It follows that $\overline{M}(t) = M(\tau) - M(t)$, where $M(\tau)$ is the number of faults which can be detected through a long testing time τ, relative to t.

Additional Notation

c_1	The cost of fixing a fault during testing phase
c_2	The cost of fixing a fault during operation phase
c_3	The cost of testing *per* unit time
T	The software release time
T_d	The scheduled delivery time
$g(t)$	The probability density function of the life-cycle length ($t > 0$)

Table 72.6. Summary of references

Group models	References
Software reliability and testing models	Hossain(1993); Hwang (2006); Jelinski (1972); Musa (1987); Pham (1993, 1997b, 2003, 2003 (a–b), 2006); Teng (2006); Yamada (1983); Zhang (2000)
Cost models	Kapur (1992); Pham (1999c, 2006); Zhang (1998, 1998a, 2002, 2003)
General fault tolerant systems	Anderson (1980, 1985); Arlat (1990); Iyer (1985); Kanoun (1993); Kim (1989); Laprie (1990); Leveson (1990); Pham. (1989, 1991b, 1992); Scott (1987).
N-version programming	Anderson (1980, 1985); Avizienis (1977, 1988); Chen (1978); Knight (1986); Pham (1994, 1995, 2006); Teng (2002)
Recovery block	Laprie (1990); Pham (1989); Randell (1975)
Other fault tolerant techniques	Eckhardt (1985); Hua (1986); Kim (1989); Pham (1991b, 1992); Tai (1993); Teng (2003)

$c_p(t)$ A penalty cost for a delay of delivering software

M(t) Number of faults which can be detected through a period of testing time t.

The expected total software life-cycle cost can be defined as follows:

$$C(T) = c_3 T + c_1 M(T) + \int_T^\infty c_2 [M(t) - M(T)] g(t) dt + I(T - T_d) c_p (T - T_d)$$

where $I(t)$ is an indicator function, that is,

$$I(t) = \begin{cases} 1 & \text{if } t \geq 0 \\ 0 & \text{otherwise} \end{cases}$$

$M(t)$ and Var[$N(t)$] contain some unknown parameters. Those unknown parameters can be obtained by using the method of MLE or least squares methods. Detailed optimal release policies and findings can be found in [43].

The benefits of using the above cost models are that they provide: (1) assurance that the software has achieved safety goals, and (2) a means of rationalizing when to stop testing the software. Further research is worth to look at what the risk cost due to the software failures after release with a specified reliability level is. And how should marketing efforts – including advertising, public relations, trade-show participation, direct mail, and related initiatives – be allocated to support the release of a new software product effectively?

A brief, but not exhaustive, list of references on software reliability models, cost models and fault-tolerant systems discussed in this chapter is given in Table 72.6 for a quick reference to readers.

References

[1] Anderson T, Lee P. Fault tolerance: Principles and practices. Prentice-Hall, Englewood Cliffs, NJ, 1980.

[2] Anderson T, Barrett P, Halliwell D, Moulding M. Software fault tolerance: An evaluation. IEEE Transactions on Software Engineering 1985; SE-11(12).

[3] Arlat J, Kanoun K, Laprie J. Dependability modeling and evaluation of software fault tolerant systems. IEEE Transactions on Computers 1990; 39(4).

[4] Avizienis A, Chen L. On the implementation of *N*-version programming for software fault-tolerance during program execution. Proceedings of IEEE COMPASAC 1977; 77:149–155.

[5] Avizienis A, Lyu M, Schutz W. In search of effective diversity: A six language study of fault tolerant flight control software. Proc. of 18th International Symposium on Fault Tolerant Computing, Tokyo, Japan 1988.

[6] Chen L, Avizienis A. *N*-version programming: A fault tolerance approach to the reliable software. Proceedings of 8th International Symposium Fault-Tolerant Computing, IEEE Computer Society Press 1978.

[7] Cox DR. Regression models and life tables (with discussion). Journal of the Royal Statistical Society, Series B 1972; 34:187–220.

[8] Dalal SR, Mallows CL. Some graphical aids for deciding when to stop testing software. IEEE Journal on Selected Areas in Communication 1992; 8(2):169–175.

[9] Eckhardt DE, Lee LD. A theoretical basis for the analysis of multiversion software subject to coincident errors. IEEE Transactions on Software Engineering 1985; SE-11(12).

[10] Friedman MA, Voas JM. Software assessment – Reliability, safety, testability. Wiley, New York, 1995.

[11] Goel AL..Okumoto K. Time-dependent error-detection rate model for software and other performance measures. IEEE Transactions on Reliability, 1979; 28:206–211.

[12] Hossain SA, Ram CD. Estimating the parameters of a non-homogeneous Poisson process model for software reliability. IEEE Transactions on Reliability 1993; 42(4):604–612.

[13] Hua KA, Abraham JA. Design of systems with concurrent error detection using software redundancy. Joint Fault Tolerant Computer Conference, IEEE Computer Society Press 1986.

[14] Hwang S, Pham H. A systematic-testing methodology for software systems. International Journal of Performability Engineering 2006; 2(3):205–221.

[15] Jelinski Z, Moranda PB. Software reliability research. In: Freiberger Evaluation W, editor. Statistical computer performance. Academic Press, New York, 1972.

[16] Kanoun K, Mohamed K, Beounes C, Laprie J-C, Arlat J. Reliability growth of fault-tolerant Software. IEEE Transactions on Reliability 1993; Jun., 42(2):205–218.

[17] Kapur PK, Bhalla VK. Optimal release policies for a flexible software reliability growth model.

Reliability Engineering and System Safety 1992; 35:45–54.

[18] Kim KH, Welch HO. Distributed execution of recover blocks: An approach for uniform treatment of hardware and software faults in real time applications. IEEE Transactions on Computers 1989; May, 38(5).

[19] Knight JC, Leveson NG. An experimental evaluation of the assumption of independence in multiversion programming. IEEE Transactions on Software Engineering 1986; 12(1).

[20] Lala RK Fault tolerant and fault testable hardware design, Prentice-Hall, London, 1985.

[21] Laprie JC, Arlat J, Beounes C, Kanoun K. Definition and analysis of hardware- and software-fault tolerant architectures. IEEE Computers, 1990; July, 23(7).

[22] Leung YW. Optimal software release time with a given cost budget. Journal of Systems and Software 1992; 17:233–242.

[23] Leveson NG, Cha SS, Knight JC, Shimeall TJ. The use of self-checks and voting in software error detection: An empirical study. IEEE Transactions on Software Engineering 1990; 16(4).

[24] Lyu MR. Handbook of software reliability engineering. McGraw-Hill, New York, 1996.

[25] Musa JD, lannino A, Okumoto K. Software reliability: Measurement, prediction, and application. McGraw-Hill, NewYork, 1987.

[26] Ohba M. Software reliability analysis models. IBM Journal of Research Development 1984; 28:428–443.

[27] Ohtera H, Yamada S. Optimal allocation and control problems for software-testing resources. IEEE Transactions on Reliability. 1990; 39:171–176.

[28] Okumoto K. Goel AL. Optimum release time for software systems based on reliability and cost criteria. J. Systems and Software 1980; 1:315–318.

[29] Pham H, Upadhyaya SJ. Reliability analysis of a class of fault tolerant systems. IEEE Transactions on Reliability 1989; 38(3):333–337.

[30] Pham H, Pham M. Software reliability models for critical applications. Idaho National Engineering Laboratory, EG&G2663, 1991; December.

[31] Pham H, Upadhyaya SJ. Optimal design of fault tolerant distributed systems based on a recursive algorithm. IEEE Transactions on Reliability 1991; 40(3):375–379.

[32] Pham H. Fault-tolerant software systems: Techniques and applications. IEEE Computer Society Press, 1992.

[33] Pham H. Software reliability assessment: imperfect debugging and multiple failure types in software development.EG&G-RAAM-10737; Idaho National Laboratory, 1993.

[34] Pham H. On the optimal design of N-version software systems subject to constraints. Journal of Systems and Software 1994; 27(1):55–61.

[35] Pham H. Software Reliability and Testing. IEEE Computer Society Press, 1995.

[36] Pham H. A software cost model with imperfect debugging, random life cycle and penalty cost. International Journal of Systems Science 1996; 27(5):455–463.

[37] Pham H, Zhang X. An NHPP software reliability model and its comparison. International Journal of Reliability, Quality and Safety Engineering 1997; 4(3):269–282.

[38] Pham H, Normann L A generalized NHPP software reliability model. Proceedings .Third ISSAT International Conf. on Reliability and Quality in Design, August, ISSAT Press, Anaheim, 1997.

[39] Pham H, Zhang X. Software release policies with gain in reliability justifying the cost. Annals of Software Engineering 1999; 8:147–166.

[40] Pham H, Nordmann L, Zhang X. A general imperfect software debugging model with s-shaped fault detection rate. IEEE Transactions on Reliability. 1999; 48(2):169–175.

[41] Pham H, Zhang X. A software cost model with warranty and risk costs. IEEE Transactions on Computers 1999; 48(1):71–75.

[42] Pham H. Software reliability. Springer, Berlin, 2000.

[43] Pham H, Wang H. A quasi renewal Process for software reliability and testing costs. IEEE Transactions on Systems, Man, and Cybernetics – Part A 2001; 31(6):623–631.

[44] Pham H. Handbook of reliability engineering. Springer, Berlin, 2003.

[45] Pham H, Deng C. Predictive-ratio risk criterion for selecting software reliability models. Proc. Ninth International Conference on Reliability and Quality in Design. August 6–8, 2003; Hawaii, U.S.A.; ISBN: 0-9639998-8-5.

[46] Pham H. Software reliability and cost models: perspectives, comparison and practice. European Journal of Operational Research 2003; 149: 475–489

[47] Pham H. A new generalized systemability model. International Journal of Performability Engineering 2005; 1(2):145–155.

[48] Pham H. System software reliability. Springer, Berlin, 2006.

[49] Randell B. System structure for software fault tolerance. IEEE Transactions on Software Engineering 1975; SE-1(2):220–232.

[50] Tai AT, Meyer JF, Aviziems A. Performability enhancement of fault-tolerant software. IEEE Transactions on Reliability 1993; 42(2):227–237.
[51] Teng X, Pham H. A software reliability growth model for *N*-version programming systems. IEEE Transactions on Reliability 2002; 51(3):311–321.
[52] Teng X, Pham H. Software fault tolerance. In: Pham Hoang, editor. The Handbook of reliability engineering. Springer, Berlin, 2003:585–611.
[53] Teng X Pham H. Software cost model for quantifying the gain with considerations of random field environments. IEEE Transactions on Computers. March 2004; 53(3):380–384.
[54] Teng X, Pham H. A new methodology for predicting software reliability in the random field environments. IEEE Transactions on Reliability. Oct. 2006; 55(3): 458-468.
[55] Tohma Y, Yamano H, Ohba M, Jacoby R. The estimation of parameters of the hypergeometric distribution and its application to the software reliability growth model. IEEE Transactions on Software Engineering 1991; SE-17(5).
[56] Yamada S, Ohba M, Osaki S. S-shaped reliability growth modeling for software error detection. IEEE Transactions on Reliability 1983; 12:475–484.
[57] Yamada S, Osaki S. Software reliability growth modeling: models and applications. IEEE Transactions on Software Engineering 1985; 11:1431–1437.
[58] Yamada S, Tokuno K, Osaki S. Imperfect debugging models with fault introduction rate for software reliability assessment. International Journal of Systems Science 1992; 23(12).
[59] Yau SS, Cheung RC. Design of self-checking software, in Reliable Software. IEEE Press, 1975; April.
[60] Zhang X, Pham H. A software cost model with warranty cost, error removal times and risk costs. IIE Transactions on Quality and Reliability Engineering 1998; 30(12):1135–1142.
[61] Zhang X, Pham H. A software cost model with error removal times and risk costs. International Journal of Systems Science 1998; 29(4): 435–442.
[62] Zhang X. Software reliability and cost models with environmental factors. Ph.D. thesis, Rutgers University, New Jersey, 1999.
[63] Zhang X, Pham H. Comparisons of nonhomogeneous Poisson process software reliability models and its applications. International Journal of Systems Science 2000; 31(9):1115–1123.
[64] Zhang X, Jeske DR, Pham H. Calibrating software reliability models when the test environment does not match the user environment. Applied Stochastic Models in Business and Industry 2002; 18:87–99.
[65] Zhang X, Teng X, Pham H. Considering fault removal efficiency in software reliability assessment. IEEE Trans. on Systems, Man, and Cybernetics – Part A 2003; 33(1):114–120.

73

Application of the Lognormal Distribution to Software Reliability Engineering

Swapna S. Gokhale[1] and Robert E. Mullen[2]

[1]University of Connecticut, Storrs, CT, 06269, USA
[2]New England Development Centre, Cisco Systems, Inc., Boxborough, MA, 01719, USA

Abstract: The theoretical foundations underlying the lognormal distribution suggest that it can be applied to important problems in software reliability engineering. Further, an overwhelming amount of evidence has emerged to confirm the lognormal hypothesis. In this chapter we provide an overview of the lognormal distribution and its transformations. We then summarize the previous evidence, place the most recent evidence in context, discuss the set of issues to which it has been successfully applied, and call attention to the unified perspective the lognormal affords. Finally, we outline potential applications of the lognormal and suggest enabling research.

73.1 Introduction

Reliable operation is required of many engineering systems which offer essential services. As software systems continue to assume increasing responsibility for providing these critical services, they will also be expected to meet such stringent reliability expectations.

In most engineering domains, a systematic, quantitative system reliability analysis is often based on mathematical models of a system. For most systems, these mathematical models are derived from a few underlying physical processes. Similar to other engineering disciplines, software reliability analysis is based on stochastic models, commonly known as software reliability growth models [1] [2]. A striking difference between software reliability engineering and other engineering disciplines, however, is that the mathematical models used in other disciplines are grounded in the physical and observable structures, properties, and behavior of the systems, whereas most of the software reliability models do not connect mathematics to observable constructs.

In this chapter we demonstrate that several observable properties of software systems are in fact related, being grounded in the conditional nature of software execution. This leads to the emergence of a lognormal distribution of rates of events in software systems. These include failure rates of defects and execution rates of code elements. We discuss how the lognormal growth model can be obtained from the distribution of the first occurrence times of defects and apply it to reliability growth. The application of the lognormal growth model to describe code coverage growth as a function of testing is also described. We extend

the lognormal further and describe the derivation and application of the discrete lognormal model for the distribution of occurrence counts of defects. The chapter concludes by identifying opportunities for further research and wider application of the lognormal.

73.2 Overview of the Lognormal

The lognormal distribution is well known in many fields including ecology, economics, and risk analysis [3]. It is used in hardware reliability, though less than the Weibull [4]. It arises in a natural way when the variant's value is determined by the multiplicative effect of many random factors, just as the normal distribution arises as a consequence of the additive effect of many random factors. Johnson, Kotz and Balakrishnan [5] provide an introduction to the lognormal distribution and the ways it can be generated.

Theorems about the conditions under which products of random variables asymptotically approach a lognormal distribution are restatements of theorems about the conditions under which sums of random variables asymptotically approach a normal distribution. Products are treated as exponentiations of sums of logarithms. If the logarithms of the factors meet the conditions that make the distribution of their sum normal, then the product of the random variables by definition follows a lognormal distribution. Two forms of the central limit theorem (CLT) are presented in Aitchison and Brown's monograph [6] on the lognormal. Each states conditions under which a product of random variables $\prod_{j=1}^{n} X_j$ is asymptotically lognormal as L($n\cdot\mu$, $n\cdot\sigma^2$). The Lindeberg–Levy form of the CLT requires that all the X_j be from the same distribution, but the Lyapunov form removes that condition and adds a condition on the expectation of the third moment of the X_j. Petrov [7] provides additional theorems in which the variables are not necessarily identically distributed. Loeve [8] establishes alternatives to the assumption of independence. Patel and Read [9] outline additional extensions. Feller [10] shows the number of factors, n, need not be constant but can be an independent Poisson variable. This is important because software conditionals may be nested at many different levels. Figure 73.1 illustrates that in a tree which is created by 10,000 branchings of randomly selected leaf nodes, the number of leaves at each level approaches a Poisson distribution.

To summarize, the key assumptions which lead to the lognormal distribution are the multiplicative effect of many relatively independent random factors, with no one factor effectively dominating the others and each being from the same distribution or having uniformly small moments.

73.3 Why Are Software Event Rates Lognormal?

In this section we illustrate the wide variety of ways analysts routinely and successfully model software by making the same assumptions that lead to a lognormal distribution. At the typical level of detail to which analysts analyze software systems we find event rates being determined by multiplicative processes, and that the factors are sufficiently numerous and independent that their product approaches the lognormal. Furthermore, we suggest that refining the following analyses to a greater level of detail would merely increase the number of factors. In real systems the number of factors is not infinite but so large as to make the lognormal distribution an adequate approximation.

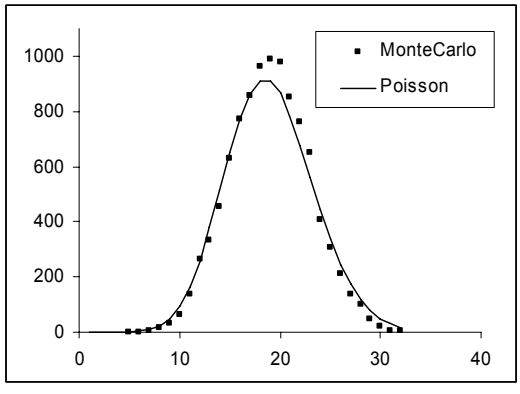


Figure 73.1. Example of a Poisson distribution of leaf depths

The assumption of independence is the most questionable, yet we find that assumption being used successfully in the following examples. It may not be fully satisfying that there are forms of the central limit theorem that do not require independence since those theorems make other even less familiar assumptions. Intuitively, if the variance of the problematic factors is overwhelmed by the total variance, any deviation from the lognormal will be difficult to detect.

73.3.1 Graphical Operational Profile

Operational profiles of customer usage [11] [12] were approved as a best current practice at AT&T. In the *graphical* or *implicit* operational profile method an event is characterized by a path through a network of operational possibilities. Specifying a set of "key input variables" is equivalent to specifying a path through the network. This method assumes that the occurrence probabilities of the key input variables are independent of each other (at least approximately so) [12]. Occurrence probabilities for each path are computed by multiplying the probabilities of those levels of key input variables corresponding to the path.

Using a call tree example, both papers [11] [12] show clearly how the network of conditioned probabilities is constructed. Figure 73.2 presents a partial depiction of a user event tree. There is a .35 chance of a call being an internal incoming call; conditioned on that, there is a .30 chance it is generated by standard dialing, and a .70 chance it is generated by abbreviated dialing; conditioned on it being generated by abbreviated dialing, there is a .10 chance of busy-no-answer, a .30 chance of ring-no-answer, and a .60 chance of being answered; conditioned on the call being answered, there is a .80 chance of talking, a .10 chance of being put on hold, and a .10 chance of it being a conference call. Thus the probability of the event "internal incoming call generated by abbreviated dialing being answered and put on hold" is given by .35 * .70 * .60 * .10 = .0147, the product of the conditional probabilities. The probabilities must be conditioned because the chance of a phone being answered differs (in the example) between the cases of internal and external calls. At each division or refinement into sub-cases, paths branch and a probability is assigned to each new path. However, the total probability over all paths remains one.

Such a process of dividing a whole into parts by repeated division is called a breakage process. The mathematical foundation of breakage processes has been studied, and Kolmogorov [6] [13] is credited with explaining why the distribution of sizes of particles resulting from rock crushing is lognormal. For software events, such as operations in an operational profile, it is not rock mass which is being split but probability.

73.3.2 Multidimensional Operational Profiles

Another way to construct an operational profile is to model the input domain of a program as having one dimension *per* input variable. Cukic and Bastani [14] use this technique to estimate how the distribution of the values of input variables affects the spread of frequencies of events in the operational profile. They studied how reducing the dimensionality of the profile reduces testing effort. They assigned values taken by the input variables to 10 bins and assumed the relative frequencies of each bin in the operational profile followed the normal distribution. For example for three dimensions there are 1000 cells, each one holding the product of three factors, namely the values of the normal distribution at that coordinate in each dimension. They assumed the three normal distributions were independent.

This process also leads to a lognormal distribution of event rates. In particular, the product of

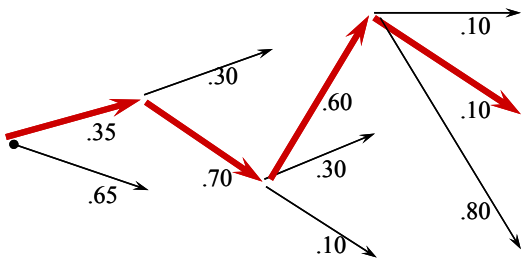


Figure 73.2. Example of a graphical operational profile or user event tree

variables from a distribution with central tendencies, such as the normal, quickly approaches the lognormal. Note that if we randomly zero some of the cells (to represent events that are somehow known to be impossible) and renormalize the operational profile, what remains are samples from a lognormal distribution. Similarly if we randomly tag some of the cells as faults and study their rates we will also find samples from a lognormal distribution.

73.3.3 Program Control Flow

A program can be viewed as a set of code blocks. A *basic block* is defined as a sequence of instructions in which only the first is a branch target and only the last is a branch or function call [15]. When a program is executed, the probability of execution flowing to a given block in the code is the product of the probabilities of the conditions needed to be met on the execution path leading to that block. There are a large number of conditional statements guarding the execution of typical code blocks, therefore a large number of factors will be multiplied to determine the probability. The central limit theorem tells us that under very general conditions the distribution of the products of those factors is asymptotically lognormal. Thus, the branching nature of software programs tends to generate a lognormal distribution of block execution rates. Similar reasoning indicates that the execution rates of other data flow elements such as decisions are lognormal [16].

Bishop and Bloomfield [17] provide a more detailed and sophisticated model of these processes. In their simplest example they modeled program structure as a branching binary tree of uniform depth and assumed branch probabilities to be uniformly distributed over (0:1). Even this simple model approached a lognormal distribution. Further, the parameters measured in real programs of known size were quantitatively consistent with relationships they derived from the simple model. The authors provide further reasons and evidence that the distribution remains lognormal even in the presence of loops and other variations in program structure.

73.3.4 Sequences of Operations

The sequences of operations or events within a system during operation are often captured in logs and traces. Examples of such event logs include packet traces flowing over a network, kernel events generated by an operating system or user-level events triggered by application software. A careful analysis and an adequate representation of such event chains is necessary to capture long term patterns of typical behavior, which can then be used to uncover unusual, perhaps intrusive, activities. For example, Ye, Zhang and Borer [18] represent the sequence of events using a Markov chain and compute the probability of a specific sequence occurring in ordinary operation as a product of the probability of the initial state in the sequence and the subsequent transition probabilities. The probability of each event sequence that occurs is compared to a threshold for intrusion detection. This threshold must be carefully set in order to achieve the desired balance between detection and false alarms.

These researchers recognized that because long sequences of events are considered, the sum of the logarithms of the probabilities follows the normal distribution, and used this fact to set control limits for anomaly detection. This example indicates that system behavior, as observed from multiple levels (network, operating system, end user/application), approaches the lognormal and that that fact can be used to inform and optimize engineering decisions.

73.3.5 Queuing Network Models

Complex systems have many queues for serializing access to IO devices, processors, locks, servers, *etc.* Queuing network models are considered sufficiently accurate descriptions of system behavior to be widely used. Many of them have product form solutions, in which the queue lengths are independent [19]. Suppose there are n queues and that we represent the state of the system as a vector where the ith component is <*zero*> if the queue is empty, and <*one*> otherwise. The defined states are interesting since some defects (*e.g.*, timing races) are conditioned on waiting by one process, other defects (*e.g.*, deadlocks) are

conditioned on two or more resources having processes waiting. Because the queue lengths are independent, the probability of the state corresponding to a given vector is the product of the probabilities of each queue being in the state defined by the given vector. As *n* becomes large, the distribution of probabilities of the states in *n*-space becomes lognormal.

73.3.6 System State Vectors

Avritzer and Larson [20] describe a telecommunications application in which up to 24 calls of five types are handled in parallel. They represented the system state as a vector of the number of calls of each type being handled. The probabilities of the state vectors were computed under the assumption of a product form solution, and the most probable states were tested. The utility of the assumptions and analysis was confirmed by the positive effect on product quality.

They implicitly assumed independence when they used Kleinrock's independence approximation [21]. Another underlying assumption was that faults are a subset of events, and that the most probable faults are a subset of the most probable events. This represents a solid example of how multiplying rates of constituent events, drawn from their own distributions, generates the distribution of rates of complex events.

In this instance the number of types of calls (five) is too small for the distribution of rates of the defined states to be lognormal. It would be expected that if the dimensionality of the state space were increased, either by having more types of calls or by admitting other state variables, the lognormal distribution would become an increasingly good approximation.

73.3.7 Fault Detection Process

Detection of a fault is not always immediate. Often a fault is not detected until the occurrence of another event that depends on an output or side effect of the fault [22]. The actual detection of the fault, therefore, depends not only on the chain of conditionals resulting in the fault, but also on a second chain involving detection of the fault. This has the effect of making the observable failure rate of faults depend on the multiplication of additional factors, and therefore approach the lognormal distribution more surely.

In summary, the perspectives offered here include queuing network models, operational profiles, and conditionals embedded in software. These exemplify the perspectives of internal state space, input space, and the path of computation, respectively. The specific examples illuminate the mechanism by which important white-box views of software operations, when taken to the limit, all approach the same black box model, one sufficiently described by the lognormal distribution and its parameters.

73.4 Lognormal Hypotheses

In Section 73.3 we discussed ways in which lognormal distributions of event rates arise. For reliability engineering we are particularly interested in faults. Faults are merely a subset of events, therefore faults have failure rates that are a sample from the rates of all events. If event rates are lognormal, then failure rates of faults are also lognormal. In this section we present a mathematical formulation of the lognormal hypotheses in software.

73.4.1 Failure Rate Model

Each defect (or fault) in a given system, against its overall operational profile, has a characteristic failure rate λ. To say that the distribution of failure rates of software faults is lognormal is to say that the logarithms of the failure rates $\ln(\lambda)$, follow the Gaussian or normal probability distribution function (pdf). For $(\lambda > 0)$:

$$dL(\lambda) = \frac{1}{\lambda\sigma\sqrt{2\pi}} e^{-\left(\ln(\lambda)-\mu\right)^2/2\sigma^2} d\lambda . \quad (73.1)$$

For the lognormal, the mean, median, and mode of the log-rate are identical and equal to μ. The variance of the log-rate is σ^2. The mean rate is exp $(\mu+\sigma^2/2)$, the median rate is exp (μ), and the mode is exp $(\mu-\sigma^2)$.

73.4.2 Growth Model

We now derive the lognormal growth model based on the failure rate model in 0. Let N denote the number of faults. The probability a single fault of failure rate λ is not encountered (does not result in a failure) until time t or later is exp $(-\lambda t)$.

The probability that fault was encountered for the first time before time t is $1 - \exp(-\lambda t)$. The mean contribution of that fault to the fault discovery rate of the system at time t is $\lambda\exp(-\lambda t)$. If λ is distributed as $L(\lambda|\mu, \sigma^2)$ then $M(t)$, the mean number of faults found (that is, having at least one failure) by time t, is given by

$$M(t) = N - N \cdot \int_{\lambda=0}^{\infty} \exp(-\lambda t) dL(\lambda). \quad (73.2)$$

This integral is formally equivalent to the Laplace transform of the lognormal, which is a transformation from a rate distribution to first occurrence time (discovery distribution) [23]. This integral has no simple form. Clearly, $M(0) = 0$, and $M(\infty) = N$. The mean fault discovery rate of the system at time t, $m(t)$, is given by dM/dt or equivalently

$$m(t) = N \cdot \int_{\lambda=0}^{\infty} \lambda \cdot \exp(-\lambda t) dL(\lambda). \quad (73.3)$$

This integral is also intractable. The intractable integrals are computed numerically by changing variables so the integrals are of the standard normal distribution and computing its height at regular intervals. A detailed discussion of this approach can be found in [24].

Note $m(0) = N\exp(\mu+\sigma^2/2)$, *i.e.,* the initial discovery rate is the product of the number of faults and their mean rate.

Unlike hardware, the mean overall failure rate for software systems as a function of time is generally at a maximum when the product is newest, since reliability growth has not yet commenced. The derivative of the Laplace transform of the lognormal, (73.3), meets this boundary condition – the lognormal itself does not. The fact that the lognormal itself is zero at zero impedes its direct use in many software engineering applications.

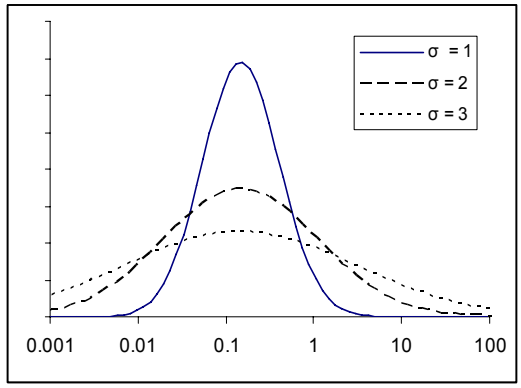


Figure 73.3. Lognormal distribution of rates, $\mu = -2$. Application: failure rates. Code execution, operational profile

73.4.3 Occurrence Count Model

Reliability growth models capture the first occurrence times of defects, usually during testing. Despite extensive testing, however, inevitably software systems are released into the field with latent defects. A shipped latent defect may cause multiple field failures until it is fixed. Modeling the defect occurrence phenomenon in the field can help answer questions that may be valuable in planning maintenance activities, for example, what percentage of defects will cause two or more field failures? The lognormal occurrence count model represents this phenomenon.

We assume each defect has a rate λ against the overall operational profile and that each specific failure, *i.e.*, each manifestation of that defect, is an event in a Poisson process with that rate. We also assume the defect is not repaired (or the repairs are not put in service) during the interval considered. Since the rates follow the lognormal, the overall occurrence count distribution is a mixture of Poisson distributions, which can be represented using the notation of [25].

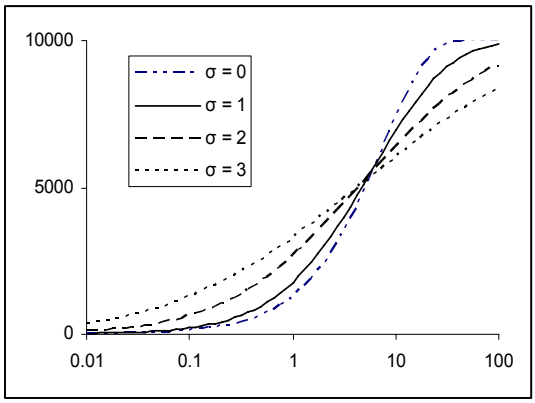


Figure 73.4. Cumulative first occurrences, x-axis: years. Laplace transform of lognormal for μ = –2, N=10000. Application: software reliability growth model

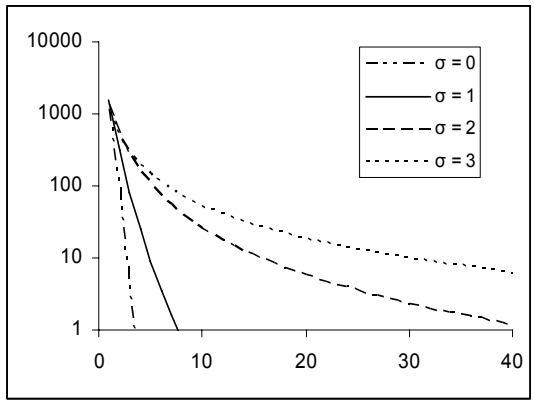


Figure 73.5. N defects having x (1:40) occurrences. Discrete lognormal for μ = –2, N = 10000, at time T = 1 year. Application: occurrence counts

$$Poisson(\lambda) \bigwedge_{\lambda} Lognormal(\mu, \sigma) \qquad (73.4)$$

This distribution is called a discrete-lognormal or Poisson-lognormal. Defining i to be the number of occurrences, the pdf of occurrences, *DLN(i),* is the integral of Poisson distributions, the rates of which follow a lognormal distribution, each evaluated at i. For ($i >= 0$, integer)

$$DLN(i) = \int_0^{\infty} Poisson(i, \lambda) \bullet dL(\lambda). \qquad (73.5)$$

73.4.4 Interpretation of Parameters

Conceptual advantages of the lognormal include the relative straightforwardness of its parameters and the way it links various observed properties of software defects.We provide a summary of how the parameter values are related to software behavior.

Figures 73.3 to 73.5 show examples of the lognormal and its two transformations. Figure 73.3 illustrates the wide range in rates which are possible for the larger values of σ. Figure 73.4 shows the reliability growth model, based on the Laplace transform from Section 73.4.2. Figure 73.5 shows the corresponding occurrence count distributions, hypothesized to be discrete lognormal, derived in Section 73.4.3.

The parameter σ makes the greatest qualitative difference and allows the lognormal its flexibility. σ, the standard deviation of the log rates, increases with increasing complexity of the software, in particular with greater depth of conditionals [17]. If σ is zero, all defects have the same occurrence rate (not shown in Figure 73.3) leading to the exponential model [26] of software reliability growth (Figure 74.4, $\sigma = 0$). In this case, the distribution of occurrences will be an ordinary Poisson distribution with rate λ = exp(μ) (Figure 73.5, $\sigma = 0$). Values of σ from 1.0 to 3.0 are more common and greater than four are unusual and problematic [27].

The contribution to the initial overall failure rate, integrated over all defects, will be dominated by contributions from the high rate defects. If σ is 2.0, more than 2% have rates more than exp(4) times the median. On the other side of the median are an equal percentage of defects with lower rates by a factor of exp(−4). The ratio of rates between the second percentile and the 98th percentile exceeds exp(8), a factor of nearly 3000. The spread is more dramatic for σ > 3.0. σ determines the ratio of the highest and the lowest occurrence rates of the defects, however defined.

Bishop and Bloomfield [17] observed and explained a rough relationship between program

size and σ: *The depth of conditionals is proportional to the log of the program size, and σ, the spread in rates, is proportional to the square root of that.* Thus a key parameter can be estimated based on information available prior to execution.

The parameter μ has a straightforward interpretation: if rates are plotted on a log scale, as in Figures 73.3 and 73.4, changing μ merely moves the distribution to the right or left with no change in shape. A system speedup or using different units of time changes μ . For $\mu = -2$, the median rate is exp(−2) or **.**14 *per* year (Figure 73.3) and fewer than half have been found by T=1 year (Figure 73.4) for all σ. In terms of occurrence counts, a majority of the 10,000 defects have not occurred even once (Figure 73.5).

Changing either μ or σ, both of which relate to ln(rate), does not affect the other. However, changing either μ or σ affects *both* the mean and variance of the rates themselves [6].

The final parameter is ***N***, the number of defects, which scales the pdf. For Figures 73.3, 73.4, and 73.5, changing *N* changes only the height of the curve, not its shape or position. In this paper, and in most situations, *N* is not a given but must be estimated in conjunction with the other parameters of the model. *N* should be understood physically as the total number of defects, including both found and latent. If the number of latent defects is large, their average rate often is low [28] This does not mean they all will occur in the practical lifetime of the product—most will not—but it is possible to use a software reliability growth model (Figure 73.4) to estimate how many will occur as a function of further exposure.

73.5 Empirical Validation

This section discusses the empirical validation of the lognormal hypotheses in software.

73.5.1 Failure Rate Model

The failure rate model was validated using two published data sets [29]. We briefly discuss validation using the data from nine IBM software products [30] here. These products consisted hundreds of thousands of lines of code and were being used at hundreds of customer sites. For each product, the data consisted of percentages of faults in eight rate classes. The fractional percentages in the highest rate buckets indicated the presence of at least several hundred defects. The means of each class formed a geometric progression. This data arrangement is equivalent to grouping the faults by log of their rates, therefore we expected to see a normal distribution of log-rates.

We used the method of minimizing Chi-square [31] to fit the distribution. It is reasonable [32] to expect a fit to be *relatively* more accurate when there are higher counts, and *absolutely* more accurate when there are lower counts. Because the Chi-square statistic is exactly the product of the relative and absolute errors, it has this desirable property.

Figure 73.6 compares the data with a fitted lognormal. The data, in log-buckets, look like a truncated Normal distribution. The fitted lognormal suggests that for every 100 faults assigned to the 8 highest rate buckets, there may be 85 more faults in lower rate buckets which were not measured. It was estimated that 55 of those faults are in the next two rate buckets.

It is impossible to perform a test of statistical significance on the resulting values of the Chi-square statistic without knowing the number of faults in each bucket. An alternative is to compute the coefficient of determination, which indicates what fraction of the variance (between buckets) is explained by the model. For the example set, the coefficient of determination was 0.99, indicating that the lognormal model explains over 99% of the variance between buckets. Similar coefficients of determination were obtained for the remaining products as well. This suggests that each product is fit very well by the lognormal, providing a better fit than Trachtenberg [33] achieved with a power-law model.

The second set used for validation consisted of data collected from replicated experiments on 12 programs reported in Nagel *et al.* [34] [35]. The programs were executed tens of thousands of times against an operational profile in order to accurately determine the frequency at which each fault occurred. Pooled *z*-scores of those rates (Figure 73.7) visually suggest overall normality, but are

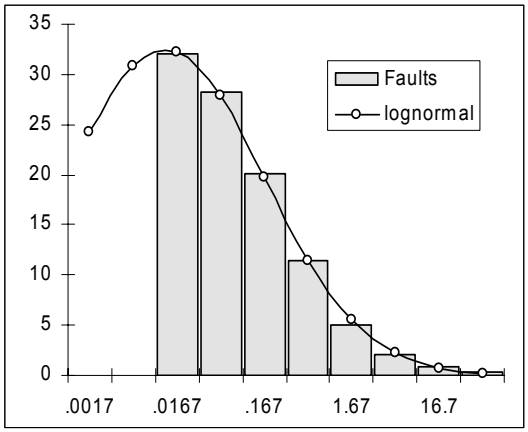


Figure 73.6. Adams [32] product 2.6: relative number of defects *per* rate bucket

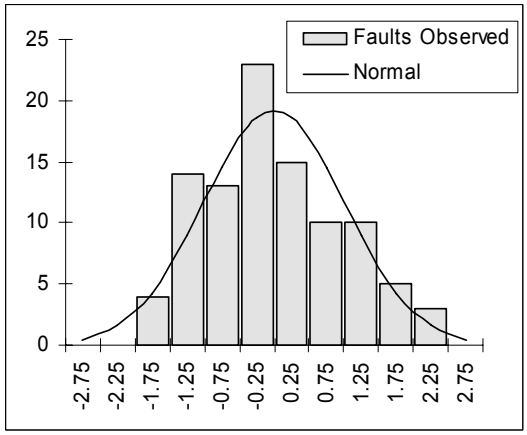


Figure 73.7. Nagel data: pooled *z*-scores of faults *per* log-rate bucket in repetitive run experiments

not conclusive. The Shapiro–Wilk [36] [37] test for normality of small samples found the distribution of rates of faults in each program were plausibly generated from a lognormal. Finally, a comparison of the lognormal distribution with the gamma family of models [23], using the same data, demonstrated that the lognormal was significantly more likely to generate the data than any of the models in gamma family, which consists of some of the well-known, commonly used software reliability models including power law models [33], Musa–Okumoto [26], Littlewood's Pareto model [23], Jelinski–Moranda [38], and Goel–Okumoto [39]. Moreover, the lognormal was more likely to generate the data than a strategy of selecting the best fitting of the gamma models in each case.

Rigorous studies of the failure rate distribution of faults such as those by Adams or Nagel *et al*., are rare. A recent detailed study by Bishop and Bloomfield [17] measured the failure rates of faults in the 10,000 line PREPRO application of the European Space Agency, as well as the distribution of execution rates of code blocks. They found both to be lognormal and elaborated many additional insights into how the parameters of the lognormal will be affected by code size, depth of conditionals, and the presence of loops.

Previously, several researchers hinted at the multiplicative origin of failure rates of rare events, but stopped short of formally modeling these rates using the lognormal. For example, Iyer and Rossetti [40] note that during periods of stress or uncommon workload patterns, rarely used code can be executed, leading to the discovery of errors, and they remark throughout on problems caused by complex sets of events, complex sets of interactions, or complex workloads. Similarly, Adams [30], in his classic paper on preventative maintenance, states that in production code the typical design error requires very unusual circumstances to manifest itself, possibly in many cases the coincidence of very unusual circumstances. Their crucial insight is that the failure rate of a fault is proportional to the product of the probabilities of its preconditions. Although they stated it in terms of rare events, in this chapter we have discussed why the multiplicative insight is applicable to common events as well.

A few efforts have also focused on estimating and modeling the distribution of failure or event rates using various approaches to achieve specific purposes. Musa [12] and Juhlin [11] estimated rates to model the operational profile. Avritzer and Larson [20] determined the distribution of occurrence rates of internal states to increase the effectiveness of testing. Although these efforts, already noted in Section 73.2, share many of the assumptions that lead to the lognormal, these authors did not explicitly study the form of the

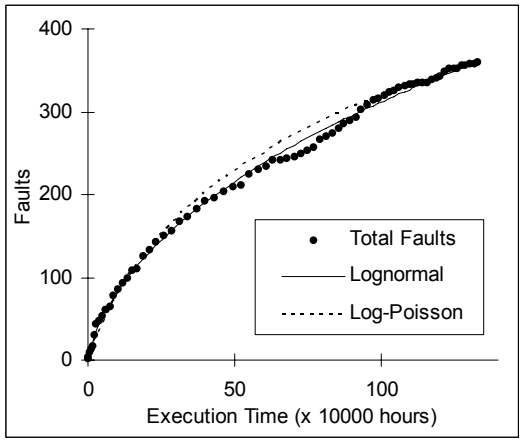


Figure 73.8. Status data: cumulative faults discovered as a function of customer execution time

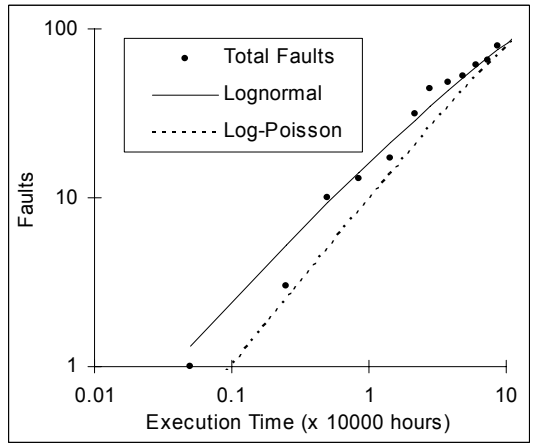


Figure 73.9. Stratus data: log scale showing early data with slight advantage to lognormal

distribution. Everett [41] measured the distribution of execution rates of lines of code and fitted it with a power-law to establish the parameters of a flexible reliability growth model with a known mathematical function.

By contrast, we have used a general-principled approach which takes the multiplicative process to the limit and finds the distribution of the event rates to be lognormal.

73.5.2 Growth Model

A detailed description of the validation of the lognormal reliability growth model using Stratus and Musa data sets is provided in [24]. First we present a synopsis of validation using one of the Stratus data sets. The Stratus data are collected from several hundred module-years of customer exposure on an operating system release. A module consists of one or more processors, peripheral controllers, and memories, all of which are typically duplexed (*i.e.,* in lockstep). The operating system itself is over one million lines of code, supports fault-tolerant hardware and is complex. The data series provides the cumulative execution time (*i.e.,* number of module-hours) and cumulative number of distinct faults discovered on a weekly basis. Each machine was attached to the Stratus Remote Service Network (RSN); failures reported by customers are logged in a call database, and when a call is resolved to be due to a fault a bug number is assigned to the call. If the fault has not been seen before, a new bug number is assigned. The earliest call for each fault (bug number) identifies the calendar week in which a failure due to the fault first occurred.

The number of machines on a given release was determined by analyzing RSN calls placed when a new release was installed, therefore only failures occurring in a specific release were counted, and each failure was counted only if it was the first time a failure due to that fault occurred in that release. Thus the data series represents the cumulative number of first-failures as a function of execution time.

The Stratus systems from which the data were collected represent initial versions of a yearly release. No new functionality was added. Only the most urgent fixes were made to the software during the course of its life in the field; most fixes were made to subsequent maintenance releases. Thus the code in question was essentially unchanged through the course of its field exposure. Stratus systems are used for continuous processing of stable, mission-critical applications so execution time on a release during a given week is equal to 168 hours times the number of machines on which the release was running. Common applications are telecommunications, banking, and brokerage. No attempt is made here to correct for the effect

processor speed may have on the observed failure rate. This would be an issue if the mean processor speed over the installed base varied widely during the life of the release, which was not the case.

The log-Poisson model, which is an infinite failures model, was used as the competing model for comparison, because it does not have an underlying failure rate distribution and is yet very successful in practice. The parameters of both the lognormal and log-Poisson models were estimated using the maximum likelihood method. Figure 73.8 shows the data and the fits obtained using the lognormal and log-Poisson models. Figure 73.9 illustrates the ability of the lognormal to fit the earliest data as well as the rest.

The models were compared objectively using log likelihood and Akaike Information Criteria (AIC) [42]. The AIC provides a natural way to compare the adequacy of models which are unrelated or have different numbers of parameters. The best model is the one with the minimum AIC value. By penalizing models that have more parameters, the AIC embodies the principle that adding more parameters may increase the ability to fit the past at the expense of decreasing the ability to fit the future. Akaike [42] provides theoretical reasons why this definition is appropriate.

When interpreting the AIC values of competing models, what matters is their difference [43]. A difference of less than one is not significant, but a difference larger than one or two is considered to be significant. For one of the Stratus data sets, the difference in AIC values is greater than 8 units in favor of the lognormal. For the second data set [24], the lognormal has an advantage, even though the AIC penalizes it for the extra parameter, but the advantage is not significant. Together these two data sets suggest the lognormal growth model has the potential to greatly exceed the performance of the log-Poisson model.

The fitted parameters of the lognormal and their standard deviations are σ (3.275, 0.305), μ (−19.31, 0.95) and N (3808, 1280). This implies the total number of defects may be over ten times the number of defects already found, and the uncertainty in that estimate is 30%. Figure 73.10 shows the uncertainty is due to the high degree of covariance between the parameters when the data

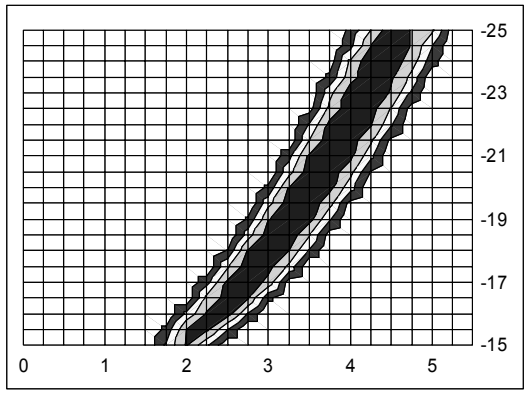


Figure 73.10. Stratus data: relative log-likelihood as a function of (σ, μ.). A long peak (*dark*) from (2, –15) to (4.5, –25) represents values within two units of the maximum log-likelihood

are not conclusive. At all points along the ridge there must be a good fit to the already observed initial discovery rate $m(0) = N \cdot \exp(\mu+\sigma^2/2)$. But as σ increases (and μ decreases) the mean rate exp $(\mu+\sigma^2/2)$ decreases and N increases leading to a much larger value of N. On the other hand, decreases in σ yield a decline in N.

A three-way comparison was conducted between the lognormal, log-Poisson and exponential models using 10 Musa data sets. In nine out of ten sets, the lognormal model fit the data better or as well as the other two models [24].

Despite the variety of models of software reliability growth proposed in the literature, there is an undercurrent of dissatisfaction. Each model has strengths, but the very existence of so many models implies that no single model is flexible enough to model software reliability growth in general. Levendel [44] has recognized earlier models as being either too optimistic or too pessimistic. The dividing line is related, if not identical, to the division between finite and infinite failure models. The problem cannot be escaped by combining or weighting models to create super models. Levendel's [44] case against super models is supported by Keiller and Miller's [32] evaluation of 6 models and 8 super models against 20 data sets, which found super models offered no improvement in prediction. The lognormal reli-

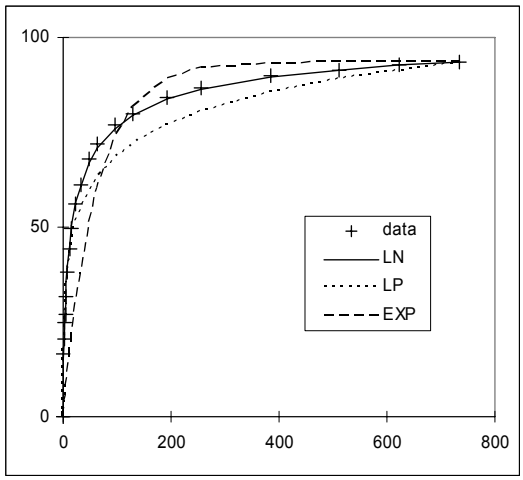


Figure 73.11. SHARPE Coverage data: growth of percent block coverage with number of tests, average of ten replications

ability growth model is attractive compared to earlier alternatives because of its robust origin, its relationship to how software works, and the fact that it is supported by failure rate distribution data.

When used to model the growth of four coverage types, namely, block, decision, c-use and p-use [27] [45], the lognormal growth model significantly outperformed the log-Poisson and the basic execution time models. Figure 73.11 compares the maximum likelihood fits for the three models to the growth of cumulative block coverage F in the 30,000 line SHARPE application. It is shown in a linear form to illustrate the ability of the lognormal to fit both early and late data. Visually, the lognormal is a better fit. Using statistical tests, the superiority of the lognormal [16] over the other models, for the entire SHARPE application and most of its constituent files was confirmed.

The significant evidence in favor of the lognormal in coverage growth is particularly interesting because it was based on data generated from replicated run experiments. As pointed out by Miller [23], a comparison of models using a single realization may not be conclusive, because the statistical fluctuations within a single realization would often mask differences among the models due to their similarity.

73.5.3 Occurrence Count Model

A synopsis of the validation of the occurrence count model is provided here, details can be obtained from [46]. The data was collected in the ordinary course of recording the occurrence of software defects in two operational databases. The first is a defect tracking system with one record for each defect. The second system uses trouble-tickets to track the occurrence of incidents at customer sites. When a customer incident is due to a defect, a bidirectional link is established between the incident and the appropriate defect. The defects for which there was a least one trouble-ticket were included, counting the initial discovery as well as rediscoveries. Each defect contains the identifiers of all trouble-tickets associated with the defect and, implicitly, the count. The data were collected for four sets of defects, each divided into three subsets.

The data showed that a relatively small percentage of defects cause a large number of incidents *per* defect and *vice versa*. This indicates that the distribution of the occurrence counts of defects is likely to be skewed, even "heavy-tailed" suggesting that the lognormal may provide a reasonable fit. The alternative model used for comparison is discrete Pareto, since the Pareto distribution is an often-used heavy tailed distribution [47].

Figure 73.12, which depicts the fits provided by the two models, shows a clear problem for the Pareto in the high count tail. It also shows error bars on each data point equal to the standard deviation of the lognormal fitted value. This illustrates that in this case, within statistical variation, the data follow the lognormal rather than the Pareto. The Chi-square, which was used to objectively compare the quality of fits of the two models, significantly favored the lognormal in three subsets at significance levels of .0001, .01, and .05. The data never reject the lognormal even at the .05 level. Thus, the data are consistent with the discrete lognormal (DLN) but not the discrete Pareto. The DLN model was also shown to be an adequate fit to the occurrence phenomenon of

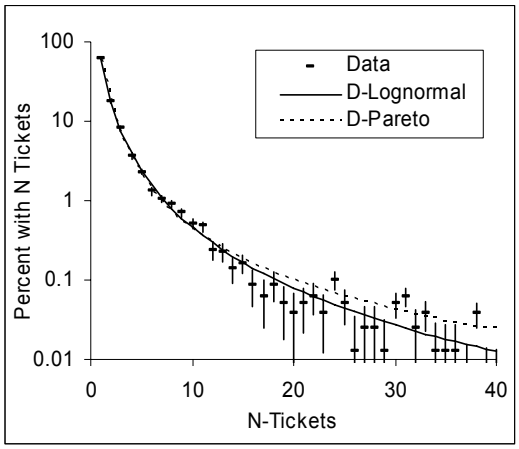


Figure 73.12. Cisco occurrence count data: percent of defects with N (0:40) occurrences

network security defects, though the data were not sufficient to discriminate against the Pareto [48].

The DLN occurrence count model could be used to predict the number of occurrences of defects and the number of latent defects that have not yet occurred. These predictions could be used to guide the allocation of resources for software maintenance activities, which will allow expeditious resolution of defects that cause field failures and improve customer satisfaction [49]. The parameters found in this manner can be used in fitting or bounding the lognormal reliability growth model for the same software.

73.6 Future Research Directions

This section summarizes the advantages and current evidence of the application of the lognormal. It also discusses future opportunities.

The lognormal model has several advantages over earlier models. Its genesis is apparent, since the mathematical form of the model is directly traceable to the structure of the subject of the model. This mathematical link between software structures and the lognormal distribution is based on the central limit theorem, a profound result of probability theory. The assumptions about software systems on which the model is founded are equivalent or similar to those successfully used within many sub-disciplines of software engineering. The lognormal distribution has also been applied in hardware reliability modeling as well as a variety of other disciplines.

Presently, the lognormal and its transformations have been successfully used to model distributions of failure rates, execution rates of code elements, reliability and coverage growth and the occurrence frequencies of software defects in both controlled and commercial environments.

Many opportunities for future research exist. Some re-validate or apply either the rate or one of the derived distributions thereby increasing confidence in the application of the lognormal, while others attempt to unlock the value of the insight by exploiting the analytical properties of the lognormal or its origins in software structure. If the lognormal appears to be nearly ubiquitous then the challenge is no longer to find it but rather to apply it. These opportunities include:

The ability of the model to predict future fault count should be assessed, using prequential likelihood [50].

Prior research has indicated that predictions using limited data from early testing, tend to be inaccurate [51]. Questions such as how much data is needed for the lognormal to ensure predictions of a given level of accuracy also merit further consideration. The effect of slow convergence in the tail as implied by the CLT [52] on predictions based on early data also needs to be explored.

A central assumption underlying software reliability models is that the software is tested according to its operational profile. Since an accurate profile is usually not available, it is necessary to assess the sensitivity of the reliability to variation in the operational profile [14]. Can the lognormal be used to assess the impact of such variations quantitatively?

It would also be useful to assess the extent to which applying priors to the lognormal parameters will improve prediction. Since the lognormal has its roots in the complexity of software states, program flows, and operational profiles, there is an opportunity to use such information to estimate the parameters in advance of execution. For this purpose, methods to estimate the parameters,

especially σ, given such preliminary information are needed. Although the "true" operational profile is usually more complex than that of any analyst, an analyst's operational profile may be used to establish a lower bound on the variance of the log-rates of operations within the actual system.

When used to model software reliability growth, the parameter N represents the ultimate number of defects, which may be estimated based on many techniques in the extensive available literature. In the case of code coverage growth, N is either the total number of code elements or the maximum percentage of code coverage that can be achieved. An exact value of the total number of elements can be obtained directly from the code, while the maximum percentage of coverage is always 100%, reduced by unreachable code.

Finally, the parameter μ, which is a location parameter in the case of reliability growth and a measure of individual test efficiency in case of code coverage growth, may be obtained from prior releases or similar products. It is likely that similar systems will have similar parameters, allowing real use of prior information**.** Because it scales rates, μ will change as processing speeds change.

The conditions under which the bounds on the lognormal parameters obtained from different data types are tight or loose needs to be determined. In particular, the covariance structure between the lognormal parameters needs to be studied in the context of estimating the parameters from first-occurrence times, especially in the practical case in which only truncated (*i.e.,* early) data are available. Reparameterizations may lead to sharper characterizations of their interrelationships.

The lognormal distribution provides a unique potential to share information from structural knowledge (or size), operational profile, code coverage growth, occurrence counts, and so on, when determining parameters within a given system, and then being able to apply those parameters with additional confidence in other contexts. To assess this potential, it is necessary to compare the parameters of the lognormal, estimated from different perspectives (measured by direct rate, *via* the Laplace transform in software reliability and code coverage growth or *via* discrete lognormal using the occurrence counts) for a single system. Further, this exercise must be repeated for several systems.

The impact of process characteristics on the lognormal parameters needs to be studied. For example, the σ values estimated from occurrence count data were generally less than 2.0, which seemed low for the large product size [46]. Could this be due to heavy prior testing? Will this model still hold if fix-times are variable?

The Pareto distribution is an alternative heavy tailed distribution [47], and a close competitor to the discrete lognormal occurrence count model. Other conditions under which that relationship holds need to be determined.

Studies similar to the other models, including methods to determine the optimal release time and the optimization of test strategies, are needed for the lognormal. Robust solutions to these problems depend on using the correct form of the distribution of the failure rates of defects. Can the knowledge of the form of the occurrence count distribution and its parameters be used to quantitatively evaluate defect repair/ship strategies or even deduce optimal ones?

The lognormal is presented as an execution time, or as a closely related test-effort model. If execution time or test effort were a known function of real time, it may be worth exploring whether simple parametric substitution yields functions with useful, recognizable, or simple forms. Among these, assumptions of linearly or exponentially ramping usage may be of practical applicability.

Adams [30] noted defects arising from imperfect repair (*i.e.,* bad fixes) have failure rates drawn from the original distribution rather than having the lower rates characteristic of the defects being repaired. Confirming this, [46] found occurrence counts of defects originating as bad fixes are well fit by the DLN, and have both a wider rate spread and higher average rate than the defects being repaired. The practical challenge is to determine the point in the lifecycle when the benefit of repairing a low-rate defect is offset by the risk of introducing a new high-rate defect.

A number of these opportunities may exploit the analytical properties of the lognormal and its related functions.

73.7 Conclusions

This chapter discussed emerging applications of the lognormal and its transformations in software reliability engineering. Software, being essentially massless, a skeleton of conditionals implementing a breakage process, is an ideal generator of the lognormal. The lognormal is widely used in other disciplines and the knowledge and the experience gained from those applications should be valuable in applying it to software engineering problems. The array of enabling research opportunities identified provides an insight into the potential of the lognormal. It is likely that the application of the lognormal to software engineering may eventually serve as a model for other disciplines.

Acknowledgments

Thanks are due to Dom Grieco, John Intintolo, and Jim Lambert of Cisco Systems, Inc., for their insight and support. Thanks are also due to Dr. William Everett, Los Alamos National Laboratory, and Professor Mark Lepper, Stanford University, for many constructive comments. The research at University of Connecticut is supported in part by a CAREER award from the National Science Foundation (#CNS-0643971).

References

[1] Farr W. Software reliability modeling survey. In: Lyu MR, editor. Handbook of Software reliability engineering. McGraw-Hill, New York, 1996; 71–117.

[2] Xie M. Software reliability modeling. World Scientific, Singapore, 1991.

[3] Crow EL, Shimizu K, editor. Lognormal distributions: Theory and applications. Marcel Dekker, New York, 1988.

[4] Kececioglu D. Reliability engineering handbook Prentice Hall, Englewood Cliffs, NJ, 1991.

[5] Johnson NL, Kotz S, Balakrishnan N. Continuous univariate distributions. Wiley, New York, 1994.

[6] Aitchison J, Brown JAC. The lognormal distribution. Cambridge University Press, 1969.

[7] Petrov VV. Sums of independent random variables. Springer, Berlin, 1975.

[8] Loeve M. Probability theory. Van Nostrand, New York, 1963.

[9] Patel JK, Read BC. Handbook of the normal distribution. Marcel Dekker, New York, 1996.

[10] Feller W. An Introduction to probability theory and its applications. John Wiley & Sons, New York, 1971.

[11] Juhlin BD. Implementing operational profiles to measure system reliability. Proceedings of 3rd International Symposium on Software Reliability Engineering. Research Triangle Park NC; October 1992: 286–295.

[12] Musa JD. The operational profile in software reliability engineering: An overview. Proceedings of 3rd International Symposium on Software Reliability Engineering. Research Triangle Park NC; October 1992: 140–154.

[13] Gnedenko BV. The theory of probability. Chelsea Publishing, New York (Translator: B.D. Seckler), 1962.

[14] Cukic B, Bastani FB. On reducing the sensitivity of software reliability to variations in the operational profile. Proceedings of 7th International Symposium on Software Reliability Engineering. White Plains NY; November 1996: 45–54.

[15] Horgan JR, London SA. Data flow coverage and the C language. Proc. of 4th International Symposium on Testing, Analysis and Verification. Victoria British Columbia; October 1991: 87–97.

[16] Gokhale S, Mullen R. The marginal value of increased testing: An empirical analysis using four code coverage measures. Journal of Brazilian Computer Society. December 2006; 12(3):13–30.

[17] Bishop P, Bloomfield R. Using a lognormal failure rate distribution for worst case bound reliability prediction. Proceedings of 14th International Symposium on Software Reliability Engineering. Denver CO; November 2003: 237–245.

[18] Ye N, Zhang Y, Borrer CM. Robustness of the Markov chain model for cyber attack detection. IEEE Transactions on Reliability 2004; R-53(1): 116–123.

[19] Trivedi KS. Probability and statistics with reliability, queuing, and computer science applications. Wiley, New York, 2001.

[20] Avritzer A, Larson B. Load testing software using deterministic state testing. Proceedings of International Symposium on Software Testing and Analysis. Cambridge MA; June 1993: 82–88.

[21] Kleinrock L. Queuing systems volume II. Wiley, New York, 1975.

[22] Hamlet D, Voas J. Faults on its sleeve: Amplifying software reliability testing. Proceedings of International Symposium on Software Testing and Analysis. Cambridge MA; November 1993: 89–89.

[23] Miller DR. Exponential order statistic models of software reliability growth. NTIS. NASA Contractor Report, 1985; 3909.

[24] Mullen RE. The lognormal distribution of software failure rates: Application to software reliability growth modeling. Proceedings of 9th International Symposium on Software Reliability Engineering. Paderborn Germany; November 1998:134–142.

[25] Johnson NL, Kotz S, Kemp A. Univariate discrete distributions. Wiley, New York, 1993.

[26] Musa JD. A theory of software reliability and its application. IEEE Transactions on Software Engineering. 1975; SE-1(1): 312–327.

[27] Gokhale S, Mullen R. From test count to code coverage using the Lognormal. Proceedings of 15th International Symposium on Software Reliability Engineering. St. Malo France; November 2004: 295–304.

[28] Bishop P, Bloomfield R. A conservative theory for long-term reliability growth prediction. Proceedings of 7th International Symposium on Software Reliability Engineering. White Plains NY; November 1996: 308–317.

[29] Mullen RE. The lognormal distribution of software failure rates: Origin and evidence. Proceedings of 9th International Symposium on Software Reliability Engineering. Paderborn Germany; November 1998: 124–133.

[30] Adams EN. Optimizing preventive service of software products. IBM Journal of Research And Development 1984; 28(1):2–14.

[31] Rao RC. Asymptotic efficiency and limiting information. Proceedings of 4th Berkeley Symposium on Mathematical Statistics and Probability. 1961; 1:531–545.

[32] Keiller PA, Miller DR. On the use and the performance of software reliability growth models. Reliability Engineering and Systems Safety 1991; 32: 95–117.

[33] Trachtenberg M. Why failure rates observe Zipf's law in operational software. IEEE Transactions on Reliability 1992; 41: 386–389.

[34] Nagel PM, Skirvan JA. Software reliability: Repetitive run experimentation and modeling. NASA, 1982; CR-165836.

[35] Nagel PM, Scholtz FW, Skirvan JA. Software reliability: additional investigations into modeling with replicated experiments. NTIS. NASA, 1984; CR-172378.

[36] Mason RL, Gunst RF, Hess, JL. Statistical design and analysis of experiments. Wiley, New York, 1989.

[37] Vasicek OA. Test for normality based on sample entropy. Journal of the Royal Statistical Society B. 1976; 38: 54–59.

[38] Jelinski Z, Moranda PB. Software reliability research. In: Freiberger W, editor. Statistical computer performance evaluation. Academic Press, New York, 1972; 465–484.

[39] Goel AL, Okumoto K. Time-dependent error detection rate models for software reliability and other performance measures. IEEE Transactions on Reliability 1979; R-28(11): 206–211.

[40] Iyer RK, Rossetti DJ. Effect of system workload on operating system reliability: A study on IBM 3081. IEEE Transactions on Software Engineering 1985; 1438–1448.

[41] Everett WW. An extended execution time software reliability model. Proceedings of 3rd International Symposium on Software Reliability Engineering. Raleigh NC; October 1992: 4–13.

[42] Akaike H. Prediction and entropy. NTIS, MRC Technical Report Summary, 1982; #2397.

[43] Sakamoto Y, Ishiguro M, Kitagawa G. Akaike Information criterion statistics. D. Reidel, Boston, 1986.

[44] Levendel Y. Can there be life without software reliability models? Proceedings of 2nd International Symposium on Software Reliability Engineering. Austin TX; November 1991: 76–77.

[45] Gokhale S, Mullen R. Dynamic code coverage metrics: A Lognormal perspective. Proceedings of 11th International Symposium on Software Metrics. Como Italy; September 2005: 33–43.

[46] Mullen R, Gokhale S. Software defect rediscoveries: A Discrete Lognormal model. Proceedings of 16th International Symposium on Software Reliability Engineering. Chicago IL; November 2005: 203–212.

[47] Downey A. Lognormal and Pareto distributions in the Internet. Computer Communications 2005; 28(7): 790–801.

[48] Mullen R, Gokhale S. A discrete lognormal model for software defects affecting QoP. In: Gollmann D, Massacci F, Yautsiukhin A (editors). Quality of protection: Security measurements and metrics. Advances in Information Security Series 2006; 37–48.

[49] Kenney GQ. Estimating defects in commercial software during operational use. IEEE Transactions on Reliability 1993; 42(1): 107–115.

[50] Brocklehurst S, Littlewood B. Techniques for prediction analysis and recalibration. In: Lyu MR, editor. Handbook of software reliability Engineering, McGraw-Hill, New York, 1996; 119–166.

[51] Xie M, Hong GY, Wohlin C. A practical method for the estimation of software reliability growth in the early stage of testing. Proceedings of 8th International Symposium on Software Reliability Engineering. Albuquerque NM; November 1997: 116–123.

[52] Bradley B, Taqqu M. Financial risk and heavy tails. Handbook of Heavy Tailed Distributions in Finance. Elsevier, Amsterdam, 2003

74

Early-stage Software Product Quality Prediction Based on Process Measurement Data

Shigeru Yamada

Department of Social Systems Engineering, Tottori University, Tottori, Japan

Abstract: In recent years, delivery time has become shorter in software development in spite of high-quality requirements. In order to improve software product quality during a limited period, we have to manage process quality and control product quality in the early-stage of software development. Software product quality can be achieved in the development process. Then, it is important for us to predict the product quality in the early-stage and to execute effective management. In this chapter, we conduct multivariate linear analysis by using process measurement data, derive effective process factors affecting product quality, and obtain quantitative relationships between quality assurance/management activity and final product quality.

74.1 Introduction

Software product quality can be achieved in the development process [1], [2]. According to quality management, software faults introduced in the development process need to be decreased by reviewing intermediate products after finishing each process in the early-stage of software development. Moreover, it is important to detect most of the remaining faults in the testing process. Then, in order to improve the product quality during the limited period, we have to control the development process and predict product quality in the early-stage of software development [3]–[10].

To control and predict product quality in the early-stage of software development, Fukushima *et al*. [8] and Yamada and Fukushima [9] have implemented risk management, process quality management, and product quality assurance activities. Through these activities, they have discussed multiple linear regression analysis by using these process measurement data and have derived a relational expression that can predict the quality of software products quantitatively. From this analysis, they examined the effects on software products quality of these management factors and quality assurance factors, and obtained a clear correlation between these activities and software product quality. That is, a prediction of product quality by using process measurement data is shown to be very effective to clarify the process factors that affect product quality and to promote the improvement of these process factors.

In this chapter, based on the results of Fukushima *et al.* [8] and Yamada and Fukushima [9], we analyze the process measurement data by using principal component analysis and multiple regression analysis according to the derivation

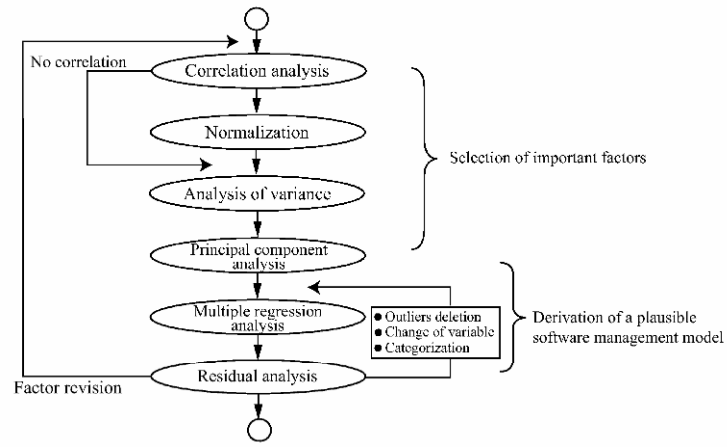


Figure 74.1. Derivation procedures

Table 74.1. Analyzed quality assurance process data

	Management of review		Rreviw technique	Test technique	Software products quality
Project No.	Rate of design review delay X_1 (0∼1.00)	Frequency of review X_2	Average score of review X_3 (0∼100)	Number of test items X_4	Number of faults detected in testing Y
1	0.50	5	80.50	71	38
2	-0.07	12	82.50	48	3
3	-0.12	4	64.00	12	7
4	0.10	1	35.50	44	20
5	0.09	3	62.00	138	26
6	0.08	14	89.25	25	0
7	0.00	3	44.25	33	22

procedures for a software management model [2] (as shown in Figure 74.1). Further, deriving the factors affecting product quality, we validate the results of Fukushima *et al*. [8] and propose more effective measures to apply project management techniques. Further, we conduct a discriminant analysis by using the observed data reflecting the management process to derive a discriminant expression judging whether or not the software project has a quality process.

74.2 Quality Prediction Based on Quality Assurance Factors

74.2.1 Data Analysis

First, we predict the software product quality by using process measurement data of quality assurance factors (as shown in Table 74.1). The factor tree diagram for software quality improvement is given by Figure 74.2. The number of faults detected in testing as the metric of software product quality is used as an objective variable.

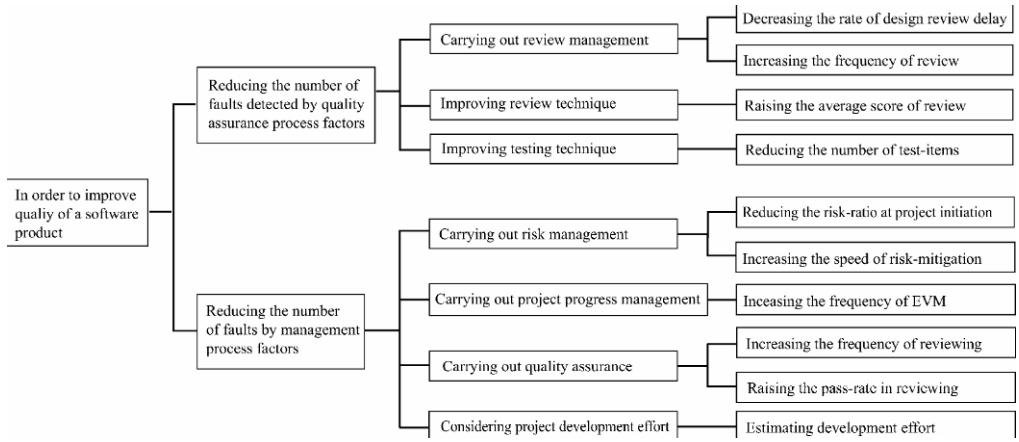


Figure 74.2. The factor tree diagram for software quality improvement

Four control variables, *i.e.*, the rate of the design review delay, the frequency of review, the average score of review, and the number of test items, are used as explanatory variables. These variables introduced above are explained in the following when the actual review has finished earlier than the planning.

X_2: the frequency of review (the frequency of review-assessment *per* development size).

Y: the number of faults detected during system testing and quality assurance testing.

X_4: the number of test items (the number of system test items and the number of quality assurance test items).

X_1: the rate of design review delay [0,1.00] (the averaged delay period/the development period). The computed value is negative X_3: the average score of review [0,100.0] (the average score of design reviews). The review score is measured by using the review checklist (maximum 100 points).

74.2.2 Correlation Analysis

A result of conducting the test of correlation analysis among the explanatory and objective variables is shown in Table 74.2, from which we can consider the correlation as follows:

Table 74.2. Correlation matrix for quality assurance factors

	X_1	X_2	X_3	X_4	Y
X_1	1				
X_2	-0.1343	1			
X_3	0.2088	0.8384	1		
X_4	0.3694	-0.2725	-0.0041	1	
Y	0.7576	-0.6769	-0.3234	0.5695	1

(1) X_1 and X_2 have shown a strong correlation to Y.
(2) X_3 has not shown a correlation to Y.
(3) X_2 and X_3 have also shown a strong correlation.

Based on the correlation analysis, X_1, X_2, and X_4 are selected as the important factors for estimating a quality prediction model because X_3 has multicollinearity with X_2 and has a low correlation to Y.

74.2.3 Principal Component Analysis

Regarding variable Y as the explanatory variable, we conduct the test of independence among explanatory variables X_i (i = 1, 2, 3, 4) by the principal component analysis. We find that the precision of analysis is high from Table 74.3. And factor loading values are obtained in Table 74.4. Let newly denote the first and second principal components as follows:

Table 74.3. Summary of eigenvalues and principal components

Component	Eigenvalue	Contribution ratio	Cumulative contribution ratio
1	2.615	0.523	0.523
2	1.615	0.323	0.846
3	0.646	0.129	0.975
4	0.091	0.018	0.993
5	0.033	0.007	1.000

Table 74.4. Factor loading values

	Component 1	Component 2
X_1	0.584	0.693
X_2	-0.835	0.514
X_3	-0.550	0.809
X_4	0.611	0.402
Y	0.949	0.236

- The first principal component is defined by the measure for evaluating total quality characteristics.
- The second principal component is defined by the measure for discriminating the process factors as the quality management activity factors(X_2, X_4) and the review management activity factors (X_1, X_3).

We have evaluated seven actual software projects by the first principal component. Then, we can confirm that several projects, *i.e.*, project numbers 2, 3, and 6, experience a small number of faults detected in testing (see Tables 74.1 and 74.5). From relations among factor loading values for the first principal component in Table 74.4, it is found that the rate of design review delay (X_1), the frequency of review (X_2), and the number of test items (X_4) affect the number of faults detected in testing (Y).

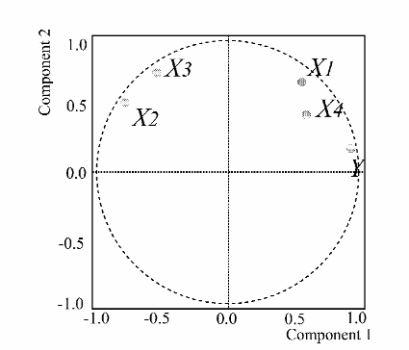


Figure 74.3. Scatter plot of the factor loading values

Table 74.5. Principal component scores

Project No.	Component 1	Component 2
1	1.032	1.528
2	-1.118	0.310
3	-0.561	-0.939
4	0.692	-1.043
5	0.959	0.342
6	-1.359	0.755
7	0.354	-0.954

We obtain a scatter plot in Figure 74.3 showing that these explanatory variables are independent each other. As a result of correlation analysis and principal component analysis, we can select X_1, X_2, and X_4 as the important factors of a software quality prediction model.

74.2.4 Multiple Linear Regression

A multiple linear regression analysis is applied to the process data as shown in Table 74.1. Then, using X_1, X_2, and X_4, we estimate the multiple regression equation predicting software product quality, $\hat{Y}$, given by (74.1) as well as the normalized multiple regression expression, $\hat{Y}^N$, given by (74.2):

$$\hat{Y} = 18.712 + 41.718X_1 - 1.502X_2 + 0.064X_4, \quad (74.1)$$

$$\hat{Y}^N = 0.613X_1 - 0.541X_2 - 0.196X_4. \quad (74.2)$$

In order to check the goodness-of-fit adequacy of our model, the coefficient of multiple determination (R^2) is calculated as 0.9419. Furthermore, the squared multiple correlation coefficient, called the contribution ratio, adjusted for degrees of freedom (adjusted R^2), is given by 0.8839. The result of multiple linear regression analysis is summarized in Tables 74.6 and 74.7.

From Table 74.7, it is found that the reliability of these multiple regression equations is high. Then, we can predict the number of faults detected in testing for the final products by using (74.1). From (74.2), the explanatory variables affecting the objective variable Y are X_1 and X_2. Therefore, we conclude that "the rate of design review delay" and "the frequency of review" have an important impact on the product quality.

Table 74.6. Estimated parameters

Factor	Coefficient	SE	t-value	Standard coefficient
Intercept	18.712	4.315	4.337	0.000
X_1	41.718	10.202	4.089	0.613
X_2	-1.502	0.402	-3.741	-0.541
X_4	0.064	0.051	1.269	0.196

By using (74.2) the predicted and actual measurement values are given in Figure 74.4 which shows that the number of faults can be predicted with high accuracy.

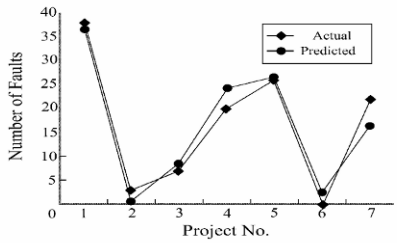


Figure 74.4. Accuracy for predicting the number of faults

Table 74.7. Analysis of variance

Source of variation	SSq	DF	MSq	F-value
Due to regression	1073.6	3	357.9	16.23 *
Error	66.2	3	22.05	
Total	1139.7	6		

74.2.5 The Effect of Quality Assurance Process Factors

We have shown the following correlation between quality assurance process factors and product quality:

- Through a regression analysis, it has become clear that the design review delay has had an important impact factor on software product quality. The review management and progress management influence the number of faults detected in testing.
- The frequency of review has also affected the number of faults detected in testing. So, we consider that the number of inspection review by the quality assurance department is insufficient.
- The average score of review has not influenced the number of faults detected in testing. We consider that the issue is in the assessment method of design review activities. Then, we have to investigate this cause.

74.3. Quality Prediction Based on Management Factors

74.3.1 Data Analysis

Secondly, we predict software product quality by using process measurement data of management process factors (see Figure 74.2) as shown in Table 74.8.

The number of faults as the metric of software products quality is used as the objective variable. Six variables (*i.e.*, the risk ratio of project initiation, the speed of risk mitigation, the frequency of EVM (earned value management), the frequency of review, the pass rate of review, and the development effort) are used as the explanatory variables. The variables introduced above and another two objective variables in addition to the number of faults are explained in the following:

Y_1: the number of faults detected during acceptance testing in operation.
Y_2: the development cost (the difference between predicted and actual development costs).
Y_3: the delivery date (the difference between predicted and actual delivery date).

X_1: the risk ratio of project initiation. The risk ratio is given by

$$R = \sum_i \{\text{risk item}(i) \times \text{weight}(i)\}, \quad (74.3)$$

where the risk estimation checklist has weight (i) in each risk item (i), and the risk ratio ranges between 0 and 100 points. Project risks are identified by interviewing the project manager using the risk estimation checklist. From the identified risks, the risk ratio of a project is calculated by (74.3).

Table 74.8. Analyzed management process data

	Risk management		Project management	Quality assurance		project scale	Software products quality		
Project NO.	Risk ratio of project initiation X_1 (0〜100)	Speed of risk mitigation X_2 (0〜1.00)	Frequency of EVM X_3	Frequency of review X_4	Pass rate of review X_5 (0〜1.00)	development size X_6	Number of faults Y_1	Development cost Y_2	Delivery date Y_3
1	73	1.00	0.21	0.05	0.50	42.8	12	113	125
2	47	0.33	0.78	0.01	0.50	20.9	0	92	91
3	38	0.87	1.18	0.14	0.50	14.0	13	112	100
4	35	0.95	0.74	0.12	1.00	8.2	3	104	100
5	34	0.51	2.70	0.22	0.50	18.2	0	93	100
6	32	1.00	1.70	1.71	0.67	1.8	1	119	108
7	32	0.28	0.79	0.07	0.00	28.1	0	92	100
8	24	0.00	0.99	0.62	0.74	6.5	0	103	100
9	23	0.00	1.84	0.31	0.50	50.2	0	82	100
10	13	0.00	2.42	0.54	1.00	5.6	0	100	102

X_2: the speed of risk mitigation (the period for which the risk ratio reached 30 or less points/the development period). The reason why we use 30 points as a benchmark is because almost all projects which have reached their QCD (quality, cost, delivery) targets had a risk ratio of 30 points or less. When the risk ratio is 30 points or less from project beginning, X_2 is 0. When the risk ratio is 30 or more points until project completing, X_2 is 1.

X_3: the frequency of EVM (the frequency of EV analysis per development effort). We have some experiences that we can mitigate project risks with more frequent EV analysis because the manager can deal with problems early on.

X_4: the frequency of review (the frequency of review *per* development effort). We have some experiences that a quality project makes review activity frequently.

X_5: the pass rate of review (the pass rate of the first review). The judgment level of the review ranges between 0 and 1.00.

X_6: the development effort measured by man-months.

74.3.2 Correlation Analysis

A result of correlation analysis among the explanatory and objective variables is shown in Table 74.9. From Table 74.9, we can consider the correlation as follows:

(1) X_1 has shown a strong correlation to X_2 and X_3.

(2) X_6 has also shown a strong correlation to X_4 and X_5.

(3) Y_2 out of three objective variables is influenced by X_6.

(4) X_1 and X_2 has shown a strong positive correlation to Y_1.

Based on the correlation analysis, X_2, X_3, X_4, and X_5 are selected as the important factors for estimating a quality prediction model because X_1 and X_6 have multicollinearity with explanatory variables X_i (i = 2, 3, 4, 5).

74.3.3 Principal Component Analysis

In a similar discussion to that in Section 74.2.3, we conduct the test of independence among explanatory variables X_i (i= 2, 3, 4, 5) for the principal component analysis. Then, we find that the precision of analysis is high from Table 74.10. Moreover, factor loading values are obtained as shown in Table 74.11. Let us denote the first and second principal components as follows:

Table 74.9. Correlation matrix for management process factors

	X_1	X_2	X_3	X_4	X_5	X_6	Y_1	Y_2	Y_3
X_1	1								
X_2	0.633	1							
X_3	-0.656	-0.354	1						
X_4	-0.338	0.125	0.332	1					
X_5	-0.302	0.050	0.238	0.290	1				
X_6	0.418	-0.132	-0.233	-0.504	-0.545	1			
Y_1	0.651	0.643	-0.455	-0.289	-0.072	0.202	1		
Y_2	0.352	0.738	-0.275	0.475	0.302	-0.479	0.589	1	
Y_3	0.597	0.501	-0.282	0.125	-0.000	0.305	0.566	0.570	1

- The first principal component is defined by the measure for evaluating total project management.
- The second principal component is defined by the measure for discriminating the process factors as the risk management activity factors (X_2, X_4, X_5) and the project management activity factor (X_3).

As a result of correlation analysis and principal component analysis, X_2, X_3, and X_4 are selected as the important factors for a software management model because X_4 and X_5 have not a high degree of independence as shown in Figure 74.5, and X_5 has a low correlation to Y_1, Y_2, and Y_3 from the correlation analysis.

Table 74.10. Summary of eigenvalues and principal components

Component	Eigenvalue	Contribution ratio	Cumulative contribution ratio
1	1.598	0.399	0.399
2	1.226	0.307	0.706
3	0.730	0.183	0.889
4	0.446	0.111	1.000

Table 74.11. Factor loading values

	Component 1	Component 2
X_2	-0.276	0.881
X_3	0.800	-0.360
X_4	0.694	0.431
X_5	0.632	0.368

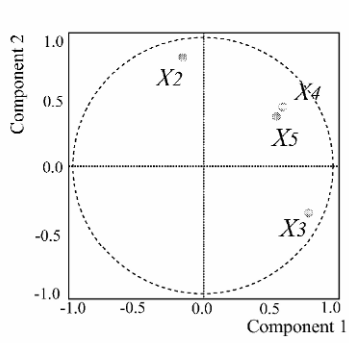


Figure 74.5. Scatter plot of the factor loading values

74.3.4 Multiple Linear Regression

A multiple linear regression analysis is applied to the management process data as shown in Table 74.8. However, the goodness-of-fit adequacy of two models about Y_1 and Y_3 is not so good because R^2 is calculated as 0.563 for Y_1 and 0.277 for Y_3, and adjusted R^2 is calculated as 0.344 for Y_1 and -0.084 for Y_3. As a result, the estimated multiple regression equation is obtained by using X_2, X_3, and X_4 as explanatory variables, and development cost (Y_2) as on objective variable. Then, we have the estimated multiple-regression equation for predicting the development cost of software project, $\hat{Y}_2$, given by (74.4) as well as the normalized multiple regression expression, $\hat{Y}_2^N$, given by (74.5):

$$\widehat{Y}_2 = 93.069 + 16.067X_2 - 3.136X_3 + 10.773X_4, \quad (74.4)$$

$$\widehat{Y}_2^N = 0.601X_2 - 0.219X_3 + 0.473X_4. \quad (74.5)$$

In order to check the goodness-of-fit adequacy of our model, R^2 calculated as 0.728. Furthermore, adjusted R^2 is given by 0.592. The results of multiple linear regression analysis are summarized in Tables 74.12 and 74.13.

From (74.5), the explanatory variables affecting the objective variable Y_2 are X_2 and X_4. It is found that "the speed of risk mitigation" and "the frequency of review" have an important impact on Y_2.

By using (74.5) the predicted and actual measurement values are as shown in Figure 74.6, which shows that the development cost can be predicted with high accuracy.

Table 74.12. Estimated parameters

Factors	Coefficient	SE	t-value	Standard coefficient
Intercept	93.069	6.568	14.171	0.000
X_2	16.067	6.325	2.540	0.601
X_3	-3.136	3.567	-0.879	-0.219
X_4	10.773	5.349	2.014	0.473

Table 74.13. Table of analysis of variance

Source of variation	SSq	DF	MSq	F-value
Due to regression	866.488	3	288.829	5.3568 *
Error	323.512	6	53.919	
Total	1190.0	9		

74.3.5 The Effect of Management Process Factors

We have shown the following correlation between management process factors and the development cost:

- Through a regression analysis, it has become clear that the speed of risk mitigation has had an important impact factor on the development cost.
- Early-stage risk mitigation in software projects is important in shortening the difference between predicted and actual development costs.
- We have found that the review activity is very important as a management process factor as well as a quality assurance process factor because the frequency of review affects the development cost.
- The passing status of reviews has not affected the development cost. Then, we have to consider this issue in the assessment method of review activities.

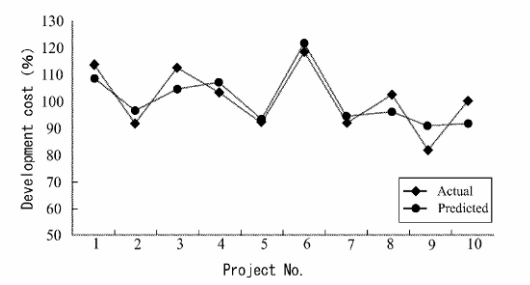


Figure 74.6. Accuracy for predicting the development cost

74.3.6 Relationship Between Development Cost and Effort

As a result of correlation analysis, we find that the development cost (Y_2) and the development effort (X_6) have a correction. Then, a multiple linear regression analysis has conducted again by normalizing the development cost as $Z_2 \equiv Y_2/X_6$. That is, a multiple linear regression analysis is conducted based on explanatory variables of X_2, X_3, and X_4, and a objective variable of Z_2. Then, we have the estimated multiple regression (for the normalized development cost, $\hat{Z}_2$, given by (74.6) as well as the normalized multiple regression expression, $\hat{Z}_2^N$, given by (74.7):

$$\hat{Z}_2 = -3.907 + 9.148X_2 - 0.659X_3 + 36.142X_4, \quad (74.6)$$

$$\hat{Z}_2^N = 0.204X_2 - 0.027X_3 + 0.947X_4. \quad (74.7)$$

In order to check the goodness-of-fit adequacy of our model, R^2 is calculated as 0.974. Furthermore, adjusted R^2 is given by 0.960. The result of multiple linear regression analysis is summarized in Tables 74.14 and 74.15.

From (74.7) the explanatory variable affecting the objective variable is X_4. It is found that the frequency of review has an important impact on $\hat{Z}_2$.

By using (74.6) the predicted value and actual measurement values are as shown in Figure 74.7, which shows that the normalized development cost can be predicted with high accuracy.

Table 74.14. Estimated parameters

Factor	Coefficient	SE	t-value	Standard coefficient
Intercept	-3.907	3.431	-1.139	0.000
X_2	9.148	3.304	2.769	0.204
X_3	-0.659	1.863	-0.353	-0.027
X_4	36.142	2.794	12.933	0.947

Table 74.15. Table of analysis of variance

Source of variation	SSq	DF	MSq	F-value
Due to regression	3250.89	3	1083.63	73.6452 **
Error	88.29	6	14.71	
Total	3339.17	9		

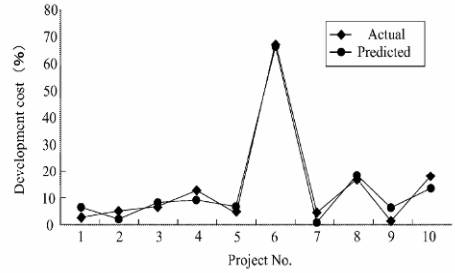


Figure 74.7. Accuracy for predicting the development cost

74.4. Relationship Between Product Quality and Development Cost

In the preceding section, we have shown the relationship between management process factors and the development cost (Y_2) instead of the number of faults (Y_1). Assuming that there is a logarithmic linearity relation between the number of faults and the development cost (Y_2), we conduct logarithmic linear regression analysis by using the mathematical expression:

$$Y_2 = a(1 + Y_1)^b. \tag{74.8}$$

Then, we have the estimated regression and 95% confidence limits as shown in Figure 74.8,

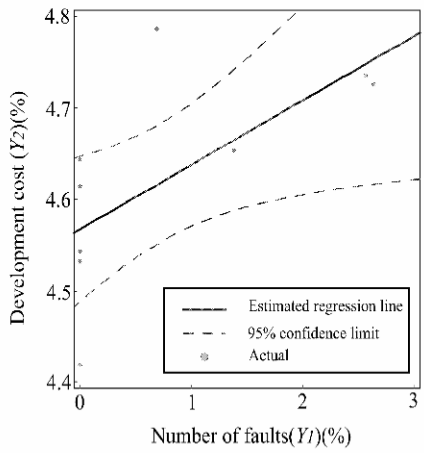


Figure 74.8. Relationship between the number of faults (Y_1) and the development cost (Y_2)

where the estimated parameters are given as $a = 0.07$ and $b = 4.57$.

As a result of analysis of variance, we find that the reliability of regression analysis is high as shown in Table 74.16. And we also have the estimated exponential curve in Figure 74.9, which shows the interdependency between the number of faults (Y_1) and the development cost (Y_2).

Table 74.16. Table of analysis of variance

Source of variation	SSq	DF	MSq	F-value
Due to regression	0.053	1	0.053	6.6489 *
Error	0.064	8	0.008	
Total	0.116	9		

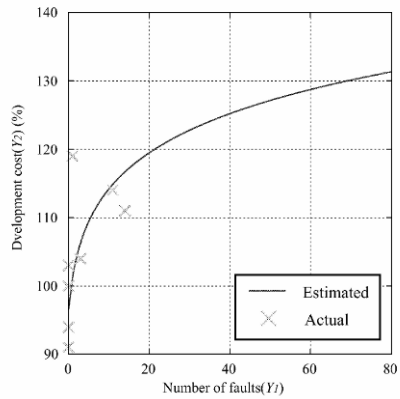


Figure 74.9. Estimated exponential curve

Table 74.17. General judgment

Project No.	Actual	Predicted	Score	1:(D^2)	1:(%)	2:(D^2)	2:(%)
Project 1	2	2	-12.966	27.130	0.001	1.198	75.351
Project 2	1	1	6.443	1.904	59.261	14.791	0.200
Project 3	2	2	-7.289	16.026	0.112	1.447	69.457
Project 4	2	2	-10.515	21.597	0.008	0.568	90.374
Project 5	1	1	6.073	5.471	14.037	17.618	0.053
Project 6	2	2	-15.589	36.890	0.000	5.712	12.649
Project 7	1	1	7.939	1.410	70.326	17.288	0.062
Project 8	1	1	13.887	2.385	49.640	30.158	0.000
Project 9	1	1	17.296	1.423	70.026	36.015	0.000
Project 10	1	1	17.900	2.483	47.842	38.282	0.000

74.5 Discriminant Analysis

A discriminant analysis is conducted by using the process data as shown in Table 74.8. Based on the same selected explanatory variables as the multiple regression analysis, X_2, X_3, and X_4 are selected for explanatory variables. The response variable for a discriminant analysis, Z, is defined as follows:

- Z=1: The software product released for user operation will experience no software failure.
- Z=2: The software product released for user operation will experience more than 0 of software failures.

Then, we have the estimated discriminant (for software product quality given by (74.9) as follows:

$$Z = -27.059X_2 + 2.588X_3 - 3.903X_4 + 13.745. \quad (74.9)$$

In order to check the goodness-of fit adequacy of our model, the Mahalanobis distance (D_2) is checked, and given as 39.519. Furthermore, the discrimination error rate has been checked, and given as 0.084. Therefore, the goodness-of-fit of this discriminant (is very high.

If the discrimination score in (74.9) is more than 0, the response variable is discriminated 1, otherwise 2. The discriminated response variables in (74.9 and actual measurement values are shown in Table 74.17 where we apply actual measurement values in all ten projects to the discriminated variables. Therefore, the discriminant (in (74.9) can judge whether or not the software project has a quality process with high accuracy.

74.6 Conclusion

In this chapter we have derived quality prediction models by using early-stage process measurement data. As a result of analysis of variance for quality assurance process factors, we have obtained a quality prediction model with five levels of significant. Based on the quality prediction model, we have found that the rate of design review delay and the frequency of review have an impact on product quality; that is, effective quality and review management can reduce the number of faults detected in the final testing.

As a result of analysis for management process factors, we have obtained a software management model with five levels of significance. Based on the software management model, we have found that the speed of risk mitigation and the frequency of review have an impact on the development cost on management activity. That is, it is very important to involve early-stage mitigation of risk and frequent review activities in software project management. Furthermore, we have been able to establish the relationship between product quality and the development cost.

Finally, based on the process data derived from effective management process factors, we have derived a discriminant expression that can judge whether or not the software project has a quality process.

Acknowledgements

The author is grateful to Dr. Toshihiko Fukushima of Nissin Systems Co., Ltd., and Mr. Masafumi Haramoto and Mr. Atsushi Fukuta of the Graduate School of Engineering, Tottori University, for their helpful suggestions. This work was supported in party by the Grant-in-Aid for Scientific Research (C), Grant No. 18510124, from the Ministry of Education, Culture, Sports, Science, and Technology of Japan.

References

[1] Yamada S. Software reliability modeling: fundamentals and applications (in Japanese). JUSE Press, Tokyo, 1994.

[2] Yamada S, Takahashi M. Introduction to software management model (in Japanese). Kyoritsu–Shuppan, Tokyo, 1993.

[3] Fukushima T Yamada S. Continuous improvement activities in software process. Proceedings of Software Japan 2004; 9–14.

[4] Fukushima T, M Ezaki, K Kobayashi, Yamada S. Software process improvement based on risk management activities (in Japanese). Proceedings of the 20th Symposium on Quality Control in Software Production. 2001; 265–272.

[5] Fukushima T, Yamada S. Measurement and assessment for software process improvement: Software project monitoring and management by using EV analysis (in Japanese). Proceedings of the 21st Symposium on Quality Control in Software Production 2002; 71–78.

[6] Fukushima T, Yamada S. The EVM and its effect to software project development. Proceedings of the Second International Conference on Project Management (ProMac2004). 2004; 665–670.

[7] Project Management Institute, Inc., Guide to the project management body of knowledge (PMBOK Guide), 2000 Edition, PMI, Tokyo, 2003.

[8] Fukushima T, Fukuta A, Yamada S. Early-stage product quality prediction by using software process data. Proceedings of the 11th ISSAT International Conference on Reliability and Quality in Design 2005; 261–265.

[9] Yamada S, Fukushima T. Quality-oriented software management (in Japanese). Morikita Publishing, Tokyo, 2007.

[10] Shigeru Y. Human factor analysis for software reliability in design-review process. International Journal of Performability Engineering. July 2006; 2(3): 223–232.

On the Development of Discrete Software Reliability Growth Models

P.K. Kapur[1], P.C. Jha[1] and V.B. Singh[2]

[1]Department of Operational Research, University of Delhi, Delhi
[2]Delhi College of Arts and Commerce, University of Delhi, Delhi

Abstract: In this chapter we discuss the software reliability growth models (SRGMs) that describe the relationship between the number of faults removed and the number of test cases used. Firstly we describe the discrete exponential and S-shaped models in a perfect debugging environment. We also discuss flexible discrete SRGM, which can depict either exponential or S-shaped growth curves, depending upon the parameter values estimated from the past failure data. Further, we describe an SRGM for the fault removal phenomenon in a perfect debugging environment. Most testing processes are imperfect in practice, therefore we also discuss a discrete model that incorporates the impact of imperfect debugging and fault generation into software reliability growth modeling. Faults in the software are generally not of the same type, rather the faults contained in a large software may differ from each other in terms of the amount of time and skill of the removal team required to remove them. Three discrete models: the generalized Erlang model, modeling severity of faults with respect to testing time, and a model with faults of different severity incorporating logistic learning function have been discussed. A discrete model in a distributed environment is also discussed. The above discrete SRGMs assume a constant fault detection rate while testing the software under consideration. In practice, however, the fault detection rate varies because of changes in the testing skill, the system environment, and the testing strategy used to test the software. SRGMs for the fault removal phenomenon, the generalized Erlang model, and the generalized Erlang model with logistic function are discussed, incorporating the concept of change point. It is also shown how equivalent continuous models can be derived. This chapter describes the state-of-the-art in discrete modeling.

75.1 Introduction

In the last two decades of the 20th century the proliferation of information technology has gone far beyond even the most outrageously optimistic forecasts. Consequently, computers and computer-based systems now pervade every aspect of our daily lives. While this has benefited society and increased our productivity, it has also made our lives more critically dependent on the correct functioning of these systems. There are already numerous instances where the failure of computer-controlled systems has led to colossal loss of human lives and money.

The successful operation of any computer system depends largely on its software components. The revolutionary advancement in the

computer technology has posed several challenges to the management of software crisis. In the early 1970s, the software engineering discipline emerged to establish and use sound engineering principles in order to economically obtain software systems that are not only reliable but also work efficiently in real machines, thus bringing the software development under the engineering umbrella. The immediate concern of software engineering was aimed at developing highly reliable software, scheduling and systematizing the software development process at reduced costs.

The most desirable attribute of software is quality. Using well-established software engineering methodologies developers can design high quality software. Software engineering is the discipline that aims to provide methods and procedures for developing quality software systems. There exist a number of models describing the software development process, commonly known as life cycle models. Most of the models model the SDLC in the following stages: requirement analysis and definition, system design, program design, coding, testing, and system delivery, maintenance. Even though highly skilled professionals develop software under an efficient management, the developer must measure the quality of software before release in order to provide guarantees and reduce the loss of finance and goodwill.

The testing phase is an extremely important stage of SDLC, in which around half the development resources are consumed. Testing consists of three successive stages: unit testing, integration testing, and system testing. In the phase test, cases that simulate the user environment are run on the software, and any departure from specifications or requirements is called a failure, and an effort is immediately an effort to remove the cause of that failure. Therefore, it is important to understand the failure pattern and faults causing the failures. Reliability is the most important quality metric used to measure the quality of software. It can provide vital information for the software release decision.

Many software reliability growth models (SRGMs) have been developed in the last two decades and can describe the reliability growth during the testing phase of the software development. Most of these models describe either exponential or S-shaped reliability growth curves. A large munber of proposed SRGMs are based on the non-homogeneous Poisson process (NHPP). NHPP based SRGMs are generally classified into two categories. The first category of the models, which use calendar/execution time as a unit of the failure/fault removal process, are known as continuous time SRGMs. The other category of models, which use the test cases as a unit of the failure/fault removal process, are known as discrete time SRGMs.

Among all SRGMs a large family of stochastic reliability models based on NHPP [11] reliability models, has been widely used. SRGMs based on NHPP are fault-counting models. Goel and Okumoto [2] have proposed NHPP based SRGM assuming that the failure intensity is proportional to the number of faults remaining in the software describing exponential failure curves. Ohba [21] refined the Goel–Okumoto model by assuming that the fault detection/removal rate increases with time, and that there are two types of faults in the software. The SRGM proposed in [1] has similar forms as that in [21], but is developed under a different set of assumptions. These models can describe both exponential and S-shaped growth curves and, therefore, are termed flexible models. Similar SRGMs that describe the failure phenomenon with respect to testing efforts have been developed in the literature [3], [20], and [22]. Models proposed in [5], [10], [11] and [18] incorporate some realistic issues such as imperfect debugging, fault generation and learning phenomenon of software testing team. Categorization of faults, faults of different severity, faults removal as two-stage and three-stage process, *etc*., has also been developed [17].

NHPP based SRGMs are generally classified into two groups. First, models that use the execution time (*i.e.*, CPU time) or calendar time. Such models are called continuous time models. Second, models, which use the test cases as a unit of fault removal period. Such models are called discrete time models [4], [9], and [20]. A test case can be a single computer test run executed in an hour, day, week, or even month. Therefore, it

includes the computer test run and the length of time spent on its execution. A large number of models have been developed in the first group, while there are fewer in the second group due to the difficulties in terms of the mathematical complexity involved. The utility of discrete reliability growth models cannot be underestimated. As the software failure data sets are discrete, these models many a time provide better fit than their continuous time counterparts. In this chapter, we discuss briefly several discrete SRGMs based on NHPP, developed in the literature.

75.1.1 Notation

a : Initial fault-content of the software

b : Constant fault removal rate *per* remaining fault *per* test case.

$m(n)$: The expected mean number of faults removed by the *n*th test case.

$m_f(n)$: The expected mean number of failures incurred by the *n*th test case.

$m_r(n)$: The expected mean number of removals incurred by the *n*th test case

d : Constant for rate of increase in delay

p : Proportion of leading faults in the software

$m_1(t)$: Expected number of leading faults detected in the interval (0, t].

$m_2(t)$: Expected number of dependent faults detected in the interval (0, t].

n : Number of test occasions.

a_i: Fault-content of type $_i$ and $\left(\sum_{i=1}^{k} a_i = a\right)$, where a is the total fault-content

b_i: Proportionality constant failure rate/fault isolation rate *per* fault of type i

$b_i(n)$: Logistic learning function, *i.e.*, fault removal rate *per* fault of type i

$m_{if}(n)$: Mean number of failure caused by fault-type i by n test cases.

$m_{ii}(n)$: Mean number of fault-isolated of fault-type i by n test cases.

$m_{ir}(n)$: Mean number of faults removed of fault-type i by n test cases.

β: Constant parameter in the logistic learning-process function.

$W(n)$: The cumulative testing resources spent up to the *n*th test run.

$w(n)$: The testing resources spent on the n^{th} test run

Definition: We define $t = n\delta$ and $\lim_{x \to 0} (1+x)^{\frac{1}{x}} = e$.

75.2 Discrete Software Reliability Growth Models

SRGM describes the failure or a removal phenomenon during the testing and operational phases. Using the data collected over a period of time of the on-going testing and based on some assumption of the testing environment, one can estimate the number of faults that can be removed by a specific time t and hence the reliability. Several discrete SRGMs have been proposed in literature under different sets of assumptions. Here we discuss and review briefly discrete SRGM based on NHPP.

The general assumptions of discrete NHPP based SRGM are:

1. The failure observation/fault removal phenomenon is modeled by NHPP with the mean value function $m(n)$.
2. Software is subject to failures during execution caused by faults remaining in the software.
3. Each time a failure is observed, an immediate effort takes place to remove the cause of failure.
4. The failure rate is equally affected by faults remaining in the software.

Under these general assumptions and some specific assumptions based on the testing environment different models are developed.

75.2.1 Discrete SRGM in a Perfect Debugging Environment

During the debugging process on a failure, the testing team reports the failure to the fault removal team (programmers), who identify the corresponding fault and make attempts to remove them. Most SRGM assume a perfect debugging environment, *i.e.*, whenever an attempt is made to remove a fault it is removed perfectly. However, in practical situations three possibilities are observed. First the fault is removed perfectly, secondly the fault is not removed perfectly due to which the fault content remains unchanged, known as imperfect fault debugging, and third, the fault is removed perfectly, but a new fault is generated during removal, known as fault generation. In the next section we discuss some discrete SRGMs that assume a perfect debugging environment. During the removal process, however, the testing team may remove some additional faults without these faults causing failure while removing an identified fault. These models are also discussed here

75.2.1.1 The Discrete Exponential Model [25]

Under the basic assumption, the expected cumulative number of faults removed between the nth and the (n+1)th test cases is proportional to the number of faults remaining after the execution of the nth test run , satisfies the following difference equation:

$$\frac{m(n+1)-m(n)}{\delta} = b(a-m(n)) \qquad (75.1)$$

Multiplying both sides of (75.1) by z^n and summing over n from 0 to ∞ , we get

$$\sum_{n=0}^{\infty} z^n m(n+1) - \sum_{n=0}^{\infty} z^n m(n) = ab\delta \sum_{n=0}^{\infty} z^n - b\delta \sum_{n=0}^{\infty} z^n m(n)$$

Solving the above difference equation under the initial condition $m(n=0)=0$ and using a probability generating function (PGF) given as

$$P(z) = \sum_{n=0}^{\infty} z^n m(n) \qquad (75.2)$$

we get the solution as

$$m(n) = a(1-(1-b\delta)^n) \qquad (75.3)$$

The model describes an exponential failure growth curve. The equivalent continuous SRGM [2] corresponding to (75.3), is obtained taking limit $\delta \to 0$

$$m(n) = a(1-(1-b\delta)^n) \to a(1-e^{-bt}) \qquad (75.4)$$

75.2.1.2 The Discrete Modified Exponential Model [25]

Assuming that the software contains two types of faults, type I and type II, we can write the differential equation corresponding to faults of each type as

$$\frac{m_1(n+1)-m_1(n)}{\delta} = b_1(a_1 - m_1(n)) \qquad (75.5)$$

and

$$\frac{m_2(n+1)-m_2(n)}{\delta} = b_2(a_2 - m_2(n)) \qquad (75.6)$$

where $a = a_1 + a_2$ and $b_1 > b_2$

On solving the above equation by the method of PGF we get

$$m_1(n) = a_1(1-(1-b_1\delta)^n)$$

$m_2(n) = a_2(1-(1-b_2\delta)^n)$, So

$$m(n) = m_1(n) + m_2(n) = \sum_{i=1}^{2} a_i(1-(1-b_i\delta)^n) \qquad (75.7)$$

The equivalent continuous SRGM proposed in [24] corresponding to (75.7), is obtained taking limit $\delta \to 0$.

$$m(n) = \sum_{i=1}^{2} a_i\left(1-(1-b_i\delta)^n\right) \to \sum_{i=1}^{2} a_i\left(1-e^{-b_i t}\right)$$

(75.8)

75.2.1.3 The Discrete Delayed S–shaped Model [6]

This model describes the debugging process in two phases. First, on the execution of a test case a failure is observed, and second, on a failure the corresponding fault is removed.

Accordingly, following the general assumptions of a discrete SRGM the testing process can be modeled as a two-stage process. The difference equations corresponding to each phase are given as

$$\frac{m_f(n+1)-m_f(n)}{\delta} = b(a-m_f(n)) \qquad (75.9)$$

and

$$\frac{m_r(n+1)-m_r(n)}{\delta} = b(m_f(n+1)-m_r(n)) \qquad (75.10)$$

Solving (75.9) by the method of PGF and the initial condition $m_f(n=0)=0$, we get

$$m_f(n) = a(1-(1-b\delta)^n) \qquad (75.11)$$

Substituting value of $m_f(n+1)$ from (75.11) in (75.10) and solving by the method of PGF with initial condition $m_r(n=0)=0$ we get

$$m_r(n) = a[1-(1+bn\delta)(1-b\delta)^n] \qquad (75.12)$$

The equivalent continuous SRGM corresponding to (75.12), is obtained taking limit $\delta \to 0$, *i.e.*,

$$m_r(n)=a[1-(1+bn\delta)(1-b\delta)^n] \to a(1-(1+bt)e^{-bt}) \qquad (75.13)$$

The continuous model is due to [23] and describes the delayed fault removal phenomenon.

75.2.1.4 The Modeling Fault Removal Phenomenon

The test team can remove some additional faults in the software, without these faults causing any failure during the removal of identified faults, although this may involve some additional effort. A fault that is removed consequent to a failure, is known as a leading fault, whereas the additional faults removed, which may have caused failures in future, are known as dependent faults. Models discussed in this section consider the effect of removing dependent faults while removing leading faults.

Discrete SRGM for the Fault Removal Phenomenon [15]

Under the assumption that while removing leading faults the testing team may remove some dependent faults, the difference equation for the model can be written as

$$m_r(n+1)-m_r(n)=b[a-m_r(n)]+\frac{c}{a}m_r(n+1)[a-m_r(n)] \qquad (75.14)$$

where b and c are the rates of leading and dependent fault detection, respectively.

Solving (75.14) by the method of PGF and initial condition $m(n=0)=0$, we have

$$m_r(n) = a\left[\frac{1-\{1-(b+c)\}^n}{1+\frac{c}{b}\{1-(b+c)\}^n}\right] \qquad (75.15)$$

If the difference equation (75.14) is rewritten as

$$\frac{m_r(n+1)-m_r(n)}{\delta}=b[a-m_r(n)]+\frac{c}{a}m_r(n+1)[a-m_r(n)] \qquad (75.16)$$

we get $$m_r(n) = a\left[\frac{1-\{1-\delta(b+c)\}^n}{1+\frac{c}{b}\{1-\delta(b+c)\}^n}\right] \qquad (75.17)$$

The equivalent continuous SRGM [5], corresponding to (75.17) is obtained taking, *i.e.,* limit $\delta \to 0$.

$$m_r(n)=a\left[\frac{1-\{1-\delta(b+c)\}^n}{1+\frac{c}{b}\{1-\delta(b+c)\}^n}\right] \to a\left[\frac{1-e^{-(b+c)t}}{1+\frac{c}{b}e^{-(b+c)t}}\right] \qquad (75.18)$$

Discrete SRGM with Fault Dependency using Lag Function [12]

This model is based on the assumption that there exists definite time lag between the detection of leading faults and the corresponding dependent faults. Assuming that the intensity of dependent fault detection is proportional to the number of dependent faults remaining in the software and the ratio of leading faults removed to the total leading faults, the difference equation for leading faults is given as

$$m_1(n+1)-m_1(n) = b[ap-m_1(n)] \qquad (75.19)$$

Solving (75.19) with the initial condition $m_1(n=0)=0$, we get

$$m_1(n) = ap\left[1-(1-b)^n\right] \qquad (75.20)$$

The dependent fault detection can be put as the following differential equation:

$$m_2(n+1)-m_2(n)=c[a(1-p)-m_2(n)]\frac{m_1(n+1-\Delta n)}{ap} \qquad (75.21)$$

where Δn is the lag depending upon the number of test occasions.

When $\Delta n = \log_{(1-b)^{-1}}(1 + dn)$, we get $m_2(n)$ under with the initial condition $m_2(n = 0) = 0$ as

$$m_2(n) = a(1-p)\left[1 - \prod_{i=1}^{n}\left\{1 - c\left(1 - (1-b)^{i}(1+(i-1)d)\right)\right\}\right] \quad (75.22)$$

Hence, the expected total number of faults removed in n test cases is

$$m(n) = a\left[1 - p(1-b)^{n} + (1-p)\prod_{i=1}^{n}\left\{1 - c(1-(1-b)^{i}(1+(i-1)d)\right\}\right] \quad (75.23)$$

The equivalent continuous SRGM due to [12] corresponding to discrete mean value function given by (75.23) is due to [2]

$$m(t) = a\left[1 - pe^{-bt} - (1-p)e^{-cf(t)}\right] \quad (75.24)$$

Where $f(t) = t + \frac{1}{b}(1+\frac{d}{b})(e^{-bt} - 1) + \frac{d}{b}te^{-bt}$

Discrete SRGM In an Imperfect Debugging Environment [18]

In this section we discuss discrete SRGM with two types of imperfect debugging, namely imperfect fault debugging and fault generation. During the removal process if a fault is repaired imperfectly we reencounter a failure on execution of the same input due to which the actual fault removal is less than the removal attempts. Therefore, the FRR is reduced by the probability of imperfect fault debugging. Besides, there is a good chance that some new faults will be introduced during removal. The difference equation for a discrete SRGM in an imperfect debugging environment incorporating two types of imperfect debugging and learning process of the testing team as testing progresses is given by:

$$\frac{m_r(n+1) - m_r(n)}{\delta} = b(n+1)\left(a(n) - m_r(n)\right) \quad (75.25)$$

Let us define

$$a(n) = a_0(1 + \alpha\delta)^n \quad (75.26)$$

$$b(n+1) = \frac{b_0 p}{1 + \beta(1 - b_0 p\delta)^{n+1}} \quad (75.27)$$

An increasing *a(n)* implies an increasing total number of faults, and thus reflects fault generation. Whereas, *b(n+1)* is a logistic learning function representing the learning of the testing team and is affected by the probability of fault removal on a failure.

Substituting the above forms of *a*(*n*) and b(*n+1*) in the difference equation (75.25) and solving by the PGF method, the closed form solution is

$$m_r(n) = \frac{a_0 b_0 p\delta}{1+\beta(1-b_0 p\delta)^n}\left[\frac{(1+\alpha\delta)^n - (1-b_0 p\delta)^n}{(\alpha\delta + b_0 p\delta)}\right] \quad (75.28)$$

where $mr(n = 0) = 0$ and $mr(n = \infty) = \infty$.

If the imperfect fault debugging parameter $p = 1$ and fault generation rate $\alpha = 0$, *i.e.*, the testing process is perfect, then *mr*(*n*) given by expression (75.28) reduces to

$$m_r(n) = a_0\left[\frac{1 - (1 - b_0\delta)^n}{1 + \beta(1 - b_0\delta)^n}\right] \quad (75.29)$$

which is perfect debugging discrete SRGM with logistic learning function. The equivalent continuous SRGM corresponding to (75.29) is obtained taking limit $\delta \to 0$

$$\frac{a_0 b_0 p\delta}{1+\beta(1-b_0 p\delta)^n}\left[\frac{(1+\alpha\delta)^n - (1-b_0 p\delta)^n}{(\alpha\delta + b_0 p\delta)}\right] \to \frac{a_0 b_0 p}{1+\beta e^{-b_0 p t}}\left[\frac{e^{\alpha t} - e^{-b_0 p t}}{\alpha + b_0 p}\right] \quad (75.30)$$

The equivalent continuous model is an extension of [6] with imperfect fault removal and fault generation [17]. Besides its interpretation as a flexible S-shaped fault removal model, this model has the exponential model [23] and the imperfect debugging model [13] as special cases.

75.2.2 Discrete SRGM with Testing Effort

During testing, resources such as manpower and time (computer time) are consumed. The failure, fault identification, and removal are dependent upon the nature and amount of resources spent. The time dependent behavior of the testing effort has been studied earlier in [3], [20], and [22] for continuous time models. exponential, Rayleigh, logistic, and Weibull functions are used to describe the relationship between the testing effort consumption and testing time (the calendar time). Here we discuss a discrete SRGM with testing

effort. Assuming $w(n)$ is described by a discrete Rayleigh curve, we may write

$$w(n+1) = W(n+1) - W(n) = \beta(n+1)\left[\alpha - W(n)\right] \quad (75.31)$$

Solving (75.31) using PGF, we get

$$W(n) = \alpha\left(1 - \prod_{i=0}^{n}(1 - i\beta)\right) \quad (75.32)$$

and hence

$$w(n) = \alpha\beta n\prod_{i=0}^{n-1}(1 - i\beta) \quad (75.33)$$

Under the above assumptions, the difference equation for the SRGM is written as

$$\frac{m(n+1) - m(n)}{w(n)} = b\left(a - m(n)\right) \quad (75.34)$$

Solving (75.34) using PGF we get [7]

$$m(n) = a\left(1 - \prod_{i=0}^{n}\left(1 - bw(i)\right)\right) \quad (75.35)$$

75.2.3 Modeling Faults of Different Severity

The SRGMs discussed above assume that the faults in the software are of the same type. This assumption implies that the fault removal rate *per* remaining fault is independent of the testing time. However, this assumption is not truly representative of reality. The faults contained in large software may differ from each other in terms of the amount of time and skill of the removal team required to remove the fault. Accordingly, the faults can be distinguished as simple (fault type I), hard (fault type II), complex faults (fault type III), and so on. In the next section we discuss the models conceptualizing the concept of faults of different severity.

75.2.3.1 Generalized Discrete Erlang SRGM [11]

Assuming that the software consists of n different types of faults and on each type of fault a different strategy is required to remove the cause of failure due to that fault. We assume that for a type i (i =I, II,..., k) fault, i different processes (stages) are required to remove the cause of failure. Accordingly we may write the following difference equations for faults of each type .

Modeling Simple Faults (Fault Type I)

The simple fault removal is modeled as a one-stage process

$$m_{i1}(n+1) - m_{i1}(n) = b_i(a_i - m_{i1}(n)) \quad (75.36)$$

Modeling Hard Faults (Fault Type II)

The harder type of faults is assumed to require more testing effort. The removal process for such faults is modelled as a two-stage process.

$$\begin{aligned} m_{i1}(n+1) - m_{i1}(n) &= b_i(a_i - m_{i1}(n)) \\ m_{i2}(n+1) - m_{i2}(n) &= b_i(m_{i1}(n+1) - m_{i2}(n)) \end{aligned} \quad (75.37)$$

Modeling Fault Type k

The modeling procedure of the hard fault can be extended to formulate a model that describes the removal of a fault type k with k stages of removal.

$$\begin{aligned} m_{i1}(n+1) - m_{i1}(n) &= b_i(a_i - m_{i1}(n)) \\ m_{ik}(n+1) - m_{ik}(n) &= b_i(m_{ik-1}(n+1) - m_{ik}(n)) \end{aligned} \quad (75.38)$$

The first subscript stands for the type of fault and the second subscript stands for the number of processes (stages).

Solving the above difference equation, we get

$$m_k(n) = m_{kk}(n) = a_k(1 - (1 - b_k)^n \left(\sum_{j=0}^{k-1}\frac{b_k^j}{j!(n+j)}\prod_{l=0}^{j}(n+l)\right) \quad (75.39)$$

Since $m(n) = \sum_{i=1}^{k} m_i(n)$, we get

$$m(n) = \sum_{i=1}^{k} a_i(1 - (1 - b_i)^n)\left(\sum_{j=0}^{i-1}\frac{b_i^j}{j!(n+j)}\prod_{l=0}^{j}(n+l)\right) \quad (75.40)$$

In particular, we have

$$m_1(n) = m_{11}(n) = m_1(1 - (1 - b_1)^n)$$

$$m_2(n) = m_{22}(n) = a_2(1 - (1 + b_2 n)(1 - b_2)^n) \text{ and}$$

$$m_3(n) = m_{33}(n) = a_3\left(1 - \left(1 + b_3 n + \frac{b_3^2 n(n+1)}{2}\right)(1 - b_3)^n\right)$$

The removal rate per fault for the above three types of faults is given as

$$d_1(n) = b, \qquad d_2(n) = \frac{b_2^2(n+1)}{b_2 n\delta + 1} \qquad \text{and}$$

$$d_3(n) = \frac{b_3^3(n^2+3n+2)}{2(b_3^2 \frac{n(n+1)}{2} + b_3 n + 1)}$$

respectively. We observe that $d_1(n)$ is constant with respect to n_1 while $d_2(n)$ and $d_3(n)$ increase with n and tend to b_2 and b_3 as $n \to \infty$. Thus in the steady state, $m_2(n)$ and $m_3(n)$ behave similarly to $m_1(n)$ and hence there is no loss of generality in assuming steady state rates b_2 and b_3 equal to b_1. Generalizing for arbitrary k, we can assume $b_1 = b_2 = ... = b_k = b$ (say). We thus have

$$m_k(n) \equiv m_{kk}(n) = a_k(1-(1-b)^n \left(\sum_{j=0}^{k-1} \frac{b^j}{j!(n+j)} \prod_{l=0}^{j} (n+l) \right)$$

(75.41)

and

$$m(n) = \sum_{i=1}^{k} a_i (1-(1-b)^n \left(\sum_{j=0}^{i-1} \frac{b^j}{j!(n+j)} \prod_{l=0}^{j} (n+l) \right) \quad (75.42)$$

The equivalent continuous time model [8], modeling faults of different severity is

$$m(t) = \sum_{i=1}^{k} a_i \left[1 - e^{-b_i t} \left(\sum_{j=0}^{i-1} \frac{(b_i t)^j}{j!} \right) \right] \quad (75.43)$$

which can be derived as a limiting case of discrete model substituting $t = n\delta$ and taking limit $\delta \to 0$.

Discrete SRGM with Faults of Different Severity Incorporating Logistic Learning Function [14]

Kapur *et al*., incorporated a logistic learning function during the removal phase, for capturing variability in the growth curves depending upon the environment it is being used and learning-process of the test team as the number of test run executed increases for modeling faults of different severity. Such a framework is very much suited for object-oriented programming and distributed development environments. Assuming that the software contains finite number of fault types and that the time delay between the failure observations and its subsequent removal represents the severity of the faults, the concept of faults of different severity can be modeled as follows:

Modeling the Simple Faults (i.e., Fault Type I)

The simple fault removal is modeled as a one-stage process

$$m_{1r}(n+1) - m_{1r}(n) = b_1(n+1)(a_1 - m_{1r}(n)) \quad (75.44)$$

where $b_1(n+1) = b_1$

Solving the above difference equation using the PGF with the initial condition, $m_{1r}(n=0)=0$, we get

$$m_{1r}(n) = a_1(1-(1-b_1)^n) \quad (75.45)$$

Modeling Hard Faults (Fault Type II)

The harder type of faults is assumed to take more testing effort. The removal process for such faults is modelled as a two-stage process,

$$m_{2f}(n+1) - m_{2f}(n) = b_2(a_2 - m_{2f}(n)) \quad (75.46)$$

$$m_{2r}(n+1) - m_{2r}(n) = b_2(n+1)(m_{2f}(n+1) - m_{2r}(n))$$

where $b_2(n+1) = \frac{b_2}{1+\beta(1-b_2)^{n+1}}$.

Solving the above system of difference equations using the PGF with the initial conditions $m_{2f}(n=0)=0$ and $m_{2r}(n=0)=0$ we get

$$m_{2r}(n) = a_2 \frac{1-(1-b_2 n)(1-b_2)^n}{1+\beta(1-b_2)^n} \quad (75.47)$$

Modeling Complex Faults (Fault Type III)

The complex fault removal process is modelled as a three-stage process,

$$m_{3f}(n+1) - m_{3f}(n) = b_3(a_3 - m_{3f}(n)) \quad (75.48)$$

$$\frac{m_{3i}(n+1) - m_{3i}(n)}{\delta} = b_3(m_{3f}(n+1) - m_{3i}(n)) \quad (75.49)$$

$$m_{3r}(n+1) - m_{3r}(n) = b_3(n+1)(m_{3i}(n+1) - m_{3r}(n)) \quad (75.50)$$

where $b_3(n+1) = \frac{b_3}{1+\beta(1-b_3)^{n+1}}$

Solving the above system of difference equations using the PGF with the initial conditions $m_{3f}(n=0)=0$, $m_{3i}(n=0)=0$ and $m_{3r}(n=0)=0$, we get

$$m_{3r}(n) = a_3 \frac{1-(1-b_3 n + \frac{b_3^2 n(n+1)}{2})(1-b_3)^n}{1+\beta(1-b_3)^n} \quad (75.51)$$

Modeling Fault Type k

The modeling procedure of the complex fault can be extended to formulate a model that describes the removal of a fault type *k* with *r* stages of removal.

$$m_{kf}(n+1)-m_{kf}(n)=b_k(a_k-m_{kf}(n)) \quad (75.52)$$

$$m_{kq}(n+1)-m_{kq}(n)=b_k(m_{kf}(n+1)-m_{kq}(n)) \quad (75.53)$$

$$m_{kr}(n+1)-m_{kr}(n)=b_k(n+1)(m_{k(r-1)}(n+1)-m_{kr}(n)) \quad (75.54)$$

where $b_k(n+1)=\dfrac{b_k}{1+\beta(1-b_k)^{r+1}}$

Solving the above system of difference equations using the PGF with the initial conditions, $m_{kf}(n=0)=m_{kf}(n=0)=m_{kr}(n=0)=0$, we get

$$m_{kr}(n)=a_k\frac{1-\left(1+\sum_{j=1}^{k-1}\frac{b_k^j}{j!(n+j)}\prod_{l=0}^{j}(n+l)\right)(1-b_k)^n}{(1+\beta(1-b_k)^n)} \quad (75.55)$$

Modeling the Total Fault Removal Phenomenon

The proposed framework is the superposition of the NHPP with mean value functions given in (75.45), (75.47), (75.51), and (75.55) Thus, the mean value function of the superposed NHPP is

$$m_{GF-k}(n)=\sum_{i=1}^{k}m_{ir}(n)=a_1(1-(1-b_1)^n)+\sum_{i=2}^{k}a_i\frac{1-\left(1+\sum_{j=1}^{i-1}\frac{b_i^j}{j!(n+j)}\prod_{l=0}^{j}(n+l)\right)(1-b_i)^n}{(1+\beta(1-b_i)^n)} \quad (75.56)$$

where $m_{GF-k}(n)$ provides the general framework with *k* types of faults.

The fault removal rate per fault for fault types 2 and 3 are given, respectively, as follows

$$d_1(n)=\frac{m_1(n+1)-m_1(n)}{a_i-m_1(n)}=b_i \quad (75.57)$$

$$d_2(n)=\frac{m_2(n+1)-m_2(n)}{a_2-m_1(n)}=\frac{b_2(1+\beta+b_2n)-b_2(1+\beta(1-b_2)^n)}{(1+\beta(1-b_2)^n)(1+\beta+b_2n)} \quad (75.58)$$

$$d_3(n)=\frac{b_3(1+\beta+b_3n+\frac{b_3^2n(n+1)}{2})-b_3(1+\beta(1-b_3)^n)(1+b_3n)}{(1+\beta(1-b_3)^n)(1+\beta+b_3n+\frac{b_3^2n(n+1)}{2})} \quad (75.59)$$

It is observed that $d_1(n)$ is constant with respect to *n,* while $d_2(n)$ and $d_3(n)$ increase monotonically with *n* and tend to constants b_2 and b_3 as $n\to\infty$. Thus, in the steady state, $m_{2r}(n)$ and $m_{3r}(n)$ behave similarly to $m_{1r}(n)$ and hence there is no loss of generality in assuming the steady state rates b_2 and b_3 to be equal to b_1. After substituting $b_2=b_3=b_1$ in the right hand side of (75.58) and (75.59), one can see that $b_1>d_2(n)>d_3(n)$, which is in accordance with the severity of the faults. Generalizing for arbitrary *k,* assuming $b_1=b_2=b_k=b$ (say) we may write (75.56) as follows:

$$m_{GF-k}(n)=\sum_{i=1}^{n}m_{ir}(n)=a_1\left(1-(1-b)^n\right)+\sum_{i=2}^{k}a_i\frac{1-\left(1+\sum_{j=1}^{i-1}\frac{b^j}{j!(n+j)}\prod_{l=1}^{j}(n+l)\right)(1-b)^n}{(1+\beta(1-b)^n)} \quad (75.60)$$

The equivalent continuous time model, modeling faults of different severity is

$$m_{GF-k}(t)=\sum_{i=1}^{n}m_{ir}(t)=a_1\left(1-e^{-bt}\right)+\sum_{i=2}^{k}a_i\frac{1-\left(\sum_{j=0}^{k-1}\frac{(bt)^j}{j!}\right)e^{-bt}}{(1+\beta e^{-bt})} \quad (75.61)$$

which can be derived as a limiting case of discrete model substituting $t=n\delta$ and taking, *limit* $\delta\to 0$.

75.2.3.2 Discrete SRGM Modeling Severity of Faults With Respect to Testing Time [17]

Faults can be categorized on the basis of their time to detection. During testing the faults, which are easily detected at the early stages of testing, are called simple faults or trivial faults. However, as the complexity of faults increases, so does the

detection time. Faults, which take maximum time for detection, are termed as complex faults.

For classification of faults, first we define non-cumulative instantaneous fault detection function $f(n)$ using discrete SRGM for fault removal phenomenon discussed in Section 75.2.1.4, which is given by first order difference equation of $m(n)$.

$$f(n)=\Delta m(n)=\frac{m(n+1)-m(n)}{\delta}= \frac{\overline{N}p(p+q)^2\left[1-\delta(p+q)\right]^n}{\left[p+q\left(1-\delta(p+q)\right)^n\right]\left[p+q\left(1-\delta(p+q)\right)^{n+1}\right]} \quad (75.62)$$

Above, $f(n)$ defines the mass function for non-cumulative fault detection. It takes the form of a bell-shaped curve and represents the rate of fault removal for n.

The peak of $f(n)$ occurs when

$$n=\begin{cases}[n^*] & \text{if } f[n^*])\geq f([n^*]+1)\\ [n^*]+1 & \text{otherwise}\end{cases} \quad (75.63)$$

Where $n^* = \dfrac{\log(p/q)}{\log(1-\delta(p+q))}-1$

and $\left[n^*\right]=\left\{n:\max\left(n\leq n^*\right),n\in Z\right\}$

Then as $\delta\to\mathbf{0}$, *i.e.* n^* converges to the inflection point of continuous S-shaped SRGM [5]

$$t^*=\frac{\delta\log(p/q)}{\log\left(1-\delta(p+q)\right)}-\delta \to -\frac{\log(p/q)}{p+q} \qquad as\,\delta\to 0$$

The corresponding $f(n^*)$ is given by

$$f(n^*)=\frac{\overline{N}(p+q)^2}{2q\left(2-\delta(p+q)\right)}\to f(t^*)=\frac{\overline{N}(p+q)^2}{4q}\ \text{s}\ \delta\to 0$$

The curve for $f(n)$, the non-cumulative fault detection is symmetric about point n^* up to $2n^*+1$.

Here $f(0)=f\left(2n^*+1\right)=\overline{N}p/\left(1-\delta q\right)$

As $\delta\to\mathbf{0}, f(t)$ is symmetric about t^* up to $2t^*$ then, $f(t=\mathbf{0})=f\left(\mathbf{2}t^*\right)=\overline{N}p$

To get the insight into type of trend shown by $f(n)$, we need to find $\Delta f(n)$, *i.e.*, the rate of change in non-cumulative fault detection $f(n)$.

$$\Delta f(n)=\frac{f(n+1)-f(n)}{\delta}=\frac{f_1}{f_2},\ \text{where}$$

$$f_1=-\overline{N}p(p+q)^3\left[1-\delta(p+q)\right]^n.\left[p-q\left(1-\delta(p+q)\right)^{n+1}\right] \quad (75.64)$$

$$f_2=\left[p+q\left(1-\delta(p+q)\right)^n\right]\left[p+q\left(1-\delta(p+q)\right)^{n+1}\right].\left[p+q\left(1-\delta(p+q)\right)^{n+2}\right]$$

Here we observe that the fault removal rate increases for (0, n_1^*) with increasing rate and decreasing rate for (n_1^*+1 to n^*). This is because of the fact that as the testing grows, so does the skill of the testing term. The faults detected during (0, n_1^*) are relatively easy faults, while those detected during (n_1^*+1, n^* n^*) are relatively difficult faults. The trend shown by $f(n)$ can be summarized as in Table 75.1

Table 75.1. The trend shown by $f(n)$

No. of test cases	Trends in $f(n)$
Zero to n_1^*	Increasing at an increasing rate
n_1^*+1 to n^*	Increasing at a decreasing
$n^*+\mathbf{1}$ to n_2^*	Decreasing at an increasing rate
n_2^*+1 to ∞	Decreasing at a decreasing rate

In Table 75.1 n^* is the point of maxima for $f(n)$. For (n_1^*+1, n_2), the fault detection rate decreases, *i.e.*, a fewer number of faults are detected upon failure. These faults can be defined as relatively hard faults. For (n_2^*+1, ∞), very few faults are detected upon failure. So testing is terminated. Faults detected beyond n_2^*+1 are relatively

complex faults. The results are summarized in Table 75.2. Here, n_1^* and n_2^* are points of inflection for $f(n)$.

Point of Maxima of Δf(n)

$$n_1^* = \begin{cases} [n_1] & \text{if } \Delta f[n_1]) \geq \Delta f([n_1]+1) \\ [n_1]+1 & \text{otherwise} \end{cases} \quad (75.65)$$

where

$$n_1 = \frac{1}{\log(1-\delta(p+q))} \log\left[\frac{p}{q}\left\{\frac{g_1}{(1-\delta(p+q))}\right\}\right] - 1$$

$$\text{where } g_1 = (2-\delta(p+q)) + \sqrt{(1-\delta(p+q))^2 + (2-\delta(p+q))}$$

And $[n_1] = \{n \mid \max(n \leq n_1), n \in Z\}$

Point of Minima of Δf(n)

$$n_2^* = \begin{cases} [n_2] & \text{if } \Delta f[n_2]) \geq \Delta f([n_2]+1) \\ [n_2]+1 & \text{otherwise} \end{cases} \quad (75.66)$$

where

$$n_2 = \frac{1}{\log(1-\delta(p+q))} \log\left[\frac{p}{q}\left\{\frac{g_1}{(1-\delta(p+q))}\right\}\right] - 1$$ and

$$g_{1=}(2-\delta(p+q)) - \sqrt{\left(1-\left(\overline{p+q}\right)\delta\right)^2 + (2-\delta(p+q))}$$

$$[n_2] = \{n \mid \max(n \leq n_2), n \in Z\}$$

Table 75.2. Size of each fault category

No. of test cases	Fault category	Expression for the fault category size
0 to n_1^*	Easy faults	$m(n_1)$
n_1^*+1 to n^*	Difficult faults	$m(n^*) - m(n_1)$
$n^* + 1$ to n_2^*	Hard faults	$m(n_2) - m(n^*)$
Beyond n_2^*	Complex fault	$\overline{N} - m(n_2)$

It may be noted that the corresponding inflection points T_1 and T_2, for the continuous case can be derived from n_1 and n_2 as δ→0, *i.e.*,

$$n_1 \to T_1 = \frac{-1}{p+q} \log\left(\frac{p}{q}(2+\sqrt{3})\right) \qquad s \quad \delta \to 0$$

75.2.4 Discrete Software Reliability Growth Models for Distributed Systems [16]

Computing has now reached the state of distributed computing, which is built on the following three components: (a) personal computers, (b) local and fast wide area networks, and (c) system and application software. By amalgamating computers and networks into one single computing system, and providing appropriate system software, a distributed computing system has created the possibility of sharing information and peripheral resources. Furthermore, these systems have improved the performance of a computing system and individual users. Distributed computing systems are also characterized by enhanced availability and increased reliability. A distributed development project with some or all of the software components generated by different teams presents complex issues of quality and reliability of the software.

The SRGM for distributed development environment discussed in this section considers that software system consists of finite number of reused and newly developed components and takes into account the time lag between the failure and fault isolation/removal processes for the newly developed components. The fault removal rate of the reused sub-system is proportionality constant, and the fault removal rate of newly developed sub-system is a discrete logistic learning function, as it is expected the learning process will grow with time.

Additional Notation

a_i : Initial fault content of type i reused component.

a_j : Initial fault content of type j newly developed components with hard faults.

a_k : Initial fault content of type *k* newly developed component with complex faults.

b_i : Proportionality constant failure rate *per* fault of *i*th reused component.

b_j : Proportionality constant failure rate *per* fault of *j*th newly developed component.

b_k : Proportionality constant failure rate *per* fault of *k*th newly developed component.

$b_j(n)$: Fault removal rate *per* fault of *j*th newly developed component.

$b_k(n)$:Fault removal rate *per* fault of *k*th newly developed component.

$m_{ir}(n)$:Mean number of faults removed from *i*th reused component by *n* test cases.

$m_j f(n)$:Mean number of failures caused by *j*th newly developed component by n test cases.

$m_{jr}(n)$:Mean number of faults removed from *j*th newly developed component by n test cases.

$m_k f(n)$:Mean number of failures caused by *k*th newly developed component by n test cases.

$m_k u(n)$:Mean number of faults isolated from *k*th newly developed component by n test cases.

$m_k r(n)$:Mean number of faults removed from *k*th newly developed component by *n* test cases.

75.2.4.1 Modeling the Fault Removal of Reused Components Modeling

Simple Faults

Fault removal of reused components is modeled as one-stage processes

$$\frac{m_{ir}(n+1)-m_{ir}(n)}{\delta} = b_i(n+1)\left(a_i - m_{ir}(n)\right)$$

$$\text{Where } b_i(n+1) = b_i \tag{75.67}$$

Solving the above difference equation using PGF with the initial condition $m_{ir}(n = 0) = 0$, we get

$$m_{ir}(n) = a_i\left(1-(1-\delta b_i)^n\right) \tag{75.68}$$

75.2.4.2 Modeling the Fault Removal of Newly Developed Components

Software faults in the newly developed software component can be of different severity. Time required for fault removal depends on the severity of faults. The faults can either be modeled as two stage or three-stage process according to the time lag for removal.

Components Containing Hard Faults

The removal process for hard faults is modeled as a a two-stage process, given as

$$\frac{m_{jf}(n+1)-m_{jf}(n)}{\delta} = b_j\left(a_j - m_{jf}(n)\right) \tag{75.69}$$

$$\frac{m_{jr}(n+1)-m_{jr}(n)}{\delta} = b_j(n+1)\left(m_{jf}(n+1)-m_{jr}(n)\right)$$

where

$$b_j(n+1) = b_j \Big/ \left(1+\beta(1-b_j)^{n+1}\right) \tag{75.70}$$

Solving the above system of difference equations using PGF with the initial conditions $m_{if}(n = 0) = 0$ and $m_{jr}(n = 0) = 0$, we get

$$m_{jr}(n) = a_j \frac{1-\left(1+\delta b_j n\right)\left(1-\delta b_j\right)^n}{1+\beta\left(1-b_j\right)^n} \tag{75.71}$$

Components Containing Complex Faults

There can be components having still harder faults or complex faults. These faults can require more effort for removal after isolation. Hence they need to be modeled with greater time lag between failure observation and removal. The third stage added below to the model serves the purpose.

$$\frac{m_{kf}(n+1)-m_{kf}(n)}{\delta} = b_k\left(a_k - m_{kf}(n)\right) \tag{75.72}$$

$$\frac{m_{ku}(n+1)-m_{ku}(n)}{\delta} = b_k\left(m_{kf}(n+1)-m_{ku}(n)\right) \tag{75.73}$$

$$\frac{m_{kr}(n+1)-m_{kr}(n)}{\delta} = b_k(n+1)\left(m_{ku}(n+1)-m_{kr}(n)\right)$$

$$\text{where } b_k(n+1) = \frac{b_k}{1+\beta(1-b_k)^{n+1}} \tag{75.74}$$

Solving the above system of difference equations using PGF with the initial conditions $m_{kf}(n = 0) = 0$, $m_{ku}(n = 0) = 0$ and $m_{kr}(n = 0) = 0$, we get

$$m_{kr}(n) = a_3 \frac{1-\left(1+b_k n\delta+\left(b_k^2 n\delta(n+1)\delta\right)/2\right)(1-\delta b_k)^n}{1+\beta(1-b_k)^n} \quad (75.75)$$

Modeling the Total Fault Removal Phenomenon

The model is the superposition of the NHPP of "*p*" reused and "*q*" newly developed components with hard faults and "*s*" newly developed components with complex faults with the mean value function of superposed NHPP being:

$$m(n) = \sum_{i=1}^{p} m_{ir}(n) + \sum_{j=p+1}^{p+q} m_{jr}(n) + \sum_{k=p+q+1}^{p+q+s} m_{kr}(n) \text{ Or}$$

$$m(n) = \sum_{i=1}^{p} a_i \left(1-(1-\delta b_i)^n\right) + \sum_{j=p+1}^{p+q} a_j \frac{1-(1+\delta b_j n)(1-\delta b_j)^n}{1+\beta(1-b_j)^n}$$

$$+ \sum_{k=p+q+1}^{p+q+s} a_k \frac{1-\left(1+\delta b_k n+\frac{b_k^2 n\delta(n+1)\delta}{2}\right)(1-\delta b_k)^n}{1+\beta(1-b_k)^n} \quad (75.76)$$

where $\sum_{i=1}^{p+q+s} a_i = a$ (the total fault content of the software). Note that a distributed system can have any number of used and newly developed components.

The equivalent continuous model can be derived (75.76) taking limit $\delta \to 0$, [11], *i.e.*

$$m(n) \to m(t) = \left(\sum_{i=1}^{p} a_i\left(1-e^{-bt}\right) + \sum_{j=p+1}^{p+q} a_j \frac{1-(1+bt)e^{-bt}}{1+\beta e^{-bt}} + \sum_{k=p+q+1}^{p+q+s} a_k \frac{g_1}{1+\beta e^{-bt}},\right)$$

$$\text{where } g_1 = 1-\left(1+bt+\left(b^2 t^2\right)/2\right)e^{-bt} \quad (75.77)$$

75.2.5 Discrete SRGM with Change Points

The discrete SRGMs discussed above assume a constant fault detection rate, duing testing the software under consideration. Whereas, in practice, the fault detection rate varies because of change in the testing skill, the system environment, and the testing strategy used to test the software. Several questions arise: Has a change occurred? Has more than one change occurred? When did the change occur? These questions can be answered by performing a change-point analysis. A change-point analysis is capable of detecting changes. The change point characterizes the changes and controls the overall fault rate.

75.2.5.1 Discrete SRGM with a Change Point for the Fault Removal Phenomenon [19]

The delayed S-shaped discrete SRGM discussed in Section 75.2.1.3 due to Yamada *et al*., can be derived alternatively in one stage as follows

$$\frac{m_r(n+1) - m_r(n)}{\delta} = b(n)\left(a - m_r(n)\right)$$

$$\text{Where } b(n) = \frac{b^2(n+1)}{1+bn} \quad (75.78)$$

However, to incorporate the concept of change point into software reliability growth modeling it is assumed that the fault detection rate during testing may vary. As a consequence, the fault detection rate before the change point is different from the fault detection rate after the change point. Under this basic assumption, the expected cumulative number of faults removed between the *n*th and the $(n+1)$th test cases is proportional to the number of faults remaining after the execution of the *n*th test run , satisfies the following difference equation:

$$\frac{m(n+1) - m(n)}{\delta} = b(n)\left(a - m(n)\right) \quad (75.79)$$

where

$$b(n) = \frac{{b_1}^2(n+1)}{1+b_1 n}; \; 0 \le n < \eta_1 \quad (75.80)$$

$$b(n) = \frac{{b_2}^2(n+1)}{1+b_2 n}; \quad n \ge \eta_1 \quad (75.81)$$

Case 1: ($\mathbf{0 \le n < \eta_1}$*)*

Solving the difference equation (75.79), substituting *b(n)* from (75.80), and using the probability generating function under the initial condition at $n = 0$, $m(n) = 0$, we get

$$m(n) = a\left(1-\left(1+\delta b_1 n\right)\left(1-\delta b_1\right)^n\right) \quad (75.82)$$

The equivalent continuous model of (75.82) can be derived taking *limit* $\delta \to 0$, *i.e.*

$$m(n) = a\left(1-(1+\delta b_1 n)(1-\delta b_1)^n\right) \to a\left(1-(1+bt)e^{-bt}\right)$$

Case 2: ($n \geq \eta_1$)

Solving the difference equation (75.79) substituting *b(n)* from (75.81), and using the probability generating function with the initial condition at $n = \eta_1$, $m(n) = m(\eta_1)$, we get

$$m(n) = a\left[1-\frac{(1+\delta b_1 \eta_1)}{(1+\delta b_2 \eta_1)}(1+\delta b_2 n)(1-\delta b_2)^{(n-\eta_1)}(1-\delta b_1)^{\eta_1}\right] \quad (75.83)$$

The equivalent continuous of (75.83) can be derived taking limit $\delta \to 0$, *i.e.*

$$m(n) \to m(t) = a\left(1-\left(\frac{1+b_1 t_1}{1+b_2 t_1}\right)(1+b_2 t)\, e^{-(b_1 t_1 + b_2 (t-t_1))}\right)$$

75.2.5.2 Discrete SRGM with a Change Point for Modeling Faults of Different Severity

There are many factors that affect software testing. These factors are unlikely to be kept stable during the entire process of software testing, with the result that the underlying statistics of the failure process is likely to experience major changes. The fault detection rate for all the faults lying in the software differs on the basis of their severity. Therefore there is the need to define the different fault detection rates to cater the faults of different severity. In most NHPP software reliability growth models, the fault detection rate is constant. However, during the testing, the fault detection rate can change at some point, say n_1, n_2. The concept of the change point is introduced in the generalized Erlang model, see Section 75.2.4.1, and the generalized Erlang model with logistic function, see Section 75.2.4.2. The position of the change point can be judged by the graph of actual failure data.

Discrete SRGM with a Change Point for the Generalized Erlang Model

The model is described by the following difference equation:

$$m(n+1) - m(n) = b(n)\left(a - m(n)\right) \quad (75.84)$$

where

$$b(n+1) = b_1; \quad 0 \leq n < \eta_1 \quad (75.85)$$

$$b(n+1) = \frac{b_2{}^2 (n+1)}{1 + b_2 n}; \quad n_1 < n \leq n_2 \quad (75.86)$$

$$b(n+1) = \frac{\frac{b_3{}^2 (n+1)(n+2)}{2}}{1 + b_3 n + \frac{b_3{}^2 (n+1)(n+2)}{2}}; \quad n > n_2 \quad (75.87)$$

Case 1: $\mathbf{0} \leq n \leq n_1$

Solving the difference equation (75.84) substituting *b(n)* from (75.85), using the PGF with the initial condition at $n = 0$, $m(n) = 0$, we get

$$m(n) = a\left[\mathbf{1} - (\mathbf{1} - b_1)^n\right] \quad (75.88)$$

Case 2: $n_1 < n \leq n_2$

Solving the difference equation (75.84) substituting *b(n)* from (75.86), using the probability generating function with the initial condition at $n = \eta_1$, $m(n) = m(\eta_1)$, we get

$$m(n) = a\left[1-\left(\frac{1+b_2 n}{1+b_2 n_1}\right)(1-b_1)^{n_1}(1-b_2)^{n-n_1}\right] \quad (75.89)$$

Case 3: $n > n_2$

Further solving the difference equation (75.84) substituting *b(n)* from (75.87), using the probability generating function with the initial condition $n = n_2$, $m(n) = m(n_2)$ we get

$$m(n) = a\left[1-\left(\frac{1+b_2 n_2}{1+b_2 n_1}\right)\left(\frac{1+b_3 n + \frac{b_3{}^2 n(n+1)}{2}}{1+b_3 n_2 + \frac{b_3{}^2 n_2 (n_2+1)}{2}}\right)\cdot (1-b_1)^{n_1}(1-b_2)^{n_2-n_1}(1-b_3)^{n-n_2}\right] \quad (75.90)$$

Modeling the Total Fault Removal Phenomenon

The model framework is the superposition of NHPP with mean value functions given in (75.88), (75.89), and (75.90). Thus, the mean value function of the superposed NHPP is

$$m(n) = m_1(n) + m_2(n) + m_3(n) \quad (75.91)$$

$$\text{or}\quad m(n)=a_1\left[1-(1-b_1)^n\right]+a_2\left[1-\left(\frac{1+b_2n}{1+b_2n_1}\right)(1-b_1)^{n_1}(1-b_2)^{n-n_1}\right]$$
$$+a_3\left[1-\left(\frac{1+b_2n_2}{1+b_2n_1}\right)\left(\frac{1+b_3n+\frac{b_3^2n(n+1)}{2}}{1+b_3n_2+\frac{b_3^2n_2(n_2+1)}{2}}\right)(1-b_1)^{n_1}(1-b_2)^{n_2-n_1}(1-b_3)^{n-n_2}\right] \quad (75.92)$$

where $a_1 + a_2 + a_3 = a$.

Discrete SRGM with a Change Point for the Generalized Erlang Model with Logistic Function

The model is described by the following difference equation:

$$m(n+1)-m(n)=b(n)\left(a-m(n)\right) \quad (75.93)$$

$$\text{where } b(n+1)=b_1;\quad 0\le n<\eta_1 \quad (75.94)$$

$$b(n+1)=\frac{b_2\left(1+\beta+b_2n\right)-b_2\left(1+\beta(1-b_2)^{n+1}\right)}{\left(1+\beta+b_2n\right)\left(1+\beta(1-b_2)^{n+1}\right)};\quad n_1<n\le n_2 \quad (75.95)$$

$$b(n+1)=\frac{b_3\left(1+\beta+b_3n+\frac{b_3^2n(n+1)}{2}\right)-g_1}{\left(1+\beta+b_3n+\frac{b_3^2n(n+1)}{2}\right)\left(1+\beta(1-b_3)^{n+1}\right)};\quad n>n_2$$
$$where\quad g_1=b_3\left(1+\beta(1-b_3)^{n+1}\right)(1+b_3n) \quad (75.96)$$

Case 1: $0 \le n \le n_1$

Solving the difference equation (75.93) substituting *b(n)* from (75.94), using the PGF with the initial condition at $n = 0$, $m(n) = 0$, we get

$$m(n)=a\left[1-(1-b_1)^n\right] \quad (75.97)$$

Case 2: $n_1 < n \le n_2$

Solving the difference equation (75.93) substituting *b(n)* from (75.95), using the probability generating function with the initial condition at $n = \eta_1$, $m(n) = m(\eta_1)$ we get

$$m(n)=a\left[1-\left(\frac{1+\beta(1-b_2)^{n_1}}{1+\beta(1-b_2)^n}\right)\left(\frac{1+\beta+b_2n}{1+\beta+b_2n_1}\right)(1-b_1)^{n_1}(1-b_2)^{n-n_1}\right] \quad (75.98)$$

Case 3: $n > n_2$

Further solving the difference equation (75.93) substituting $b(n)$ from (75.96), using the PGF with the initial condition $n = n_2$, $m(n) = m(n_2)$ we get

$$m(n)=a\left[1-\left(\frac{1+\beta(1-b_2)^{n_1}}{1+\beta(1-b_2)^{n_2}}\right)\left(\frac{1+\beta(1-b_3)^{n_2}}{1+\beta(1-b_3)^n}\right)\left(\frac{1+\beta+b_3n+\frac{b_3^2n(n+1)}{2}}{1+\beta+b_3n_2+\frac{b_3^2n_2(n_2+1)}{2}}\right)\left(\frac{1+\beta+b_2n_2}{1+\beta+b_2n_1}\right)(1-b_1)^{n_1}(1-b_2)^{n_2-n_1}(1-b_3)^{n-n_2}\right] \quad (75.99)$$

Modeling the Total Fault Removal Phenomenon

The model framework is the superposition of the NHPP with mean value functions given in (75.97), (75.98), and (75.99). Thus, the mean value function of the superposed NHPP is

$$m(n) = m_1(n) + m_2(n) + m_3(n) \quad (75.100)$$

or

$$m(n)=a_1\left[1-(1-b_1)^n\right]+a_2\left[1-\left(\frac{1+\beta(1-b_2)^{n_1}}{1+\beta(1-b_2)^n}\right)\left(\frac{1+\beta+b_2n}{1+\beta+b_2n_1}\right)(1-b_1)^{n_1}(1-b_2)^{n-n_1}\right]$$
$$+a_3\left[1-\left(\frac{1+\beta(1-b_2)^{n_1}}{1+\beta(1-b_2)^{n_2}}\right)\left(\frac{1+\beta(1-b_3)^{n_2}}{1+\beta(1-b_3)^n}\right)\left(\frac{1+\beta+b_3n+\frac{b_3^2n(n+1)}{2}}{1+\beta+b_3n_2+\frac{b_3^2n_2(n_2+1)}{2}}\right)\left(\frac{1+\beta+b_2n_2}{1+\beta+b_2n_1}\right)(1-b_1)^{n_1}(1-b_2)^{n_2-n_1}(1-b_3)^{n-n_2}\right] \quad (75.101)$$

where $a_1 + a_2 + a_3 = a$.

75.3 Conclusion

In this chapter we have discussed a wide range of discrete SRGMs, which describe the relationship between the number of faults removed and the number of test cases used. These include flexible discrete SRGMs in perfect and imperfect debugging environments. A new discrete model is also introduced, which incorporates the effect of imperfect debugging and fault generation. Another category of SRGMS incorporating faults of

different severity and distributed environment is also been discussed. Lastly, SRGM incorporating the concept of the change point has been introduced. The chapter describes the state-of-the-art in the discrete modeling. release time problem, Allocation and control of testing resources have so far not been discussed in the literature. The authors propose to bring them out in their future research effort.

References

[1] Bittanti S, Blonzera P, Pedrotti E, Pozzi M. Scattolini A, a flexible modeling approach in software reliability growth. In: Goos G, Hartmanis, editors. Software reliability modeling and identification. Springer, Berlin, 1988; 101–140.

[2] Goel AL, Okumoto K. Time dependent fault detection rate model for software reliability and other performance measures. IEEE Transactions on Reliability 1979; R-28 (3):206–211.

[3] Huang C-Y, Kuo S-Y, Chen JY. Analysis of a software reliability growth model with logistic testing effort function. Proceedings 8th International Symposium on Software Reliability Engineering, IEEE Computer Society, Washington, DC, USA 1997; 378–388.

[4] Inoue S, Yamada S. Discrete software reliability assessment with discretized NHPP models. Computer and Mathematics with Applications 2006; 51(2):161–170.

[5] Kapur PK, Garg RB. A software reliability growth model for a fault removal phenomenon. Software Engineering Journal 1992; 7: 291–294.

[6] Kapur PK, M Bai, Bhushan S. Some stochastic models in software reliability based on NHPP. In: Venugopal N, editor. Contribution to stochastic. Wiley Eastern Limited, New Delhi, 1992.

[7] Kapur PK, Xie M, Garg RB, Jha AK, A discrete software reliability growth model with testing effort. Proceedings First International Conference on Software Testing, Reliability and Quality Assurance (STRQA), IEEE Computer Society , New Delhi, India 1994; Dec 21–22: 16–20.

[8] Kapur PK, Younes S, Agarwala S. Generalized erlang software reliability growth model. ASOR Bulletin, 1995; 14(1):5–11.

[9] Kapur PK, Younes S. A general discrete software reliability growth model. Operations Research – Theory and practice. Spaniel Publishers, New Delhi, 1995.

[10] Kapur PK, Younes S. Modeling an imperfect debugging phenomenon in software reliability. Microelectronics and Reliability 1996; 36(5): 645–650.

[11] Kapur PK, Garg RB, Kumar S. Contributions to hardware and software reliability. World Scientific, Singapore, 1999.

[12] Kapur PK, Bardhan AK, Shatnawi O. Software reliability growth model with fault dependency using lag function. Verma AK. Editor. Proceedings of International Conference on Quality ,Reliability and Control (in Communication and Information Systems) ICQRC-2001, Organised by IETE Mumbai Centre and IIT Bombay , Mumbai ,2001; December 27-28, R53: 1–7.

[13] Kapur PK. Shatnawi O, Singh O. Discrete imperfect software reliability growth models under imperfect debugging environment. Rajaram NJ, Verma AK (Editors) Proceedings of the International Conference on Multimedia and Design; organized by Arena Multimedia and IIT, Bombay, Mumbai, 2002.; 2:114–129.

[14] Kapur PK, Shatnawi O and Singh O. Discrete time fault classification model. In: Kapur PK, Verma AK, editors. Quality, reliability and IT (trends and future directions). Narora Publications, New Delhi, 2005.

[15] Kapur PK, Gupta Amit, Gupta Anu, Kumar A. Discrete software rleiability growth modeling. In: Kapur PK, Verma AK, editors. Quality, reliability and IT (trends and future directions). Narora Publications., New Delhi, 2005.

[16] Kapur, P.K., Singh, O.P., Kumar, Archana and Yamada Shigeru," Discrete Software Reliability Growth Models for Distributed Systems", Published in "Quality, Reliability and Infocom Technology", Eds. : P.K. Kapur and A. K. Verma, Macmillan India Ltd., New Delhi, 2007.

[17] Kapur PK, Gupta Anu, Singh, OP. On discrete software reliability growth model and categorization of faults. Opsearch 2005; 42(4): 340–354.

[18] Kapur PK. Singh OP, Shatnawi O, Gupta Anu. A discrete NHPP Model for software reliability growth with imperfect fault debugging and fault generation. International Journal of Performability Engineering 2006; 2(4):351–368.

[19] Kapur, P.K., Khatri, S.K., Jha, P.C., and Prashant Johari "Using Change-Point Concept in Discrete Software Reliability Growth Modelling",Published in "Quality, Reliability and Infocom Technology", Eds. : P.K. Kapur and A. K. Verma, Macmillan India Ltd., New Delhi, 2007.

[20] Musa JD, Iannino A, Okumoto K. Software reliability: Measurement, prediction, applications. Mc-Graw Hill, New York, 1987.
[21] Ohba M. Software reliability analysis models. IBM Journal of Research and Development 1984; 28: 428–443.
[22] Putnam L. A general empirical solution to the macro software sizing and estimating problem. IEEE Transactions on Software Engineering 1978; SE-4: 345–361.
[23] Yamada S, Ohba M, Osaki S. S-shaped software reliability growth models and their applications. IEEE Transactions on Reliability 1984; R-33: 289–292.
[24] Yamada S, Osaki S, Narihisa H. A software reliability growth model with two types of faults. Recherche Operationnelle/Operations Research (R.A.I.R.O) 1985; 19: 87–104.
[25] Yamada, S., Osaki, S. Discrete software reliability growth models. Applied Stochastic Models and Data Analysis, 1, 65–77, 1985.

76

Epilogue

Krishna B. Misra

RAMS Consultants, Jaipur, India.

Abstract: This chapter outlines the inferences that we can now draw at the end of the presentation of the 75 chapters included in this handbook on various aspects of performability engineering. The chapter projects the direction that the technologies currently being developed can lead us in realizing the objectives of sustainable world. It also attempts to paint the scenario that may be developing in the near future.

76.1 Mere Dependability Is Not Enough

Since World War II, engineers and technologists have been concerned about the poor performance of engineering products, systems and services, and about the cost of producing and running them successfully. Although the quality of a product was always in the minds of manufacturers right from the beginning of the past century, on account of business competition, reliability got prominence only during the post war period. Consequently, design for reliability became an important consideration for products, systems, and services, particularly to offset the cost of maintenance that was rising exponentially. Consequently, designers started considering quality, reliability, and maintainability as essential attributes of products and systems, and optimizing these with respect to the cost of achieving them. In other words, survivability was their prime concern. With the increased incidences of some serious accidents, the frequencies of which were increasing, designers also had to consider stringent safety measures, and safety was incorporated into the design of products and systems along with other attributes. This led to the era of dependability-based designs, and optimization was confined in relation to the cost. Thus the performance of products, systems, or services, as of now, is being assessed mainly by dependability, which is an aggregate of the attributes of survivability and safety. However, survivability in turn is dependent on quality, reliability, maintainability (or availability), *etc*. Of course, we try to optimize the cost of physically realizing these attributes; however this is not really a true optimization of the product in relation to resources employed in creating it, as we are rarely concerned about the processes employed to produce them and their environmental consequences. One must realize that these attributes are very much influenced by the design, raw material, fabrication, techniques and manufacturing processes and their control, and finally by the usage. These attributes are interrelated and reflect the level or grade of the product so designed and utilized, which is expressed through dependability.

In fact, as of now, dependability and cost effectiveness are primarily seen as instruments for conducting international trade in the free market regime and thereby deciding the economic prosperity of a nation. However, in order to preserve our environment for future generations, the internalization of the hidden costs of environment preservation will have to be accounted for, sooner or later, in order to be able to produce sustainable products in the long run. Therefore, we can no longer rely solely on the criteria of dependability for optimizing the performance of a product, system, or service. We require the introduction of sustainability as a performance criterion that would take a holistic view of the performance enhancement along with the associated environmental consequences.

76.2 Sustainability: A Measure to Save the World from Further Deprivation

From the chapters included in this handbook, it is amply clear that the state of our environment is not very conducive for sustaining our own future generations and to provide them a decent life. We have already deteriorated the environment of the planet in the name of development and achievement of materialistic prosperity. We cannot go back to the past but we can act for the future by preventing further degradation. We should not be insensitive to investments or even sacrifices needed in order for our own grandchildren to flourish in future. Let us not be so selfish as to satisfy our present needs; we will deprive future generations of all those comforts and standards of life that we are enjoying today. Therefore, it is time that we look beyond our own needs to make the future world livable. To do so, we must follow the principles of sustainability.

Some of the basic principles of sustainability are:

- Not using non-renewable, non-abundant resources faster than substitutes can be discovered.
- Not using renewable resources faster than they are replenished.
- Not releasing wastes (solid, liquid or gaseous) faster than the planet can assimilate them.
- Not disturbing the ecological balance of the earth and depleting the diversity of life that exists on the planet.

These principles must be adhered to while designing products and processes. Old polluting technologies that are have considered the earth as a large sink must be abandoned and replaced by non-polluting technologies.

We can only start with whatever technology we have today. We know that at every stage of the life-cycle of a product, be it extraction of material, manufacturing, use or disposal, energy and materials are required as inputs, and emissions (gaseous, solid effluents or residues) are always associated with these, which influence the environmental health of our habitat. Unless we consider all these factors in our plans of creating a product, we cannot call the design of products, systems, and services truly optimal from the engineering point of view. This would necessitate bringing in sustainability principles along with other performance enhancement initiatives.

Pollution prevention is just one principle of sustainability and involves developing economically viable and safe processes (clean production and clean technologies) that entail minimal environmental pollution, require minimum quantities of raw material and energy, and yield safe products of acceptable quality and reliability that can be disposed of at the end of their life without causing any adverse effects to the environment.

The U.S. Environmental Protection Agency has laid down certain priorities to prevent pollution:

- Avoidance (search for an alternative),
- Reduction (dematerialization, better quality and reliability, better tools, *etc*.),
- Re-use, recycling and recovery,
- Energy recovery (optimum utilization),
- Treatment (hopefully down to innocuous products),
- Safe disposal.

These would necessitate the efficient use of natural resources and the use of non-waste technologies,

which would ensure that all raw materials and energy are used in a most rational and integrated way to curb all kinds of wastages while maximizing the performance. Obviously, less material and energy consumption – either through dematerialization, reuse or, recycling, or through proper treatment (clean up technology) – would lead to a lesser degree of environmental degradation. Similarly, a better design would result in prolonging the lifespan of a product and hence would ensure less adverse effects on the environment over a given period of time. In other words, we must integrate the entire life cycle of activities of survivability with that of environmental lifecycle considerations to improve product or system performance within the technological barriers with minimum cost. Last but not least, at the end of life, all products must be disposed off safely so as not to create pollution after use. All systems must be decommissioned safely so as not to interfere with the biotic and abiotic environment of the earth.

Design is the most important activity to affect new changes in products, systems, or services. It is an established fact that about 70% of costs of product development, manufacture, and use are decided in the early design stages.

To achieve these objectives, we need to introduce a performability criterion of products, systems, or services (as discussed in Chapter 1), which alone would take a holistic view of their designs for performance enhancement along with the associated problems of preventing environmental degradation.

76.3 Design for Performability: A Long-term Measure

The design of products, systems, and services for dependability is not enough, and we must design them for performability so as to include sustainability principles, since these alone can guarantee permanence. Performability is thus a long-term measure for the well-being and prosperity of people living on the earth. In fact, we should redesign all our products and systems for performability, which means designing them not only for dependability but also for the sustainability. This would require making the same product in a different way so as to minimize raw materials and energy requirement, either by the product itself or by the processes that create the product, and produce minimum byproducts or effluents.

In fact a product must be designed for:

- manufacturability (ease of production),
- logistics (production activities can be well-orchestrated),
- testability (the quality can be checked),
- reliability and maintainability (works well),
- serviceability (service after sale at reasonable cost to the company),
- safety and liability (the product is safe to use), and
- the environment (reduce or eliminate environmental impacts from cradle to grave).

Except for the design for environment other factors of design are common with design for dependability. Therefore we must elaboarte on the design for environment.

Design for Environment

To improve on current design practices that fail to consider the broad environmental implications of products (and the processes that create them), Allenby and Graedel [7] suggested the implementation of DFE as a means to "integrate decision making across all environmental impacts of a product".

Under this regime, various factors discussed earlier would involve some other considerations as well. For example, design for manufacturing would involve less material, the use of fewer different materials, and safer materials and processes in order to achieve the goal of pollution prevention. Similarly, design for serviceability would involve longevity or reliability, reuse and recycling of components or parts. It should also involve ease of dissembly, and a product must be designed for dissembly (European Community Directive: WEEE is to facilitate this), so that it can be easily and quickly dissembled, and also its parts can be reused elsewhere. A product must be designed for modularity for the ease of upgrading equipment and for its serviceability. For recovery of materials

and for safer disposal of non-recyclables, a product must be designed for recycling. A product should also be designed for energy efficiency in order to reduce energy demand during its use, and for flexible energy use. Additionally, a product should also be designed for energy recovery, for safe incineration of residues, and for composting of residues.

Quite often the only way a product can be redesigned is by rethinking the way the product is made or by considering alternative technologies, materials, and taking stock of what goes into making it (raw material), the process of manufacturing it, and finally what is created as by-product or waste besides the useful product. Waste must be minimized, as it basically adds to the cost of production.

The strategy that can be followed for minimization of waste is the following:

- Waste can be reduced by application of more efficient production technologies.
- Internal recycling of waste produced during production process.
- Source oriented improvement of waste quality, *e.g.,* substitution of hazardous substances.
- Re-use of products or parts of products, for the same purpose.

Valorization of waste and effluents has a role in making designs environment friendly as well as reducing the overall cost.

Recycling can be used to conserve resources. Recycling actually returns waste material to the original process. It helps use the waste material as a raw material substitute for another process, and processes waste material for resource recovery besides processing waste material as a by-product. However, unless it is proved to beneficial on the assumption that recycling would require very few raw materials and energy, and will release less emission into the environment, than mining and manufacturing new material, recycling should not be resorted to. Recycling is not environmentally sound when additional transportation using non-renewable fossil fuels is required to collect the material prior to recycling. Therefore, for recycling to be environmentally beneficial, the effects of collection, transportation, and reprocessing operations must be considered and proved to be less harmful than those resulting from the extraction and processing of the mined material.

Another important activity to protect the environment [3] is proper disposal of waste. This may include tipping above or underground (*e.g.,* landfills, *etc.*) or biodegradation of liquid or sludge discards in soils, or deep injection into wells or release into seas/oceans including seabed insertion, or may include biological treatment or incineration, or physio-chemical treatment, or permanent storage in containers placed in a mine pit or on the ocean bed.

The progress made by the Japanese in the past can be attributed to their strategy of not only redesigning the products but also the processes of production, so that the product can not only be made reliable but also cheap. Now our priority should be on designing products and processes that are eco-friendly. A question that often haunts a designer is at what level this can be implemented. In fact, it can be implemented at the *microscale*, which means at the level of a part of a product or at the level of a unit of production. It can also be implemented at the *mesoscale,* which means at the level of a product or at the level of a factory. It can also be implemented at the *macroscale,* which means meeting the function (service) in a new way.

If a manufacturing process allows reducing the quantity of effluents, which pollute the environment, and makes rational use of raw materials and energy at a reasonable and economic cost, the process is called *cleaner production.*

According to United Nations Environment Program (UNEP), 1989, cleaner production is the continuous application of an integrated preventive environmental strategy applied to processes, products, and services to increase overall efficiency and reduce risks to humans and the environment.

- For production processes, the strategy includes conserving raw materials and energy, eliminating toxic raw materials, and reducing the quantity and toxicity of all emissions and wastes.
- For products, the strategy focuses on reducing negative impacts along the life cycle of a

product, from raw materials extraction to its ultimate disposal.
- For services, the strategy involves incorporating environmental concerns into designing and delivering services.

Cleaner production requires changing attitudes, responsible environmental management, and evaluating technology options.

More and more companies are taking recourse to clean production. The implementation of clean production is possible in any type of industrial activity regardless of its size. Implementation comprises three steps: optimizing an existing process to provide better yields and to avoid pollution due to human error through monitoring and activation of alarms; modifying the upstream and downstream processes with the purpose of recycling or recovery, or use of waste as secondary materials; and finally designing a new process based on the two earlier steps.

Another approach that is emerging in addition to the concerns indicated above is called industrial ecology (IE). In fact, IE can be called the science of sustainability, according to Graedel and Allenby [5].
The three tenets on which IE rests are [1]:

- optimization of resources (less consumption, less waste),
- optimization of energy, and
- optimization of capital (humans and capital).

IE signifies a shift in paradigm from "end-of-pipe" pollution control methods towards holistic strategies for prevention and planning of more environmentally sound industrial development. IE is advanced as a holistic approach to redesigning industrial activities. Governments, scientists, policy-makers, and the general public are becoming increasingly aware of the environmental damage associated with the large and growing material through-put required in modern industrial society. IE helps address this concern. In the traditional model of industrial activity, individual manufacturing processes take in raw materials and generate useful products to be sold, plus waste or by-products to be disposed of. In an IE model, it should be transformed into a more integrated an industrial ecosystem. In such a system the consumption of energy and materials is optimized, waste generation is minimized, and the effluents of one process serve as the raw material for another process.

Allenby [2] defines industrial ecology as the means by which a state of sustainable development is approached and maintained. It consists of a system's view of human economic activity and its interrelationship with fundamental biological, chemical, and physical systems with the goal of establishing and maintaining the human species at levels that can be sustained indefinitely, given continued economic, cultural, and technological evolution. It is a systems' view in which one seeks to optimize the total materials cycle from virgin material, to finished material, to component, to product, to obsolete product, and to ultimate disposal. Factors to be optimized include resources, energy, and capital.

76.3.1 Recourse to Alternative Technologies

Notwithstanding what we may do to prevent pollution, the maximum impact that our efforts will have will be decided by the choice of technology [4] that we employ in our production. It is here that the success of our efforts will be decided by the choice of out technology. Whatever technology we might eventually use in production processes, it must be non-polluting and should have all the advantage of clean production. There appear two seemingly very useful and powerful technologies on the horizon that are likely to change the way products and systems will be produced in the 21st century. The revolution is just around the corner and will change the way we look at products today. Undoubtedly, these are likely to be clean and sustainable technologies.

76.3.1.1 Uses of Industrial Biotechnology

We shall not discuss here the uses of biotechnology in food and agriculture, and medicines where it has done wonders, but rather we shall discuss very briefly its implication for manufacturing companies or for industrial uses. Although *industrial biotechnology* is in the early stages of development, its innovative applications are increasing rapidly into all areas of manufacturing

and it is providing useful tools for cleaner and sustainable production techniques.

The world is reverting to the use of bioprocesses in comparison to chemical processes to produce a number of useful industrial products, since it is not only environmentally cleaner but also economically viable as non-renewable resources become scarce. Biotechnology, for instance, with the advent of genetic engineering and recombinant DNA technology has opened up several vistas for new industrial applications. Even non-bio-degradable products like plastics, which once were considered environmental unfriendly, have now been made environmentally friendly by the production of biodegradable plastics based on polyhydroxybutyrate made by bacteria [6] from renewable food stock and polymeric carbohydrates such as Xanthan. Ammonia today can be produced by nitrogen-fixing bacteria and thus can be a cleaner way of producing fertilizers, whose production through chemical processes have never been environmentally friendly.

Biological leaching in extracting metals from ores can be of tremendous advantage, particularly when grades of ore are becoming poorer day by day, as we have already mined minerals extensively earlier. Biotechnology as we know can help to clean up the environmental mess especially in the case of contaminated soils, removal of heavy metal sulfates from water, and removal of hazardous elements from gaseous emissions using bio-filters or from wastewater. Chlorine bleaching in the pulp and paper industry is being substituted by biotechnology processes. Some of the industrial processes developed by companies have been very successful in using biotechnology to prevent environmental pollution.

Bio-fuels, like bio-ethanol and bio-diesel [8], are likely to become popular and help meet increasing fuel demands. Ethanol is currently produced by fermenting grain (old technology). The cellulose enzyme technology developed by Iogen, Canada allows the conversion of crop residues (stems, leaves, and hulls) to ethanol. This results in reduced CO_2 emissions by more than 90% (compared to oil) and also allows greater domestic energy production as it uses a renewable feedstock. The process is in the scale-up phase of the technology and it is likely to result in the cost of ethanol produced in this manner being competitive with the cost of gasoline produced from oil, costing USD 25 per barrel.

The vegetable oil degumming process [8] developed by Cerol, Germany, has reduced amounts of caustic soda, phosphoric acid, and sulphuric acid used compared to conventional processes. The enzymatic process has reduced the amount of water needed in washing and as dilution water. Sludge production has been reduced by a factor of 8. Hydrogen peroxide used for bleaching textiles usually requires several rinsing cycles.

A new enzyme process developed by Windel, Germany, requires only one high temperature rinsing to remove bleach residues. This has helped reduce the energy consumption by 14% and water consumption by 18%, and thereby the production costs and pollution. In the old process of refining zinc, the finishing wastewater contains heavy metals, sulfuric acid, and gypsum used to precipitate sulfates. A new biological process developed by Budel Zinc, The Netherlands, uses sulfate reducing bacterial enzymes for sulfate reduction. This process allows zinc and sulfate to be converted to zinc sulfide, which is recycled to the refinery. This process has resulted in a 10 to 40-fold decrease in the concentration of heavy metals in the refinery wastewater, gypsum is produced, and valuable zinc is recycled.

Thus *industrial biotechnology* is also in the early stages of development and its innovative applications are increasing very rapidly into all areas of manufacturing. It is providing useful tools for cleaner and sustainable production and it is expected to continue to do so in the future as well. The day is not distant when biotechnology will take over all production technologies completely and help preserve a clean environment.

The Organization for Economic Cooperation and Development (OECD) with headquarters in Paris has constituted a Task Force on Bio-technology for Sustainable Industrial Develop-ment, whose mission is to assist developed and developing countries of the world to achieve sustainable development. It is expected to play a key role in achieving the objectives of promoting clean technologies.

76.3.1.2 Industrial Uses of Nanotechnology

Nanotechnology is known as the frontier area of science in the coming years. Nanoscale materials have been used for decades in applications ranging from window glass and sunglasses to car bumpers and paints. However, the convergence of scientific disciplines (chemistry, biology, electronics, physics, engineering, *etc*.) is leading to numerous applications in materials manufacturing, computer chips, medical diagnosis and health care, energy, biotechnology, space exploration, security, and so on. Hence, nanotechnology is expected to have a significant impact on our economy and society within the next 10 to 15 years, growing in importance over the longer term as further scientific and technology breakthroughs are achieved. The US National Science Foundation has predicted that the global market for nanotechnologies will reach $1 trillion or more within 20 years. Sales of emerging nanotechnology products have been estimated by private research to have risen to 15% of global manufacturing output in 2014.

Currently, nanotechnology [9] is being incorporated selectively into high-end products, especially in automotive and aerospace applications. Forecasts indicate that by 2009, commercial breakthroughs are likely to unlock markets for nanotechnology innovations, and microprocessors and memory chips built using new nanoscale processes will appear on the market. From 2010 onwards, nanotechnology will have become commonplace in manufactured goods. Health care and life science applications are finally becoming significant as nano-enabled pharmaceuticals and medical devices emerge from lengthy human trials.

The basic building blocks of nanotechnology are carbon nanotubes, nanoparticles, and quantum dots.

Nanotubes

Carbon nanotubes, long thin cylinders of atomic layers of graphite, may be the most significant new material since plastics and are the most significant of today's nanomaterials. They come in a range of different structures, allowing a wide variety of properties. They are generally classified as single-walled (SWNT), consisting of a single cylindrical wall, or multiwalled nanotubes (MWNT), which have cylinders within the cylinders.

SWNT has amazing properties such as its size of 0.6 to 1.8 nanometers in diameter and has a density of 1.33 to 1.40 g/cm^3, whereas aluminium has a density of 2.7 g/cm^3. It has heat transmission capability is 6,000 W/m/K at room temperature, whereas pure diamond transmits 3,320 W/m/K. The current carrying capacity is estimated at 1 billion A/cm^2, whereas copper wire burns out at about 1 million A/cm^2. It has a tensile strength of 45 billion Pa, whereas high-strength steel alloys break at about 2 billion Pa. It has a temperature stability of 2,800°C in vacuum, and 750°C in air, whereas metal wires in microchips melt at 600 to 1,000°C. With all these desirable properties, SWNTs are more difficult to manufacture than MWNT. Carbon Nanotechnologies of Houston, one of the world's leading producers, only makes up to 500 g *per* day. The other drawback is that it is difficult to make nanotubes interact with other materials. For example, to fully exploit their strength in composite materials, nanotubes need to be *attached* to a polymer. They are chemically modified to facilitate this (a process known as *functionalization*), but this process reduces the very properties the nanotubes may be used for.

The most promising applications of nanotubes may be in electronics and optoelectronics. Today, the electronics industry is producing MOSFETs (metal oxide semiconductor field effect transistors) with critical dimensions of just under 100 nm, with half that size projected by 2009 and 22 nm by 2016. However, the industry will then encounter technological barriers and fundamental physical limitations to size reduction. With carbon nanotubes, it is possible to achieve higher performance without having to use ultra thin silicon dioxide gate insulating films. In addition, semiconducting SWNTs, unlike silicon, directly absorb and emit light, thus possibly enabling a future opto-electronics technology. SWNT devices would still pose manufacturing problems due to quantum effects at the nanoscale, so the most likely advantage in the foreseeable future is that carbon nanotubes will allow a simpler fabrication of

devices with superior performance at about the same length as their scaled silicon counterparts.
Carbon nanotubes have been demonstrated to be efficient field emitters and are currently being incorporated in several applications, including flat-panel display for television sets or computers, or any devices requiring an electron producing cathode such as X-ray sources (*e.g*., for medical applications).

Semiconducting nanotubes change their electrical resistance dramatically when exposed to alkalis, halogens, and other gases at room temperature, which raises hopes for better chemical sensors. The sensitivity of these devices is 1,000 times that of standard solid state devices.

There are still many technical obstacles to overcome before carbon nanotubes can be used on an industrial scale, but their enormous potential in a wide variety of applications has made them the "star" of the nano-world and encouraged many companies to commit the resources needed to ensure that the problems will be solved. Fujitsu, for example, expects to use carbon nanotubes in 45 nm chips by 2010 and in 32 nm devices by 2013.

Nanoparticles

The metal oxide ceramic, metal, and silicate nanoparticles constitute the most common of the new generation of nanoparticles. Moving to nanoscale changes the physical properties of particles, notably by increasing the ratio of surface area to volume, and the emergence of quantum effects. A high surface area is a critical factor in the performance of catalysis and structures such as electrodes, allowing improvement in performance of such technologies as fuel cells and batteries.

Nansulate is an insulative coating by Industrial Nanotech, which incorporates nanoparticles that give it unique performance characteristics in a translucent, thin film coating, which uses nano-sized particles that have been engineered to inhibit the solid, gaseous, and radiative (infrared) heat transfer through an insulator. Nansulate repels moisture from the coating itself, effectively creating a moisture-free barrier against the pipe or tank or piece of equipment being insulated. This coating has the advantage of being corrosion and mould resistant. It is reported in [13] that nansulate high heat was applied to the heat exchangers of dyeing machines in a dye house in the Trakya region of Turkey. A coating of an average thickness of 70 microns was applied to provide insulation to the equipment. This resulted in a reduction of 20% of liquid natural gas (LNG) consumption over a period of five months, which amounted to a saving of approximately US$ 40,000 per month to the company. This film may have uses in energy sector to meet air quality and energy-use restrictions; a multi-use thin film insulating coating holds many benefits for reducing energy use. Bio-fuel facilities use processing equipment as well as miles of pipelines that can benefit from the combined insulating and corrosion resistance property of nanotechnology coatings. One area currently in research is called "intelligent coatings". Intelligent coatings are coatings that self repair and self report. For example, a coating that is able to repair itself upon being scratched, removed, or damaged and then changes color in that area as an indicator of the area of damage.

This type of coating would be especially useful in areas where failure of a coating protecting a pipeline or tank could cause significant damage.

Quantum Dots

Just as carbon nanotubes are often described as the new plastics, so quantum dots can be defined as the ball bearings of the nano-age. They are 1 nm structures made of materials such as silicon, capable of containing a single electron, or a few thousand, whose energy states can be controlled by applying a given voltage. In theory, this could be used to fulfil dream of changing the chemical nature of a material, making lead into gold. It is possible to make light-emitting diodes (LEDs) from quantum dots, which may produce white light, *e.g.,* for buildings or cars. Quantum dots can be used for making ultra fast, all-optical switches and logic gates that work faster than 15 terabits a second. The Ethernet usually handles only 10 megabits per second. Other possible applications are all-optical demultiplexers (for separating various multiplexed signals in an optical fibre), all-optical computing, and encryption, whereby the spin of an electron in a quantum dot represents a quantum bit or qubit of information.

Biologists are experimenting with composites of living cells and quantum dots. These could

possibly be used to repair damaged neural pathways or to deliver drugs by activating the dots with light.

There are hundreds of applications possible for nanotechnology [11], but as the technology is still being developed, it serves no useful purpose to list all possible future applications here. The idea of discussion is to stimulate imagination of what is going to come in the near future, not in the distant future but within a couple of decades.

There is much to come by way of marriage between the two leading technologies of the future, *i.e.,* biotechnology and nanotechnology.

76.4 Parallelism Between Biotechnology and Nanotechnology

Since the discovery of deoxyribonucleic acid (DNA) in 1953, there have been tremendous advances in the field of biotechnology. DNA is a nucleic acid and is identified as the genetic material in all life. It contains the genetic instructions for the biological development of a cellular form of life or a virus. All known cellular life and some viruses have DNAs. DNA is a long polymer of nucleotides (a polynucleotide) that encodes the sequence of amino acid residues in proteins, using the genetic code. DNA is the master molecule of life that controls the development and functioning of organisms. DNA is responsible for the genetic propagation of most inherited traits. In humans, these traits range from hair color to disease susceptibility. This threadlike molecule is present in chromosomes of all organisms. It is made up of two strands that are coiled clockwise in a double helical manner like a spiral staircase. The two strands are made of phosphate and sugar called deoxyribose.

Four nitrogen compunds called “bases” form the rungs of the DNA ladder: adenine (A), guanine (G), cystosine (C), and thymine (T). The bases always join in a specific manner: A pairs with T; G pairs with C. Thus there are only four kinds of base-pair combinations: A-T, C-G, T-A and G-C. However, the sequence of base pairs along the length of the strands is not the same in DNAs of different organisms. It is this difference that is responsible for the difference between one gene and another. A gene is a segment of a DNA chain that contains codes for the production of a complete protein.

The DNA molecule is not directly involved in the functioning of the cell. Rather, it instructs the machinery of the cell to make required proteins (including enzymes). These proteins, in turn, control all chemical processes in the cell. This is actually done by DNA with the help of RNA. RNA is a complex single strand molecule found in the cytoplasm of the cell. RNA is made of the same bases as DNA except that the base T is replaced by the base uracil (U), which can also pair with A. There are many types of RNA, including m-RNA (messenger RNA), rRNA (ribosomal RNA) and tRNA (transfer RNA). The m-RNA carries information out of the nucleus and into the cytoplasm, where proteins are made. The r-RNA forms the structure of ribosomes in the cells. The t-RNA brings to the ribosomes the amonoacids needed for making protein.

The DNA molecule directs the machinery of the cell in the following way: it makes a messenger RNA (m-RNA) molecule carry the genetic information from the nucleus out into the cytoplasm, the part of the cell which makes proteins. In cytoplams , the m-RNA serves as the blueprint for making protein molecules needed by the cell. The instructions on m-RNA are in the form of a code which consistes of 64 three-base combinations available on DNA molecules.

The genetic code is the set of rules by which information encoded in genetic material (DNA or RNA sequences) is translated into proteins (amino acid sequences) by living cells. Specifically, the code defines a mapping between tri-nucleotide sequences called codons and amino acids; every triplet of nucleotides in a nucleic acid sequence specifies a single amino acid. Most organisms use a nearly universal code that is referred to as the standard genetic code. Even viruses, which are not cellular and do not synthesize proteins themselves, have proteins made using this standard code The genetic information carried by an organism, its genome, is inscribed in one or more DNA, or in some cases RNA, molecules.

The genetic information encoded by an organism's DNA is called its genome. During cell division, DNA is replicated, and during reproduction is transmitted to offspring. Genes are the units of heredity and can be loosely viewed as the organism's "cookbook" or "blueprint". DNA is often referred to as the molecule of heredity. Within a gene, the sequence of nucleotides along a DNA strand defines a messenger RNA sequence which then defines a protein that an organism is liable to manufacture or *express* at one or several points in its life using the information of the sequence.

Parallelism

The goal of molecular nanotechnology (MNT) is to manufacture complex products with almost every atom in its proper place. This requires building large molecular shapes and then assembling them into products. The molecules must be built by some form of chemistry. The MNT assumes that building shapes of the required variety and complexity will require robotic placement (covalent bonding) of small chemical pieces. Once the molecular shapes are made, they can be combined to form structures and machines. This probably will be done again by robotic assembly. It probably can be done by building diamond lattice by mechanically guided chemistry, or mechano-chemistry. By building the lattice in various directions, a wide variety of parts can be made: the parts that would be familiar to a mechanical engineer, such as levers, *etc*. The robotic system used for building the molecular parts can also be used to assemble the parts into a machine.

In fact, there is no reason why a robotic system cannot build a copy of itself. In sharp contrast to conventional manufacturing, only a few (chemical) processes are needed to make any required shape. Moroever, with each atom in the right place, each manufactured part will be precisely the right size,so robotic assembly plans may be easy to program. A small nano-robotic device that can use supplied chemicals to manufacture nanoscale products under external control is called a fabricator. A personal nanofactory will consist of trillions of fabricators, and could only be built by another nanofactory. But a fabricator could build a very small nanofactory, with just a few fabricators in it. A smaller nanofactory could build a bigger one, and so on.

The mechanical designs proposed for nano-technology are more like a factory than a living system. Molecular scale robotic arms able to move and position molecular parts would assemble rather rigid molecular products using methods more familiar to a machine shop than the complex brew of chemicals found in a cell. Although we are inspired by living systems, the actual designs are likely to owe more to design constraints and our human objectives than to living systems. Self replication is but one of many abilities that living systems exhibit. Copying that one ability in an artificial system will be challenge enough without attempting to emulate their many other remarkable abilities.

Von Neumann designed a self-replicating device that existed in a two-dimensional "cellular automata" world. The device had an "arm" capable of creating arbitrary structures, and a computer capable of executing arbitrary programs. The computer, under program control, would issue detailed instructions to the arm. The resulting universal constructor was self-replicating almost as a by-product of its ability to create any structure in the two-dimensional world in which it lived. If it could build any structure it could easily build a copy of itself, and hence was self-replicating.

One interesting aspect of von Neumann's work is the relative simplicity of the resulting device: a few hundred kilobits to a megabit. Self-replicating systems need not inherently be vastly complex. Simple existing biological systems, such as bacteria, have a complexity of about 10 million bits. Of course, a significant part of this complexity is devoted to mechanisms for synthesizing all the chemicals needed to build bacteria from any one of several simple sugars and a few inorganic salts, and other mechanisms for detecting and moving to nutrients. Bacteria are more complex than strictly necessary simply to self-reproduce.

When we contrast this with a bacterium, much of the additional complexity is relatively easy to explain. Bacteria use a relatively small number of well defined chemical components which are brought to them by diffusion. This eliminates the

mining, hauling, leaching, casting, molding, finishing, and so forth. The molecular "parts" are readily available and identical, which greatly simplifies parts inspection and handling. The actual assembly of the parts uses a single relatively simple programmable device, the ribosome, which performs only a simple rigid sequence of assembly operations (no AI in a ribosome!). Parts assembly is done primarily with "self-assembly" methods, which involve no further parts-handling. Self replication is used here as a means to an end, not as an end in itself. A system able to make copies of itself but unable to make much of anything else would not be very useful and would not satisfy our objectives. The purpose of self replication in the context of manufacturing is to permit the low cost replication of a flexible and programmable manufacturing system; a system that can be reprogrammed to make a very wide range of molecularly precise structures. This lets us economically build a very wide range of products.

A person who saw DNA's potential beyond biology was Naiman Seeman, a chemist at New York University, who theorized the concept of nanofabrication [10] some 20 years ago. Seeman began imagining how the genetic information in DNA can be engineered to perform useful tasks. DNA comes with a built-in code that researchers can re-formulate to control which DNA molecules bond with each other. The goal of this DNA tinkering is to develop microscopic factories that can produce *made-to-order* molecules, as well as electronic components ten times smaller than current limits. The ability to attach particles to DNA pieces is a step towards fabricating nano-electronics. Scientists can hitch functional materials like metals, semiconductors, and insulators to specific DNA molecules, which can then carry their cargo to pre-specified positions.

More recently, Seeman and colleagues have put DNA robots to work by incorporating them into a self-assembling array. The composite device grabs various molecular chains, or "polymers", from a solution and fuses them together. By controlling the position of the nano-bots (as these tiny robot are called), the researchers can specify the arrangement of the finished polymer. Seeman hopes this tiny assembly line can be expanded into nano-factories that would synthesize whole suites of polymers in parallel. This technique has already been used to make a simple transistor, as well as metallic wires.

Researchers have built an inchworm-like robot so small you need a microscope just to see it. The tiny bot measures about 60 micrometers wide (about the width of a human hair) by 250 micrometers long, making it the smallest controllable micro-robot. Scientists recently built the tiniest electric motor ever. One could stuff hundreds of them into the period at the end of this sentence.

76.5 A Peep into the Future

In this section, the author would like to take a journey into a future full of strange possibilities, which in his opinion may become realities some day. These are based on the current state of science and trends that are being visualized keeping the objective of sustainable development in mind.

With nanotechnology coming in vogue, our energy requirements could be slashed considerably and sustainable energy sources like solar cells would not only prove to be economical but will be a clean source of energy. Solar solutions can be implemented on an individual, village, or national scale. The energy of direct sunlight is approximately 1 kW/m^2. Dividing that by ten to account for nights, cloudy days, and system inefficiencies, present-day American power demands (about 10 kW per person) would require about 100 m^2 of collector surface per person. Multiplying this figure by a population of 325 million (estimated by the US Census Bureau for 2020) yields a requirement for approximately 12,500 square miles of area to be covered with solar collectors. This represents 0.35% of total US land surface area. Much of this could be implemented on rooftops, and conceivably even on road surfaces. Storable solar energy will reduce ash, soot, hydrocarbon, NOx, and CO_2 emissions, as well as oil spills. The system can be totally decentralized with no loss of power in long transmission lines, or distribution systems, or risk of theft or sabotage, besides saving lots of copper

and steel and release land which they occupy for giving them right of way and substations.

Molecular manufacturing can be self-contained and clean; a single suitcase could contain all equipment required for a village-scale industrial revolution. Finally, MNT will provide cheap and advanced equipment for medical research and health care, making improved medicine widely available. Even in areas that currently do not have a technological infrastructure, self-contained molecular manufacturing will allow the rapid deployment of environment-friendly technology.

Eventually, we may hope that MNT will be able to directly edit the DNA of living cells in the body. However, even without that level of sophistication, massively parallel scanning may enable the sorting of cells modified outside the body. The ability to inject only non-cancerous cells would make some kinds of genetic therapy much safer. Microsurgical techniques [12] could allow the implantation of modified cells directly into the target tissues. In fact humans can prolong their life as much they desire to live without having any kind of disease. Probably limbs and organs could be grown or renewed. Of course this will have to conform to the requirement of carrying capacity of the earth to ensure sustainability.

There will be a fusion of biotechnology and nanotechnology and this will lead to all products and systems becoming biodegradable in future so that their manufacturing and disposal does not create any environmental pollution. Development of biodegradable plastic is a step in that direction. In fact all items of daily use can be made biodegradable and possibly grown using the technology based on bio-nano-technology. We will possibly be able to make tables, chairs, beds, clothes, and anything else by molecular manipulation.

If most structures and functions can be built out of carbon and hydrogen, there will be far less use for minerals, and mining operations can be mostly shut down. Manufacturing technologies that pollute can also be scaled back.

Remembering the most complex, reliable, and sustainable machine that this planet has evolved over 3.5 billion years starting from from simple living cells through correct and unique combinations of molecules, is human not to talk of other living creatures. This biological machine (which is highly complex and biodegradable, less polluting and requires less energy for all its functions) is a marvel in many respects, and can hardly be achieved through any artificial manufacturing methods or inorganic processes. No mechanical pump can ever surpass the performance of the heart pumping blood through entire body ceaselessly for years. A three-dimensional camera like the human eyes, a stereo system like the of ears, and many such subsystems can hardly be built or copied by the technology that humans or living being are capable of having. This human machine has all the intelligence, senses, locomotion and replicating capabilities (all biologically grown or developed) that we are trying to copy or achieve through extraneous means like robots or machines (inorganic means). Why cannot the same analogy be used to create futuristic systems, accessories and services biologically using biotechnology and nanotechnology that will help satisfy our needs and make life comfortable and happier? We have not learn much from natural biological processes of product development. Like making of honey by bees or building miles and miles long silk threads. Maybe we are eventually heading towards that. that.

References

[1] Westman WE. Ecology, impact assessment, and environmental planning, Wiley, New York, 1985.

[2] Allenby, Braden R. Achieving sustainable development through industrial ecology. International Environmental Affairs; 1992: 4(1): 56–68.

[3] Allenby BR. An international design for environment infrastructure concept and implementation. Electronics and the Environment; 1993. Proceedings of the 1993 IEEE International Symposium, May 1993:10(12): 49–55.

[4] Allenby BR. Integrating environment and technology: Design for environment. In The Greening of Industrial Ecosystems. Allenby BR. and Richards DJ. National Academy Press, Washington, 1994: 137–148.

[5] Graedel TE, Allenby BR (Eds.). Industrial ecology. Prentice Hall, New York, 1995

[6] Misra KB (Ed.). Clean production: Environmental and economic perspectives. Springer, Berlin, 1996.
[7] Graedel TE, Allenby BR. Design for environment. Prentice Hall, New York, 1996.
[8] OECD. The application of biotechnology to industrial sustainability: A Primer. 2002.
[9] OECD. Opportunities and risks of nano-technologies. 2005.
[10] Schirber Michael. Beyond biology: Making factories and computers with DNA. Live Science, June 20, 2006.
[11] Bhushan Bharat. Springer Handbook of nano-technology, Springer, London, 2007.
[12] Vo-Dinh Tuan. Nanotechnology in biology and medicine: Methods, devices, and applications. CRC Press, Boca Raton, FL, 2007.
[13] Insulative Coatings. Asiapacific Coatings Journal. News Article 12020: Jan. 12, 2007.

About the Editor

Krishna B. Misra is at present the Principal Consultant for RAMS Consultants. He established the company in Jaipur in 2005 and since then he was also been working as the Editor-in-Chief of the quarterly International Journal of Performability Engineering, published by RAMS Consultants. He has held the position of a full professor since 1976 at IIT Roorkee and also at IIT Kharagpur. He was also Director of North Eastern Regional Institute of Science and Technology (a Deemed University) from 1995 to 1998. During the period 1992–1994, he was Director-grade-Scientist at the National Environmental Engineering Research Institute (NEERI, Nagpur, India) where he set up two divisions, *viz*, the *Disaster Prevention and Impact Minimization Division* and the *Information Division*. He has been Coordinator of the Ministry of Human Resource Development Project on *Reliability Engineering* since 1983 at IIT Karagpur. He also served as Dean of the Institute of Planning and Development at IIT, Kharagpur. Dr. Misra has been working in the area of reliability engineering since 1967 and has been making efforts to popularize reliability, safety, and allied concepts in India, both in the industry and in engineering education. It was due to his efforts that a master's degree program in reliability engineering was conceptualized and started for the first time in India at IIT, Kharagpur in 1982. This program has been running successfully to date. In 1983, he also founded the Reliability Engineering Center at IIT, Kharagpur, which is the first of its kind to promote research, consultancy, and teaching at an advanced level in the area of reliability, quality, and safety engineering in India.

Since 1963, he has taught and/or researched at the oldest and reputed engineering institutions of the country, which include IIT-Roorkee, IIT-Kharagpur, and NEERI, Nagpur. He has also worked in Germany at four different institutions, *viz,* GRS-Garching, Technical University-Munich, RWTH-Aachen, and Kernforschungszentrum, Karlsruhe. On invitation, he has delivered lectures in USA, England, Finland, France, Germany, Greece, Holland, Italy, Poland, and Sweden.

Dr. Misra has published over 200 technical papers in reputed international journals such as IEEE Transactions on Reliability, Microelectronics and Reliability, the International Journal of System Science, the International Journal of Control, Reliability Engineering and System Safety, the International Journal of Quality and Reliability Management, the International Journal of Reliability, Quality, and Safety Engineering, Fuzzy Sets and Systems, *etc*. Dr. Misra's research papers are widely quoted in international journals and books.

Besides being an Associate Editor of IEEE Transactions on Reliability, Dr. Misra has served as reviewer for IEEE Transactions on Reliability for nearly four decades and had also served on the editorial board of several international journals, including Microelectronics and Reliability (for more than 25 years), Reliability Engineering and System Safety, Quality and Reliability Management, the International Journal of Reliability, Quality, and Safety Engineering, the International Journal of Fuzzy Mathematics,

the Electrical Power Research Journal, *etc*. He has also been a reviewer for Fuzzy Sets and Systems, the European Journal on Operational Research, the International Journal on General Systems, *etc*. In 2005, he started the quarterly International Journal of Performability Engineering. Dr. Misra introduced the concept of performability as a holistic attribute of performance.

In 1992, Professor Misra authored a 889-page state-of-the-art book on *Reliability Analysis and Prediction: A Methodology Oriented Treatment*, published by *Elsevier Science Publishers*, Amsterdam. In 1993, Prof. Misra edited a 715-page book, *New Trends in System Reliability Evaluation*, which was also published by *Elsevier Science Publishers*. These books have received excellent reviews from the scientific community. In 1995, Professor Misra edited another 853-page book, *Clean Production: Environmental and Economic Perspectives*, published by Springer, Germany. In 2004, he authored another book, *Principles of Reliability Engineering*, which is mainly aimed at practicing engineers.

Dr. Misra is a recipient of a several best paper awards and prizes in addition to the first *Lal C. Verman Award* in 1983 by the Institution of Electronics and Telecommunications Engineering *for his pioneering work in reliability engineering in the country*. In 1995, in recognition of his *meritorious* and *outstanding contributions* to reliability research and education in India, he was awarded a plaque by the IEEE Reliability Engineering Society, USA.

Prof. Misra is a fellow of the Indian Academy of Sciences, the Indian National Academy of Engineering, the Institution of Electronics and Telecommunications (India), the Institutions of Engineers (India) and Safety and Reliability Society (UK). He has been vice president of the System Society of India, of which he is a life member. He is also a life member of the National Institute of Quality and Reliability.

Currently, Dr. Misra is the Chairman of the Indian Bureau of Standards Committee LTDC 3 on Reliability of Electrical and Electronic Components and Equipments. For several years, he served as a member of the Environmental Appraisal Committee (for nuclear power plants in India), the Ministry of Environment and Forests, Government of India, New Delhi. In 1976, Prof. Misra was invited by the Department of Science and Technology, New Delhi, to serve as the convener of the NCST *working group on Reliability Engineering in India*, set up by the Government of India. This group submitted two reports (Part Is and II) in 1978 on *the Reliability Implementation Program for India.* He also served as member of Task Force Committee on Reliability Engineering of the Department of Science and Technology, in 1979. He has served as member on the Project Assessment Committee for the National Radar Council, the Department of Electronics, CSIR, UGC, *etc*. Dr. Misra is listed in *Indo-American Who's Who.*

About the Contributors

Amari, Suprasad V., is a senior reliability engineer at Relex Software Corporation. He pursued his MS and PhD in reliability engineering at the Reliability Engineering Centre, Indian Institute of Technology, Kharagpur. He has published over 35 research papers in reputed international journals and conferences. He is an editorial board member of the International Journal of Reliability, Quality and Safety Engineering, an area editor of the International Journal of Performability Engineering, and a management committee member of RAMS. He is a member of the US Technical Advisory Group (TAG) to the IEC Technical Committee on Dependability Standards (TC 56), an advisory board member of several international conferences, and a reviewer for several journals on reliability and safety. He is a senior member of ASQ, IEEE, and IIE; and a member of ACM, ASA, SSS, SRE, and SOLE. He is also an ASQ-certified reliability engineer. E-mail: suprasad.amari@relex.com

Ang, B.W., is Professor of Industrial and Systems Engineering at the National University of Singapore. His primary research interest is systems modeling and forecasting. He has developed several index decomposition analysis techniques for quantifying factors contributing to changes in aggregate measures These techniques have been widely used to study changes in national energy consumption and energy-related greenhouse house gas emissions by researchers and national energy agencies. He is an associate editor of Energy – The International Journal and Energy Economics, and a member of the editorial boards of Energy Policy, Energy and Environment, International Journal of Performability Engineering, and the Journal of Urban Technology.

Aven, Terje, is Professor of Risk analysis and Risk Management at the University of Stavanger, Norway. He is also a principal researcher at the International Research Institute of Stavanger (IRIS). He was professor II (adjunct professor) in reliability and safety at the University of Trondheim (Norwegian Institute of Technology) from 1990 to 1995 and professor II in reliability and risk analysis at the University of Oslo from 1990 to 2000. He was the dean of the faculty of technology and science, Stavanger University College from 1994 to 1996. Dr. Aven has many years of experience in the petroleum industry (the Norwegian State Oil Company, Statoil). He has published a large number of papers in international journals on probabilistic modelling, reliability, risk and safety. He is the author of several reliability and safety related books, including Stochastic Models in Reliability, Springer, 1999 (co-author U. Jensen), Foundations of Risk Analysis, Wiley, 2003, and Risk Management, Springer, 2007 (co-author J.E. Vinnem). He is a member of the editorial boards of Reliability Engineering and System Safety, and the Journal of Risk and Reliability. He is an associate editor of the Journal of Applied Probability on Reliability Theory and an area editor (within risk management) of the International Journal of

Performability Engineering. He is a member of the Norwegian Academy of Technological Sciences and Head of the Stavanger Chapter 2005–2007. He has supervised about 20 Ph.D. students in risk and safety. He received his Master's degree (cand. real) and Ph.D (dr. philos) in mathematical statistics (reliability) from the University of Oslo in 1980 and 1984, respectively.

Ba, Dechun, obtained his Bachelor's degree from Northeastern University in July of 1977, majoring in mechanical design and manufacture, post graduated from Northeastern University in July of 1985, majoring in vacuum and fluid engineering and received his Ph.D. from Northeastern University in September of 1997. Professor Ba has a wide range of interests, including synthesis of function films and plasma modeling. Professor Ba is the member of American Vacuum Society.

Baas, Leo (1946), has a Master's of Science degree in sociology of industry and business management with a specialization in environmental sciences and a Ph.D. in social sciences on the subject of the dynamics of the introduction and dissemination of the new concepts of cleaner production and industrial ecology in industrial practice. He has been working at the Erasmus Centre on Sustainability and Management (ESM) at Erasmus University Rotterdam since April 1986. He has performed research on cleaner production since 1988 and on industrial ecology since 1994. He has been an advisor of the UNEP/UNIDO National Cleaner Production Centres Programme since 1994, and a member of UNEP's High Level Expert Forum on Sustainable Consumption and Production. He is a member of the strategic decision-making platform of the long-term innovation programme Sustainable Enterprises in the Rotterdam Harbour and Industry Complex in the Netherlands. He co-ordinates the International Off-Campus Ph.D. Programme on Cleaner Production, Cleaner Products, Industrial Ecology & Sustainability, and the Social Science Track of the International Inter-University M.Sc. Industrial Ecology (in co-operation with Delft University of Technology and Leiden University) at Erasmus University. He is responsible for the module Corporate Environmental Management at the International Institute for Housing and Urban Development. Dr Baas is an area editor (industrial ecology) of the International Journal of Performability Engineering.

Barbu, Vlad Stefan, is associate professor in statistics at the University of Rouen, France, Laboratory of Mathematics "Raphaël Salem". He received his B.Sc. in mathematics from the University of Bucharest, Romania (1997) and his M.Sc. in applied statistics and optimization from the same university (1998). He worked for three years (1998–2001) as an assistant professor in mathematics at the University "Politehnica" of Bucharest, Romania. In 2005 he received his Ph.D. in applied statistics from the University of Technology of Compiègne, France. His research focuses mainly on stochastic processes and associated statistical problems, with a particular interest in reliability and DNA analysis. He has published several papers in the field.

Barratt, Rod S., BSc PhD CSci CChem FRSC, is a chartered chemist by profession, and has spent most of his career in the teaching and practice of air quality management. He built a practical foundation in his subject in local government environmental protection and energy consultancy. At the Open University, he is Head of the Department of Environmental and Mechanical Engineering. His teaching interests focus on air quality management and wider aspects of safety, health and environmental management and he supervises several part-time research students working in these areas. In addition to about 40 journal publications, he has written two books dealing with environmental management, one on atmospheric dispersion modelling and various book chapters. As an expert witness, he has used atmospheric dispersion modelling in developing evidence for public inquiries relating to the planning aspects of road, industrial and mineral working activities. Dr. Barratt is the area editor (sustainability) of the International Journal of Performability Engineering.

Bettley, Alison, Ph.D., is a senior lecturer in Technology Management in the Faculty of Technology of the Open University. She currently chairs the university's master's course in business operations and pursues research interests in operations management, knowledge management, technology strategy, and the marketing of high technology services. As well as her academic interests, she has extensive professional experience as an R&D and technical services manager in the fields of environmental technology and management.

Brooks, Richard R., is an associate professor in the Holcombe Department of Electrical and Computer Engineering of Clemson University. His research is in adversarial systems and security technologies. He has a B.A. in mathematical sciences from The Johns Hopkins University and a Ph.D. in computer science from Louisiana State University.

Burnley, Stephen, Ph.D., is a senior lecturer in Environmental Engineering in the Faculty of Technology of the Open University. He is responsible for teaching solid waste management at undergraduate and postgraduate levels. His research interests cover municipal waste surveys and statistics, the impact of legislation on waste management practices, and the use of information and computing technology in teaching environmental engineering.

Butte, Vijay Kumar, received the B.E. degree with distinction in mechanical engineering from University of Mysore, India in 2001. He is currently pursuing his Ph.D. in the Department of Industrial and Systems Engineering at the National University of Singapore. His research interests include statistical quality control, engineering process control and time series analysis.

Chaturvedi, S.K., is currently working as Assistant Professor at the Reliability Engineering Centre, Indian Institute of Technology, Kharagpur (India). He received his Ph.D. degree from the Reliability Engineering Centre, IIT, Kharagpur (India) in 2003. His research interests include network reliability, life-data analysis, and optimization, and has published papers in international and national journals. He is an assistant editor of International Journal of Performability Engineering and reviewer for the International Journal of Quality and Reliability Management.

Coffelt, Jeremy, is pursuing a Ph.D. in Water Resources Engineering at Texas A&M University. His interests are in risk and reliability analysis of water distribution systems and characterization of uncertainty in water availability modeling. He has an M.S. degree in mathematics from Kansas State University and a B.S. in mathematics and biology from Midwestern State University.

Cui, **Lirong,** is a professor in the School of Management and Economics, Beijing Institute of Technology. He received his Ph.D. degree in statistics from the University of Wales, UK, in 1994, his M.S.degree in operations research and control theory from the Institute of System Sciences, Chinese Academy of Sciences, in 1986, his B.E. degree in textile engineering in 1983 from Tianjin Polytechnic University, P.R. China. He has been working on reliability related problems since 1986. He has more than 15 years industrial working experience in quality and reliability. In 2000 he coauthored the book "Reliabilities of Consecutive-*k* Systems" published by Kluwer. His recent research interests are in stochastic modeling, quality and reliability engineering, simulation and optimization, risk management, software development for quality and reliability, operations research, supply chain management, and applications of probability and statistics in various fields. He is currently serving as an associated editor of IEEE Transactions on Reliability.

Dai, Y.S., is a faculty member of the Computer Science Department of Purdue University School of Science at IUPUI, USA. He received his Ph.D. degree from the National University of Singapore, and his bachelor degree from Tsinghua University. His research interests lie in the fields of dependability, grid computing, security, and autonomic computing. He has published 4 books, and over 70 articles in these areas. His research has been featured in the Industrial Engineer Magazine (p. 51, December, 2004). Dr. Dai is a Program Chair for the 12th IEEE Pacific Rim Symposium on Dependable Computing (PRDC2006) and a General Chair for the 2nd IEEE Symposium on Dependable Autonomic and Secure Computing (DASC06), and for the DASC07. He also chairs many other conferences and is a member of the editorial board of the International Journal of Performability Engineering. He is on the editorial board of some other journals, *e.g.,* Guest Editor for IEEE Transactions on Reliability, Lecture Notes in Computer Science, the Journal of Computer Science, and the International Journal of Autonomic and Trusted Computing. He is a member of IEEE.

Dam-Mieras, Rietje van, was born in 1948, studied chemistry at Utrecht University and obtained her Ph.D. degree in biochemistry at the same university. In 1992 she was nominated Professor of Natural Sciences, especially biochemistry and biotechnology at the Open University of the Netherlands. Her activities at this institute are in the fields of molecular sciences, sustainable development, and innovative ways of e-enhanced learning. She is actively involved in the Regional Centre of Expertise (RCE) on Learning for Sustainable Development in the region Eindhoven (NL)–Cologne (G)–Leuven (B). In addition to her work at the Open University of the Netherlands she has several advisory and supervisory functions. From 1992–1997, she was a member of the Programme Committee Science and Technology of the European Association of Distance Teaching Universities (EADTU). In 1997 she became a member of the Supervisory Board of Akzo Nobel Netherlands. From 1997–2004 she was the chairperson of the Copernicus-campus network of European universities and through this became one of the founding members of GHESP, the Global Higher Education for Sustainable Development Partnership. From 1998 until 2003 she was a member of the Dutch Scientific Council for Government Policy. Since 2000 she has been a member of the Supervisory Board of the Netherlands Organization for Applied Scientific Research (TNO). In 2002 she became a member of the program committee The Social Component in Genomics Research of the Netherlands Council for Scientific Research (NWO) and in 2005 she became a member of the Supervisory Board of Unilever Netherlands.

Dill, Glenn, is a senior software engineer for Relex Software Corporation. He is responsible for designing and programming the highly sophisticated calculation models within the Relex reliability analysis modules. He has a B.S. degree in mathematics and computer science from California University of Pennsylvania. A professional software engineer for 17 years, his previous career experiences include writing codes for high-performance computer games. His research interests include software engineering, software reliability, and high performance computing. He is a member of the IEEE Computer Society.

Ding, Yi, received his B.S. degree from Shanghai Jiaotong University, China, and his Ph.D. degree from Nanyang Technological University, Singapore. He is currently a research fellow in the Department of Mechanical Engineering University of Alberta, Canada.

El-Azzouzi, Tarik, is a research scientist, at ReliaSoft Corporation, USA. Mr. El-Azzouzi is involved in the theoretical formulation and validation of ReliaSoft's reliability analysis and modeling software products and provides reliability expertise to ReliaSoft's clients. Mr. El-Azzouzi regularly trains and lectures about various subjects of reliability and is involved in the development of courses and in the writing of reliability reference books and articles for magazines about reliability. He also has experience

with implementing reliability programs in addition to being part of reliability consulting projects for major companies. He holds an M.S. degree in reliability and quality engineering from the University of Arizona.

Feng, Qianmei, is an assistant professor in the Department of Industrial Engineering at the University of Houston, Texas. Her research interests are quality and reliability engineering, especially inspection strategies, optimization of specifications, tolerance design and optimization, reliability modeling and optimization, and Six Sigma. She received the Ph.D. degree in industrial engineering from the University of Washington, Seattle, Washington in 2005. She received her double Bachelor degrees in mechanical engineering and industrial engineering from Tsinghua University, Beijing, China (1998) with *summa cum laude*, and her Master's degree in management science from Tsinghua University (2000). Her research has been published in peer-reviewed journals such as IIE Transactions, the International Journal of Reliability, Quality and Safety Engineering, Quality Technology and Quantitative Management, and the International Journal of Six Sigma and Competitive Advantage. She is a member of IIE, INFORMS, ASQ, and Alpha Pi Mu. E-mail: qmfeng@uh.edu

Fidler, Jan, is a Ph.D. student in the Department of Industrial Technology, Ecology at the Royal Institute of Technology (KTH) in Stockholm, Sweden. Her research is focusses on risk assessment.

Fitzgerald, Daniel P., earned his M.S. degree in mechanical engineering from the University of Maryland in December 2006 and is currently a Ph.D. student at the University of Maryland. His research interests include design for environment and decision-making systems in product development.

Gogoll, Thornton H. (Ted), is the Director, Engineering Standards for the North American Power Tool and Accessories Business at Black & Decker. He reports to the Vice President of Engineering, DeWalt, and is responsible for the development and management of key global standards and processes related to the environmental, quality, and safety performance of new and existing products. Ted has a background in product development in the aerospace and consumer product areas and holds a Master's of Science degree in Mechanical Engineering from Virginia Tech.

Goh, Thong-Ngee, BE (University of Saskatchewan), PhD (University of Wisconsin-Madison), is Director at the Centre for Design Technology, and Professor of Industrial and Systems Engineering. Dr. Goh is a former dean of engineering and director of the Office of Quality Management at the National University of Singapore. He is a GE-certified Six Sigma trainer. Professor Goh is an academician of the International Academy for Quality, Fellow of the American Society for Quality (ASQ), and associate editor (Western Pacific Rim) of the ASQ Quality Engineering Journal. He is also on the editorial boards of several other international journals, such as Quality and Reliability Engineering International, International Journal of Production Economics, International Journal of Reliability, Quality, and Safety Engineering, and the TQM Magazine.

Gokhale, Swapna S., is currently an assistant professor in the Department of Computer Science and Engineering at the University of Connecticut. She received her B.E. (Hons.) in electrical and electronic engineering and computer science from the Birla Institute of Technology and Science, Pilani, India in 1994, and M.S. and Ph.D. degrees in electrical and computer engineering from Duke University in 1996 and 1998, respectively. Prior to joining the University of Connecticut, she spent one year as a post-graduate researcher at the University of California, Riverside and three years as a research scientist at Telcordia Technologies (Bell Communications Research), New Jersey. Her research interests lie in the areas of system and software reliability analysis, performance analysis of middleware and web-based

systems, and QoS issues in wireless and wire-line networks. She has published over 75 journal and conference papers on these topics.

Guikema, Seth D., is an assistant professor in the Zachry Department of Civil Engineering at Texas A&M University. His areas of expertise are risk and decision analysis, Bayesian probability modeling, and resource allocation for critical infrastructure systems. He has a Ph.D. in engineering risk and decision analysis from the Department of Management Science and Engineering at Stanford University, an M.S. in civil engineering from Stanford University, an M.E. in civil engineering from the University of Canterbury, and a B.S. in civil and environmental Engineering from Cornell University.

Haldar, Achintya, is Professor of Civil Engineering and Engineering Mechanics and a da Vinci Fellow at the College of Engineering at the University of Arizona. He received his graduate degrees (M.S., 1973 and Ph.D., 1976) from the University of Illinois, Urbana-Champaign. He also taught at Illinois Institute of Technology and at Georgia Institute of Technology. Dr. Haldar has over five years of industrial experience including working for Bechtel Power Corporation in their nuclear power division. Dr. Haldar has received many awards for his research, including the first Presidential Young Investigator Award and the ASCE's Huber Civil Engineering Research prize. He received an Honorable Diploma from the Czech Society for Mechanics. Dr. Haldar received Graduate Advisor of the Year award from the University of Arizona. He also received the Honorable Recognition Award from ASME. He received the Distinguished Alumnus award from the Civil and Environmental Engineering Alumni Association, the University of Illinois. Dr. Haldar has received numerous recognitions for his exceptional teaching including the Burlington North Foundation Faculty Achievement Award, Outstanding Faculty Member Award in 1991, 2004, and 2006, the Professor of the Year Award in 1998, and the Award for Excellence at the Student Interface in 2004 and 2005. At Gerogia Tech, Dr. Haldar received the Outstanding Teacher Award for being the best professor. He also received the Outstanding Civil Engineering Faculty Member Award in 1982 and 1987. For his services, Dr. Haldar received the Outstanding Faculty Award from the UA Asian American Faculty, Staff and Alumni Association, the Governor's Recognition Award from Governor Fife Symington of the State of Arizona, and the Service Award from the Structural Engineering Institute of ASCE. An ASCE Fellow, Dr. Haldar is a registered professional engineer in several states in the U.S. Professor Haldar is a member of the editorial board of International Journal of Performability Engineering.

He, Liping, is a Ph.D. scholar of the School of Mechanical Engineering, Dalian University of Technology, Dalian, Liaoning, 116023, China. Her research interests include reliability engineering, product warranty, design optimization, total quality management, and production and engineering management.

Hegde, Vaishali, is a member of the Reliability Department at Respironics Inc. In her role as a Senior Reliability Engineer, she is responsible for ensuring that all new medical products introduced onto the market meet the high reliability standards set by Respironics. Prior to joining Respironics, she worked as an application engineer at Relex Software Corporation. She was responsible for consulting services and assisting customers with reliability theory and reliability software. Vaishali has also worked at R&D labs in the defense industry. She has over ten years of experience in design, testing, manufacturing, and consulting. She has co-authored two papers and presented at the Reliability and Maintainability Symposium .She received her B.S. in electrical engineering from West Virginia University. She is an ASQ certified reliability engineer. Vaishali is an active member of the American Society of Quality. She has been serving on the Executive Committee of the ASQ Pittsburgh Chapter for the past three years.

Herrmann, Jeffrey W., is an associate professor at the University of Maryland, where he holds a joint appointment with the Department of Mechanical Engineering and the Institute for Systems Research. He is the director of the Computer Integrated Manufacturing Laboratory. Dr. Herrmann earned his B.S. in applied mathematics from Georgia Institute of Technology. As a National Science Foundation Graduate Research Fellow from 1990 to 1993, he received his Ph.D. in industrial and systems engineering from the University of Florida. His current research interests include the design and control of manufacturing systems, the integration of product design and manufacturing system design, and decision-making systems in product development.

Hobbs, Gregg K., Ph.D., P.E., is the originator of the principles of HALT and HASS. He has been a consulting engineer since 1978, specializing in the fields of stress screening, robust and flaw tolerant design, dynamic analysis and testing. He has been employed as a consultant by many leading companies in the aerospace, commercial, military, and industrial fields. He has introduced, and continues to introduce many new concepts, techniques, and equipment. He has authored 13 patents on equipment to perform HALT and HASS. He has also written hundreds of papers in many fields. He is the author of the book "HALT and HASS, Accelerated Reliability Engineering".

Hokstad, Per, was born July 3, 1942 in Oslo, Norway. He received his M.Sc. degree in mathematical statistics from the University of Oslo in 1968. He then had a position at the University of Science and Technology (NTNU), Trondheim, Norway until 1985, and since then he has been employed at SINTEF Safety and Reliability. During the period 1990–2000, he was also adjunct professor at NTNU. He has broad experience with both theory and applications of reliability, safety, and risk analyses. The main application areas are offshore oil and gas industry and transportation. Mr. Hokstad is a member of the editorial board of International Journal of Performability Engineering.

Huang, Hong-Zhong, is a full professor and the Dean of the School of Mechanical, Electronic, and Industrial Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, 610054, China. He has held visiting appointments at several universities in Canada, USA, and Asia. He received a Ph.D. degree in reliability engineering from Shanghai Jiaotong University, China in 1999. He has published 120 journal papers and 5 books in fields of reliability engineering, optimization design, fuzzy sets theory, and product development. He is a (senior) member of several professional societies, and has served on the boards of professional societies. He received the Golomski Award from the Institute of Industrial Engineers in 2006. His current research interests include system reliability analysis, warranty, maintenance planning and optimization, and computational intelligence in product design. Professor Huang is a member of the editorial board of International Journal of Performability Engineering.

Jha, P.C., is a reader in the Department of Operational Research, University of Delhi. He obtained his Master's degree, M. Phil., and Ph. D. from the University of Delhi. He has published more than 25 research papers in the areas of software reliability, marketing, and optimization in Indian and international journals and has edited books. He has guided M.B.A. dissertations and is also supervising Ph.D. students in operational research.

Joanni, **Andreas** studied civil engineering at the Technical University of Munich and is presently a research assistant and Ph.D. student at the same university. He has authored of a number of important publications in structural reliability.

Jugulum, Rajesh, is a researcher in the Department of Mechanical Engineering at MIT and a Vice President of Global Wealth and Investment Division of Bank of America. Rajesh earned his doctorate

degree under the guidance of Dr. Genichi Taguchi. He has published several articles in leading technical journals and magazines. He co-authored a book on pattern information technology and a book on computer-based robust engineering, and holds a US patent. He is a senior member of the American Society for Quality (ASQ) and the Japanese Quality Engineering Society, and is a Fellow of the Royal Statistical Society and International Technology Institute (ITI). He was featured as "Face of Quality" in the September 2001 issue of Quality Progress. He is the recipient of ASQ's Richard A. Freund international scholarship (2000), ASQ's Feigenbaum medal (2002), and ITI's Rockwell medal (2006). He was inducted into the world level of the Hall of Fame for science, engineering and technology in 2006 and in the same year he was listed in the "Who's Who in the World" list by Marquis.

Kafka, Peter, earned his Master's degree in mechanical engineering and his Ph.D. in thermal hydraulics from the Technical University of Graz, Austria. He worked for nine years at the Reactor Development Branch at Siemens Erlangen (D). From 1971, he worked for GRS, GmbH (Company for Plant and Reactor Safety) in the field of reliability, risk issues and probabilistic safety assessment (PSA) mainly for nuclear power plants but also for non-nuclear industries. After retirement from GRS in 2001, he is now working as an independent consultant for safety, risk and reliability (RAMS) issues for different type of systems and industries. He was General Chairman of the ESREL'99 Conference in Munich. He is Founding Member and a past Chairman of the European Safety and Reliability Association (ESRA). He is a member of the editorial board of the International Journal of Performability Engineering. For more details see www.relconsult.de.

Kapur, Kailash C. (Kal) is Professor in the Industrial Engineering Department at the University of Washington, Seattle, Washington. He was the Director of Industrial Engineering at the University of Washington from January 1993 to September 1999. He was Professor and the Director of the School of Industrial Engineering, University of Oklahoma (Norman, Oklahoma) from 1989–1992 and a professor in the Department of Industrial and Manufacturing Engineering at Wayne State University, Detroit, Michigan from1970–1989. Dr. Kapur has worked with General Motors Research Laboratories as a senior research engineer, with Ford Motor Company as a visiting scholar, and the U.S. Army, Tank-Automotive Command as a reliability engineer. Dr. Kapur has served on the Board of Directors of the American Supplier Institute, Inc., Michingan. He received his Bachelor's degree (1963) in mechanical engineering with distinction from Delhi University, his M. Tech. degree (1965) in industrial engineering from the Indian Institute of Technology, Kharagpur, his M.S. degree (1967) in operations research, and his Ph.D. degree (1969) in industrial engineering from the University of California, Berkeley. He co-authored the book Reliability in Engineering Design, published by Wiley in 1977. He has written chapters on reliability and quality engineering for several handbooks such as Industrial Engineering and Mechanical Design. He has published over 60 papers in technical, research, and professional journals. He received the Allan Chop Technical Advancement Award from the Reliability Division and the Craig Award from the Automotive Division of American Society for Quality. He is a Fellow of American Society for Quality, a Fellow of the Institute of Industrial Engineers, and a registered professional engineer. Prof. Kapur is on the editorial board of International Journal of Performability Engineering. E-mail: kkapur@u.washington.edu

Kapur, P.K., is a professor and former Head in the Department of Operational Research, University of Delhi. He is a former president of the Operational Research Society of India. He obtained his Ph.D. from the University of Delhi in 1977. He has published more than 125 research papers in the areas of hardware reliability, optimization, queueing theory, and maintenance and software reliability. He has edited three volumes and is currently editing fourth volume of Quality, Reliability and IT. He has co-authored the book Contributions to Hardware and Software Reliability, published by World Scientific, Singapore. He has edited special issues of the International Journal of Quality Reliability and Safety Engineering

(IQRSE, USA-2004) OPSEARCH, India (2005) and the International Journal of Performability Engineering (July, 2006), and is on the editorial board of the International Journal of Performability Engineering. He organized three international conferences successively in the years 2000, 2003, and 2006 on quality reliability and information technology. He has guided M.Tech./Ph.D. theses in computer science as well as in operations research. He has been invited to edit a special issue of IQRSE (2007) and a special issue of Communications on Dependability and Quality Management, Belgrade, Serbia. He has traveled extensively in India and abroad, and delivered invited talks. He is cited in "Marquis Who's Who in the World".

Kleyner, Andre, has over 20 years of experience as a mechanical engineer specializing in reliability of mechanical and electronic systems designed to operate in severe environments. He received his Doctorate in mechanical engineering from the University of Maryland, and his Master's in business administration from Ball State University, USA. Dr. Kleyner is currently employed by Delphi Corporation as a reliability and quality sciences manager, and as part of his job responsibilities he has developed and taught several training courses on reliability, quality, and design. He is a senior member of the American Society for Quality and is a certified reliability engineer. Dr. Kleyner is a recipient of the P.K. McElroy award for the best paper at the 2003 Reliability and Maintainability Symposium (RAMS). He holds several US and foreign patents, and has authored multiple papers on the topics of vibration, statistics, reliability, warranty, and lifecycle cost analysis.

Kohda, Takehisa, is an associate professor in the Department of Aeronautics and Astronautics, Kyoto University. He received his B.Eng., M.Eng., and Dr.Eng. degrees all in precision mechanics from Kyoto University in 1978, 1980, and 1983, respectively. Prior to joining Kyoto University in 1988, he worked with the National Mechanical Engineering Laboratory, Japan, as a researcher from 1983 to 1988. From 1985 to 1986, he was with the Department of Chemical Engineering, University of Houston. From 1999 to 2002, he was an associate editor of IEEE Transactions on Reliability. Since 2001, he has been a chair of the Technical Committee System Safety of the IEEE Reliability Society. Since 2004, he has been an area editor of International Journal of Performability Engineering. His interests lie in systems safety, reliability, and risk analysis. E-mail: kohda@kuaero.kyoto-u.ac.jp

Kontoleon, John, is Professor of Electronics in the Department of Electrical and Computer Engineering at the Aristotle University of Thessaloniki, Greece. He obtained his degree in physics from the University of Athens (Greece) and his Ph.D. in Electrical Engineering and Electronics from the University of Liverpool (UK). From 1972–1974, he was with the research group of the Research Directorate of the Hellenic Telecommunications Organization and from 1974–1981 he was with the Department of Electrical Engineering at the University of Wollongong (Australia). He served for many years as a member of the Executive Committee at the International Centre of Technical Co-operation (ITCC) and as a member of the Executive Committee in the European Safety and Reliability Association. He is the author of numerous research papers and is a member on the editorial boards of the International Journal of Performability Engineering, the International Journal of Reliability and Quality Management, and Facta Universitatis. His research interests include digital systems, fault tolerant systems, reliability modeling, and optimization of networks and systems.

Kulkarni, M.S., is currently working as an assistant professor at the Indian Institute of Technology Delhi in the Mechanical Engineering Department. He received his Ph.D., in manufacturing from the Indian Institute of Technology Bombay. His research interests include quality, reliability, and maintenance engineering, and their integration with operation planning.

Kumar, U. Dinesh, is Professor of Quantitative Methods and Information Systems at the Indian Institute of Management Bangalore. Professor Dinesh Kumar holds a Ph.D. in mathematics from IIT Bombay and an M.Sc. in applied sciences (Operations Research) from P.S.G. College of Technology, Coimbatore, India. Dr. Kumar has over 11 years of teaching and research experience. Prior to joining IIM Bangalore, Dr. Kumar has worked at several institutes across the world including Stevens Institute of Technology, USA, the University of Exeter, UK, the University of Toronto, Canada, the Federal Institute of Technology, Zurich, Switzerland, Queensland University of Technology, Australia, the Australian National University, Australia, and the Indian Institute of Management Calcutta. Dr. Kumar's research interests include pricing and revenue management, defense logistics, reliability, maintainability, logistics support, spare parts provisioning, Six Sigma, supply chain architecture, decision making and systems thinking. Dr. Kumar has written two books and over 50 articles in refereed International journals. Dr. Kumar is one of the leading authors of the books Reliability and Six Sigma, published by Springer, USA, and Reliability, Maintainability, and Logistic Support – A Life Cycle Approach, published by Kluwer. Dr. Kumar is Associate Editor of the Journal OPSEARCH, the Journal of the Operational Research Society of India. He is also an editorial member of the Journal Risk and Reliability published by the Institution of Mechanical Engineers (IMechE), UK, and an *ad hoc* referee for several international journals in operations research and systems engineering. Dr. Kumar was awarded the Best Young Teacher award by the Association of Indian Management Schools in 2003. E-mail: dineshk@iimb.ernet.in

Kumar, Udai, is Professor of Operation and Maintenance Engineering at Luleå University of Technology, Sweden. He is also director of The Center for Maintenance and Industrial Services, an industry sponsored neutral platform established with a main goal to facilitate exchange of maintenance related knowledge and experiences. He is also chairman of the Scientific Council of the Swedish Maintenance Society. Dr. Kumar has more than 25 years of experience in consulting and finding solutions to industrial problems directly or indirectly related to maintenance. His research and consulting efforts are mainly focused on enhancing the effectiveness and efficiency of maintenance process at both operational and strategic levels, and visualizing the contribution of maintenance in an industrial organization. Some of the manufacturing and process industries he has advised through sponsored R&D projects are ABB, Atlas Copco, SAAB Aerosystem, Statoil, LKAB, Vattenfall AB, Swedish Rail Road Administration, *etc*. Dr. Kumar has been a guest lecturer and invited speaker at numerous seminars, industrial forums, workshops, and academic institutions both in Scandinavia and overseas. He has published more than 125 papers in peer reviewed international fournals and chapters in books. He is a reviewer and member of the editorial advisory boards of several international journals, including the International Journal of Performability Engineering. His research interests are maintenance management and engineering, reliability and maintainability analysis, LCC, *etc*.

Lad, Bhupesh Kumar, received his M.E. in industrial engineering and management from Ujjain Engineering College, Ujjain, and is currently a research scholar at the Indian Institute of Technology, Delhi in the Mechanical Engineering Department. His current research interests are in the field of reliability, maintenance, and quality engineering.

Lam, Shao-Wei, holds a Bachelor's degree in mechanical engineering and a Master's degree in industrial and systems engineering from the National University of Singapore, and is a research fellow and Ph.D. candidate in the Department of Industrial and Systems Engineering, National University of Singapore. His current research interests are in the fields of quality and reliability by design and operations research in supply chain management. He has many years of experience in research, training, and consultancy, particularly in the areas of Six Sigma, robust design and statistical reliability engineering. He is a Certified Reliability Engineer (CRE) of the American Society of Quality (ASQ) and a member of the IEEE.

Levitin, Gregory, received the B.S. and M.S. degrees in electrical engineering from Kharkov Politechnic Institute (Ukraine) in 1982, a B.S. degree in mathematics from Kharkov State University in 1986, and a Ph.D. degree in industrial automation from Moscow Research Institute of Metalworking Machines in 1989. From 1982 to 1990, he worked as software engineer and researcher in the field of industrial automation. From 1991 to 1993, he worked at the Technion (Israel Institute of Technology) as a postdoctoral fellow in the Faculty of Industrial Engineering and Management. Dr. Levitin is presently an engineer-expert in the Reliability Department of the Israel Electric Corporation and an adjunct senior lecturer at the Technion. His current interests are in operations research and artificial intelligence applications in reliability and power engineering. In this field, Dr. Levitin has published more than 120 papers and four books. He is a senior member of IEEE. He serves on the editorial boards of IEEE Transactions on Reliability, Reliability Engineering and System Safety and the International Journal of Performability Engineering.

Limnios, Nikolaos, is Professor in Applied Mathematics at the University of Technology of Compiègne, France. His research interest is stochastic processes and statistics with application to reliability. He is (co-)author of the books: Semi-Markov Processes and Reliability (Birkhäuser, 2001, with G. Oprisan), Stochastic Systems in Merging Phase Space (World Scientific, 2005, with V.S.Koroliuk) and Fault Trees (ISTE, 1991, 2004, 2007). Professor Limnios is a member of the editorial board of the International Journal of Performability Engineering.

Lin, Zeng, received his Bachelor's degree majoring in mechanical design and manufacture from Jinan University in July 1997 and obtained his Master's degree majoring in motor vehicle engineering from Northeastern University in July 2001. He earned his Ph.D. in the area of vacuum and fluid engineering from Northeastern University in September 2004. Dr. Lin has a strong interest in hydrogenated amorphous carbon (a-C:H) nanofilms. He has recently worked on the models of the plasma enhanced chemical vapor deposition process in a-C:H, in order to try to understand the controlled synthesis of these materials. He has written ten papers and hold two patents on a-C:H films.

Liu, Yung-Wen, is an assistant professor in the Department of Industrial and Manufacturing Systems Engineering at the University of Michigan-Dearborn. He received his Ph.D. degree in industrial engineering from the University of Washington in 2006. He also received both his M.A. degrees in applied statistics and applied economics from the University of Michigan-Ann Arbor in 2000. His research interests include reliability theory, stochastic modeling, applied statistics, and healthcare modeling.
E-mail: ywliu@umich.edu

Lyngby, Narve, was born on January 12, 1976 in Oslo, Norway. He received his MSc degree in HSE (health, safety, and environment studies) from the University of Science and Technology (NTNU), Trondheim, Norway in 2002. Currently, he is a PhD student at the Norwegian University of Science and Technology (NTNU) in the Department of Production and Quality Engineering. He is working with degradation models for railway tracks, maintenance planning, and optimization.

Makis, Viliam, is a professor in the Department of Mechanical and Industrial Engineering, University of Toronto. His research and teaching interests are in the areas of quality assurance, stochastic OR modeling, maintenance, reliability, and production control with a special interest in investigating the optimal operating policies for stochastic controlled systems. His recent contributions have been in the area of modeling and optimization of partially observable processes with applications in CBM and multivariate

quality control. He has also contributed to the development of EMQ and other production models with inspections and random machine failures, joint SPC and APC for deteriorating production processes, scheduling of operations in FMS, reliability assessment of systems operating under varying conditions, and modeling and control of queuing systems. He was a founding member of the CBM Consortium at the University of Toronto in 1995. He is an area editor of the International Journal of Performability Engineering and has served for many years on the editorial advisory board of JQME. He is also on the advisory boards of several international conferences. He is a senior member of IIE and ASQ.

Mettas, Adamantios, is the Vice President of Product Development at ReliaSoft Corporation, USA and fulfills a critical role in the advancement of ReliaSoft's theoretical research efforts and formulations in the subjects of life data analysis, accelerated life testing and system reliability and maintainability. He has played a key role in the development of ReliaSoft's software including Weibull++, ALTA and BlockSim, and has published numerous papers on various reliability methods. Mr. Mettas holds an M.S. in reliability engineering from the University of Arizona.

Modarres, Mohammad, is Professor of Nuclear Engineering and Reliability Engineering and Director of the Center for Technology Risk Studies at the University of Maryland, College Park. His research areas are probabilistic risk assessment, uncertainty analysis, and physics of failure modeling. In the past 23 years that he has been with the University of Maryland, served as a consultant to several governmental agencies, private organizations, and national laboratories in areas related to risk analysis, especially applications to complex systems and processes such as nuclear power plants. Professor Modarres has authored over 200 papers in archival journals and proceedings of conferences, and three books in various areas of risk and reliability engineering. He is a University of Maryland Distinguished Scholar-Teacher. Professor Modarres is a member of the editorial board of International Journal of Performability Engineering. Dr. Modarres received his Ph.D. in nuclear engineering from Massachusetts Institute of Technology in 1980, his M.S. in mechanical engineering from Massachusetts Institute of Technology in 1977.

Moon, Hwy-Chang, received his Ph.D. from the University of Washington and is currently Professor of International Business and Strategy in the Graduate School of International Studies at Seoul National University. He has also taught at the University of Washington, the University of the Pacific, State University of New York at Stony Brook, Helsinki School of Economics, Kyushu University, and Keio University. Professor Moon has published numerous journal articles and books on topics such as international business strategy, foreign direct investment, and cross-cultural management. Dr. Moon is currently the Editor-in-Chief of the Journal of International Business and Economy, and is a member of the editorial board of the International Journal of Performability Engineering. He has provided consultancy to many international companies, international organizations (APEC, World Bank, UNCTAD), and governments (Korea, Malaysia).

Mullen, Robert E., is a Quality Systems Staff Engineer, Software Operations, at Cisco Systems. He received a B.A. from Princeton University and an M.S. (nuclear engineering) from Northwestern University. Prior to joining Cisco, he was the Director, Engineering. Software Support at Stratus Computers and a consulting engineer at Honeywell Multics. He is now involved with addressing software reliability issues both within Cisco and externally. At Cisco, he architected and prototyped SHARC and NARC reliability calculators for hardware and networks implemented orthogonal defect classification (ODC) and integrated software reliability growth models into the defect tracking system. He has empirically demonstrated the application of the lognormal distribution to software reliability growth.

Myers, Albert F., retired in 2006 as Corporate Vice President of Strategy and Technology for Northrop Grumman Corporation. He also served as B-2 chief project engineer, deputy program manager, and vice president of test operations. Myers earned B.S. and M.S. degrees in mechanical engineering from the University of Idaho. He was a Sloan Fellow at the Massachusetts Institute of Technology. In 2006, Myers was elected as a member of the National Academy of Engineering. Myers served from 1989 through 1998 on the NASA Aeronautics Advisory Board. He received the NASA Exceptional Service Medal and the 1981 Dryden Director's Award, and was elected to the University of Idaho Alumni Hall of Fame in 1997. E-mail: Al.Myers@ngc.com

Myers, Jessica, received her B.S. degree in mechanical engineering in 2005 from the University of Maryland, College Park. She is currently completing a MS degree in mechanical engineering at the University of Maryland. Ms. Myers research work is on obsolescence driven design refresh planning and the connection of technology road-mapping to the design refresh optimization process. E-mail: jlmyers@wam.umd.edu

Naikan, V.N.A., is currently an associate professor in the Reliability Engineering Centre of the Indian Institute of Technology, Kharagpur, India, where he teaches quality and reliability engineering to undergraduate and post-graduate students. He was born in the Indian state of Kerala in 1965 and graduated in mechanical engineering from the University of Kerala with second rank and pursued his M.Tech. and Ph.D. studies in reliability engineering at the Reliability Engineering Centre and obtained these degrees from the Indian Institute of Technology, Kharagpur. He started his professional carrier with Union Carbide India Limited and thereafter worked in the Indian Space Research Organization and the Indian Institute of Management, Ahmedabad, India. Thereafter, he joined the Indian Institute of Technology Kharagpur as a faculty member. He has published more than 50 research papers, organized several short term courses, has done research projects and consultancies in related areas. He has been a referee for many international journals.

Nakagawa, Toshio, is currently Professor of Information Science at Aichi Institute of Technology in Toyota. He received his Ph.D. from Kyoto University in 1977. He has authored two books entitled on "Maintenance Theory of Reliability" (2005) and "Shock and Damage Models in Reliability Theory" (2007). Springer will publish his book entitled "Advanced Reliability Models and Maintenance Policies" in 2008. He also has 6 book chapters and more than 150 journal research papers to his credit. His research interests lie in the area of optimization problems, applications to actual models, and computer and information systems in reliability and maintenance theory. He now researching new and latest topics in reliability engineering, computer and management sciences, and discusses them. Dr. Nakagawa is a member of the editorial board of the International Journal of Performability Engineering.

Nanda, Vivek (Vic), is a Quality Manager at Motorola at Horsham, PA, USA. He is a CMQ/OE, CSQE, CQA, Certified ISO 9000 Lead Auditor, and Certified in ITIL Foundations. He is the author of the books ISO 9001:2000 Achieving Compliance and Continuous Improvement in Software Development Companies (ASQ Quality Press, 2003), and Quality Management System Handbook for Product Development Companies (CRC Press, 2005). He is a member of the editorial review board of the Software Quality Professional Journal, and a member of the reviewer panels of IEEE Software, and ASQ Quality Press. Vic is a Senior Member of the ASQ and a Steering Committee member of the Philadelphia SPIN. Vic has been awarded the Feigenbaum medal (2006) by the American Society for Quality. He is listed in the 60th and 61st editions of "Marquis Who's Who in America", in the ninth edition of "Marquis Who's Who in Science and Engineering (2006–2007)", and in the first edition of "Marquis Who's Who of

Emerging Leaders", 2007. Vic has a MS degree in computer science from McGill University (Canada) and Bachelor's degree in engineering from the University of Pune (India).

Nathan, Swami, is a senior staff engineer at Sun Microsystems. His field of interest is field data analysis, statistical analysis and reliability/availability modeling of complex systems. He received his B.Tech. from the Indian Institute of Technology, and M.S. and Ph.D. degrees in reliability engineering from the University of Maryland, College Park. He has authored over 20 papers in peer reviewed journals and international conferences and holds two patents.

O'Connor, Patrick, received his engineering training at the UK Royal Air Force Technical College. He served for 16 years in the RAF Engineer Branch, including tours on aircraft maintenance and in the Reliability and Maintainability office of the Ministry of Defence (Air). He joined British Aerospace Dynamics in 1975, and was appointed Reliability Manager in 1980. In March 1993 he joined British Rail Research as Reliability Manager. Since 1995 he has worked as an independent consultant on engineering management, reliability, quality, and safety. He is the author of "Practical Reliability Engineering", published by Wiley (4th edition 2002), "Test Engineering" (Wiley 2001), and "The Practice of Engineering Management", (Wiley 1994) (updated and re-published as "The New Management of Engineering" in 2005). He is also the author of the chapter on reliability and quality engineering in the Academic Press Encyclopaedia of Physical Science and Technology, and until 1999 was the UK editor of the Wiley journal Quality and Reliability Engineering International. He has written many papers and articles on quality and reliability engineering and management, and he lectures at universities and at other venues on these subjects. In 1984 he received the Allen Chop Award, presented by the American Society for Quality, for his contributions to reliability science and technology. For a more detailed description of his past and current work, visit www.pat-oconnor.co.uk.

Pecht, Michael G., is Chair Professor and the Director of the CALCE Electronic Products and Systems Center at the University of Maryland. Dr. Pecht has an MS in electrical engineering and MS and PhD degrees in engineering mechanics from the University of Wisconsin at Madison. He is a Professional Engineer, an IEEE Fellow, an ASME Fellow, and a Westinghouse Fellow. He has written 11 books on electronics products development. He has written six books on the electronics industry in S.E. Asia. He served as chief editor of the IEEE Transactions on Reliability for eight years and on the advisory board of IEEE Spectrum. He is currently the chief editor of Microelectronics Reliability and is a member of the editorial board of the International Journal of Performability Engineering. He serves as a consultant for various companies, providing expertise in strategic planning, design, test, and risk assessment of electronic products and systems.

Pham, Hoang, is Professor and Director of the undergraduate program of the Department of Industrial and Systems Engineering at Rutgers University, Piscataway, NJ. Before joining Rutgers, he was a senior engineering specialist at the Boeing Company, Seattle, and the Idaho National Engineering Laboratory, Idaho Falls. He has authored and coauthored over 150 papers, 4 books, 2 handbooks, and 10 edited books. He is editor-in-chief of the International Journal of Reliability, Quality and Safety Engineering, associate editor of the IEEE Transactoins on Systems, Man, and Cybernetics, and the editor of the Springer Series in Reliability Engineering. He has served on the editorial boards of over 10 international journals including the International Journal of Performability Engineering, and as conference chair and program chair of over 30 international conferences and workshops. He is a Fellow of the IEEE.

Rackwitz, Rüdiger, has been Professor of Structural Reliability at the Technical University of Munich since 1985. He studied civil engineering at the Technical University of Munich and continued there as a

principal research associate working primarily in the development of structural reliability methods and modeling of uncertain phenomena. He is author of over 100 reviewed publications and even more for conferences and symposia. He is a member of the editorial board of the International Journal of Performability Engineering.

Rai, Suresh, is a professor with the Department of Electrical and Computer Engineering at Louisiana State University, Baton Rouge, Louisiana. Dr. Rai has taught and researched in the area of network traffic engineering, ATM, reliability engineering, fault diagnosis, neural net-based logic testing, and parallel and distributed processing. He is a co-author of the book "Wave Shaping and Digital Circuits", and the tutorial texts "Distributed Computing Network Reliability" and "Advances in Distributed System Reliability". He was an associate editor for IEEE Transactions on Reliability from 1990 to 2004. Currently, he is on the editorial board of the International Journal of Performability Engineering. Dr. Rai is a senior member of the IEEE.

Ramirez-Marquez, Jose E., is an assistant professor at Stevens Institute of Technology in the Department of Systems Engineering and Engineering Management. His research interests include system reliability and quality assurance, uncertainty modeling, meta-heuristics for optimization, applied probability and statistical models, and applied operations research. He has authored more than 20 articles in leading refereed technical journals and has conducted funded research for the both government and commercial organizations on these topics. He obtained his Ph.D. degree at Rutgers University in industrial and systems engineering and received his B.S. degree in actuarial science from UNAM in Mexico City in 1998. He also holds M.S. degrees in industrial engineering and statistics from Rutgers University. He is a member of IIE, IFORS, and INFORMS.

Rausand, Marvin, was born on December 20, 1949 in Nesset, Norway. He was educated at the University of Oslo and was employed at SINTEF Safety and Reliability for ten years until 1989. The last four years of this period, he was head of this department. Since 1989 he has been a professor in reliability engineering at the Norwegian University of Science and Technology. His research activities have mainly been related to safety and reliability issues in the offshore oil and gas industry.

Rauzy, Antoine, received his Ph.D. in computer sciences in 1989 and a "habilitation à diriger des recherches" in 1996. He joined the Centre National de la Recherche Scientifique in 1991 and the Institut de Mathématiques de Luminy in 2000. His topics of research are reliability engineering, formal methods, and algorithms. He has authored more than 100 articles for international conferences and journals. His main contributions lie in the area of design of algorithms and high level formalisms for risk analysis. He has designed various software products including the fault tree assessment tool Aralia. Since 2001, he has been the president of the ARBoost Technologies Company. http://iml.univ-mrs.fr/~arauzy/; E-mail: arauzy@iml.univ-mrs.fr

Renn, Ortwin, serves as full professor and chair of environmental sociology at Stuttgart University, Germany. He directs the Interdisciplinary Research Unit for Risk Governance and Sustainable Technology Development (ZIRN) at the University of Stuttgart and the non-profit company DIALOGIK, a research institute for the investigation of communication and participation processes in environmental policy making. Ortwin Renn has a doctoral degree in sociology and social psychology from the University of Cologne. His professional career began with an appointment at the National Research Center, Julich; he served as professor at Clark University (Worcester, USA)and at the Swiss Institute of Technology (Zurich), and directed the Center of Technology Assessment in Stuttgart for ten years. He is a member of the panel on Public Participation in Environmental Assessment and Decision Making of the U.S. National

Academy of Sciences in Washington, D.C., an ordinary member of the Berlin-Brandenburg Academy of Sciences (Berlin), the German Academy for Technology and Engineering, and the European Academy of Science and Arts (Vienna and Salzburg). His honors include the Distinguished Achievement Award of the Society for Risk Analysis (SRA) and the Outstanding Publication Award from the Environment and Technology Section of the American Sociological Association. Professor Renn is primarily interested in risk governance, political participation, and technology assessment. He has published more than 30 books and 200 articles.

Sandborn, Peter A., is an associate professor and the Research Director for the CALCE Electronic Products and Systems Center (EPSC) at the University of Maryland. His interests include technology tradeoff analysis for electronic packaging, virtual qualification of electronic systems, parts selection and management for electronic systems, including electronic part obsolescence forecasting and management, supply chain management and design for environment of electronic systems, and microelectromechanical systems (MEMS), system lifecycle and risk economics. Prior to joining the University of Maryland, he was a founder and Chief Technical Officer of Savantage, Inc. Prof. Sandborn has a Ph.D. degree in electrical engineering from the University of Michigan and is the author of over 100 technical publications and several books on multichip module design and electronic parts. He is an associate editor for the IEEE Transactions on Electronics Packaging Manufacturing and a member of the editorial board of the International Journal of Performability Engineering. E-mail: sandborn@umd.edu

Schmidt, Linda C., is an associate professor at the University of Maryland, where she holds a joint appointment with the Department of Mechanical Engineering and the Institute for Systems Research. She is the founder and director of the Designer Assistance Tool Laboratory. She completed her doctorate in mechanical engineering at Carnegie Mellon University and developed a grammar-based, generate and optimize approach to mechanical design. Her B.S. and M.S. degrees were granted by Iowa State University for work in industrial engineering with a specialization in queuing theory, the theory of waiting in lines. Her research interests include computational design, design optimization, and developing formal methods for design.

Sharit, Joseph, received his B.S. degree in chemistry and psychology from Brooklyn College and his M.S. and Ph.D. degrees from the School of Industrial Engineering at Purdue University. He is currently a research professor in the Department of Industrial Engineering at the University of Miami. He also holds secondary appointments in the Department of Anesthesiology and in the Department of Psychiatry and Behavioral Sciences at the University of Miami Miller School of Medicine. He is involved in research with the Center on Research and Education for Aging and Technology Enhancement, the Ryder Trauma Center, and the Miami Patient Safety Center. His research interests include human–machine interaction, human reliability analysis and system safety, aging and performance on technologically-based tasks, and human decision making. His current teaching responsibilities include the areas of probability and statistics, system safety engineering, human factors engineering and occupational ergonomics, and engineering economy.

Singh, Jagmeet, received his Ph.D. degree from the Department of Mechanical Engineering at MIT, U.S.A. He received a S.M. degree in mechanical engineering from MIT, in 2003 and a B.Tech. degree in mechanical engineering from the Indian Institute of Technology, Kanpur, India. He worked on the subject of his chapter as a part of his research towards his Ph.D. His areas of expertise include assembly architecture, datum flow chains, and noise strategies in large scale systems.

Singh, V.B., is a lecturer in the Department of Computer Science, Delhi College of Arts and Commerce (University of Delhi). He obtained his M.C.A degree from the M.M.M. Engineering College, Gorakhpur, India. Presently, he is working towards a Ph.D. degree at the University of Delhi. His area of research is software reliability.

Soh, Sieteng, is a lecturer with the Department of Computing at Curtin University of Technology, Perth, Australia. He was a faculty member (1993–2000), and the Director of the Research Institute (1998–2000) at Tarumanagara University, Indonesia. He has a B.S. degree in electrical engineering from the University of Wisconsin, Madison, and M.S. and Ph.D. degrees in electrical engineering from Louisiana State University, Baton Rouge. His research interests include network reliability, and parallel and distributed processing. He is a member of the IEEE.

Spitsyna, Anna is currently a Ph.D. student in the Department of Industrial Technology, Ecology at the Royal Institute of Technology (KTH) in Stockholm, Sweden. Her research interest is focussed on sustainable technology.

Stahel, Walter R., founded the Product-Life Institute in Geneva in 1982 and has been its director since then. He is visiting professor in the School of Engineering, University of Surrey, UK, head of the Geneva Association's Risk Management Research program, guest lecturer at Tohoku University, and lecturer at University Pforzheim, Germany. A graduate of the Swiss Federal Institute of Technology in Zurich, he has authored several prize-winning papers, and the books The Performance Economy (2006, in English and Chinese) and The Limits to Certainty (with Orio Giarini 1992), published in six languages. Websites: http://product-life.org http://performance-economy.org http://genevaassociation.org

Tang, Loon-Ching, is an associate professor and Deputy Head (Research) of the Department of Industrial and Systems Engineering. He obtained a Ph.D. degree in 1992 from Cornell University in the field of operations research with minors in statistics and civil engineering. Dr. Tang has published widely in more than 20 international peer-reviewed journals, including IEEE Transactions on Reliability, Journal of Quality Technology, Naval Research Logistics and Queueing Systems. Besides being the area editor (quality engineering) of the International Journal of Performability Engineering since its inception, Professor Tang is on the editorial review board of the Journal of Quality Technology and has been an active reviewer for a number of international journals. He has been consulted on problems demanding innovative application of probability, statistics and other operations research techniques, and is also a well-known trainer in Six Sigma. He is the main author of the book "Six Sigma: Advance Tools for Black Belts and Master Black Belts" (Wiley). His research interest includes the application of operations research tools, particularly statistics, probability and optimization techniques, to problems with high degree of uncertainty. His research is motivated by actual problems from industries, ranging from those in the area of quality and reliability to those related to business processes and operations strategies.

Trindade, David, is a Distinguished Engineer at Sun Microsystems. Formerly, he was a Senior Fellow at AMD. His fields of expertise include reliability, statistical analysis, and modeling of components, systems, and software, and applied statistics, especially design of experiments (DOE) and statistical process control (SPC). He is co-author (with Dr. Paul Tobias) of the book Applied Reliability (second edition, published in 1995). He has a B.S. degree in physics, an M.S. degree in statistics, an M.S. degree in material sciences and semiconductor physics, and a Ph.D. degree in ,mechanical engineering and statistics. He has been an adjunct lecturer at the University of Vermont and Santa Clara University.

Trivedi, Kishor S., holds the Hudson Chair in the Department of Electrical and Computer Engineering at Duke University, Durham, NC. He has been on the Duke faculty since 1975. He is the author of a well known text entitled Probability and Statistics with Reliability, Queuing and Computer Science Applications (published by Prentice-Hall; a thoroughly revised second edition (including its Indian edition) of this book has been published by Wiley. He has also published two other books entitled Performance and Reliability Analysis of Computer Systems (published by Kluwer) and Queueing Networks and Markov Chains (published by Wiley). He is a Fellow of the Institute of Electrical and Electronics Engineers. He is a Golden Core Member of the IEEE Computer Society. He has published over 400 articles and has supervised 40 Ph.D. dissertations. He is on the editorial boards of IEEE Transactions on Dependable and Secure Computing, the Journal of Risk and Reliability, the International Journal of Performability Engineering, and the International Journal of Reliability, Quality and Safety Engineering. He has made seminal contributions in software rejuvenation, solution techniques for Markov chains, fault trees, stochastic Petri nets, and performability models. He has actively contributed to the quantification of security and survivability. He was an editor of the IEEE Transactions on Computers from 1983–1987. He is a co-designer of the HARP, SAVE, SHARPE, and SPNP software packages that have been well circulated. e-mail: kst@ee.duke.edu

Tuchband, Brian, received the B.S. degree in mechanical engineering from the University of Delaware in 2005. He is currently working towards the M.S. degree in mechanical engineering at the University of Maryland, College Park. His research interests include health and usage monitoring systems, and prognostic solutions for military electronic systems.

Vassiliou, Pantelis, is President and CEO, ReliaSoft Corporation, USA. Mr. Pantelis Vassiliou directs and coordinates ReliaSoft's R&D efforts to deliver state-of-the-art software tools for applying reliability engineering concepts and methodologies. He is the original architect of ReliaSoft's Weibull++, a renowned expert and lecturer on reliability engineering and is ReliaSoft's founder. He is currently spearheading the development of new technologically advanced products and services. In addition, he also consults, trains, and lectures on reliability engineering topics to Fortune 1000 companies worldwide. Mr. Vassiliou holds an M.S. degree in reliability engineering from the University of Arizona.

Vatn, Jørn, was born on January 24, 1961 in Inderøy, Norway. He received his M.Sc. degree in mathematical statistics from the University of Science and Technology (NTNU), Trondheim, Norway in 1986, and his Ph.D. degree from the same university in 1996, with a thesis on maintenance optimization. He has almost 20 years of experience as a researcher at SINTEF Safety and Reliability, and currently he holds the position of a professor at NTNU, Department of Production and Quality Engineering.

Vichare, Nikhil M., received the B.S. degree in production engineering from the University of Mumbai, India, and the M.S. degree in industrial engineering from the State University of New York at Binghamton. He is currently working towards the Ph.D. degree in mechanical engineering at the University of Maryland, College Park, in the area of electronic prognostics.

Wang, Peng, received his B.Sc. degree from Xian Jiaotong University, China, in 1978, the M. Sc. degree from Taiyuan University of Technology, China, in 1987, and also M.Sc. and Ph.D. degrees from the University of Saskatchewan, Canada, in 1995 and 1998, respectively. Currently, he is an associate professor of Nanyang Technological University, Singapore.

Wang, Zheng, received his B.S. in Mmchanical design from Shenyang Institute of Technology, China in 2003 and is currently a Ph.D. candidate in the Mechanical Engineering Department of Northeastern

University, Shenyang, China. His research interests are in mechanical system reliability and structural fatigue.

Wennersten, Ronald, is head of the Department of Industrial Ecology at Royal Institute of Technology (KTH) in Stockholm, Sweden. He received his Ph.D. in chemical engineering at Lund University in 1981. After working in the industry for some time, he came to KTH in 1996. Afterwards, he became head of the Department of Industrial Ecology in 2000. His ambition has been to merge existing research in the areas of environmental management and environmental system analysis with his own research on risk management within the framework of industrial ecology and sustainable development. He is head of the Joint Research Center for Industrial Ecology at Shandong University in China, where he is a guest professor.

Wu, Jianmou, is a recent Ph.D. graduate from the Department of Mechanical and Industrial Engineering, University of Toronto. His research interests are CBM modeling and optimization, development of condition monitoring and fault detection schemes for deteriorating equipment, statistical data analysis, multivariate time series modeling, and stochastic OR modeling.

Xie, Liyang, has been a professor in the Department of Mechanical Engineering at Northeastern University, Shenyang, China, since 1992. He received his B.S. degree (1982) in mechanical manufacturing, his M.S. (1985) and Ph.D. (1988) degrees in mechanical fatigue and reliability from Northeastern University, Shenyang, China. He has published more than 100 papers in journals such as IEEE Transactions on Reliability, Reliability Engineering and System Safety, Fatigue and Fracture of Engineering Materials and Structures, the International Journal of Performability Engineering, and the International Journal of Reliability, Quality and Safety Engineering. His research interests are in structural fatigue, system reliability, and probability risk assessment. E-mail: lyxie@me.neu.edu.cn

Xing, Liudong, received her B.E. degree in computer science from Zhengzhou University, China, in 1996, and was a research assistant at the Chinese Academy of Sciences from 1996 to 1998. She was awarded M.S. and Ph.D. degrees in electrical engineering from the University of Virginia, Charlottesville, in 2000 and 2002, respectively. Since 2002, Dr. Xing has been an assistant professor in the Electrical and Computer Engineering Department, University of Massachusetts Dartmouth. Dr. Xing served as an associate guest editor for the Journal of Computer Science for a special issue of Reliability and Autonomic Management, and program co-chair for the IEEE International Symposium on Dependable, Autonomic and Secure Computing in 2006. She also serves as a program vice chair for the 2007 International Conference on Embedded Software and Systems. She is an editor of short communications in the International Journal of Performability Engineering. She is a member of IEEE and Eta Kappa Nu. E-mail: ldxing@ieee.org

Yamada, Shigeru, was born in Japan, on July 6, 1952. He received the B.S.E., M.S., and Ph.D. degrees from Hiroshima University, Hiroshima, Japan, in 1975, 1977, and 1985, respectively. From 1977 to 1980, he worked at the Quality Assurance Department of Nippondenso Company, Japan. From 1983 to 1988, he was an assistant professor of the Okayama University of Science, Okayama, Japan. From 1988 to 1993, he was an associate professor at the Faculty of Engineering, Hiroshima University. Since 1993, he has been working as professor with the Faculty of Engineering, Tottori University, Tottori, Japan. He has published numerous technical papers in the areas of software reliability engineering, project management, reliability engineering, and quality control. He has authored several books entitled Software Reliability: Theory and Practical Application (Soft Research Center, 1990), Introduction to Software Management Model (Kyouritsu Shuppan, 1993), Software Reliability Models: Fundamentals and Applications (JUSE, 1994),

Statistical Quality Control for TQM (Corona Publishing, 1998), Software Reliability: Model, Tool, Management (The Society of Project Management, 2004), and Quality–Oriented Management Technology for toftware Projects (Morikita Publishing, 2007). Dr. Yamada is the recipient of the Best Author Award from the Information Processing Society of Japan in 1992, the TELECOM System Technology Award from the Telecommunications Advancement Foundation in 1993, the Best Paper Award from the Reliability Engineering Association of Japan in 1999, the International Leadership Award in Reliability Engineering Research from the ICQRIT/SRECOM in 2003, and the Best Paper Award from the Society of Project Management in 2006. He is a regular member of IEICE, the IPSJ, the ORSJ, the Japan SIAM, the REAJ, the JIMA, the JSQC, the Society of Project Management, and the IEEE. He is on the editorial board of the International Journal of Performability Engineering.

Yoshimura, Masataka, earned his Bachelor of Engineering degree in mechanical engineering, his Master of Engineering Degree in precision engineering from Kyoto University, and received his Doctor of Engineering degree from Kyoto University in 1976. He is currently a professor in the Graduate School of Engineering at Kyoto University. His research interests include concurrent optimization of product design and manufacturing, information systems for manufacturing, collaborative optimization, concurrent engineering, and the dynamics of machine tools and industrial robots. He has published more than 180 papers in journals and proceedings of the ASME, AIAA, IJPR, CERA (Concurrent Engineering: Research and Applications), Structural Optimization, JSME (Japan Society of Mechanical Engineers), and JSPE (Japan Society for Precision Engineering), and elsewhere. He has received awards from the JSPE and the Japan Society for the Promotion of Machine Tool Engineering, an achievement award from the Design Engineering Division of JSME, and remarkable service awards from the Design Engineering Division of ASME. He is a Fellow of ASME, JSME, and JSPE.

Yuanbo, Li, is Ph.D. candidate in Department of Industrial Engineering & Management, School of Mechanical Engineering, Shanghai Jiao Tong University, China. His main research interests include semiconductor manufacturing scheduling and simulation.

Zhibin, Jiang, is Professor and Chairman of Industrial Engineering and Management at Shanghai Jiao Tong University (SJTU). He obtained his Ph.D. degree in manufacturing engineering and engineering management from City University of Hong Kong in 1999. He is a senior member of IEEE and IIE, and 2006–2007 President of the Beijing (China) chapter of IIE. He is member of the editorial boards of the International Journal of Performability Engineering and IJOE. He has authored more than 100 papers in international journals and at conferences. His research interests include system modeling and simulation, production planning and scheduling, and system reliability. He has been included in the 2006–2007 edition of "Who's Who in Science and Engineering".

Zhou, P., received the B.S. degree in computational mathematics and the M.S. degree in operations research from Dalian University of Technology, China, in 2000 and 2003, respectively. Currently, he is a Ph.D. candidate in the Department of Industrial and Systems Engineering, National University of Singapore. His main research interests include energy and environmental systems analysis, efficiency and productivity analysis, performance measurement, and multiple criteria decision analysis.

Zuo, Ming J., received the Bachelor of Science degree in agricultural engineering in 1982 from Shandong Institute of Technology, China, and the Master of Science degree in 1986 and the Ph.D. degree in 1989 both in industrial engineering from Iowa State University, Ames, Iowa, USA. He is currently a professor in the Department of Mechanical Engineering at the University of Alberta, Canada. His research interests include system reliability analysis, maintenance planning and optimization, signal processing, and fault

diagnosis. He is Associate Editor of IEEE Transactions on Reliability, Department Editor of IIE Transactions, area editor of the International Journal of Performability Engineering, and editorial board Member of International Journal of Quality, Reliability and Safety Engineering. He is a senior member of IEEE and IIE. He received the Killam Professorship Award in 2004 and the McCalla Professorship Award in 2002 at the University of Alberta. He received the 2006 IIE Golomski Award and the Best Paper Award at the 2005 IIE Industrial Engineering Research Conference.

Index

Abrasive wear, 956
Acceleration factor, 551
Acceptance sampling, 173, 180, 181, 184
Accident cause analysis, 683
Accident occurrence condition, 684
Accoustic emission (Ultrasonics), 762
Acquisition reform, 91
Activation energy, 550
Active redundancy, 525
Active signals, 243
Adhesive wear, 956
Ad hoc on demand distance vector (AODV), 1063
Ad hoc network, 1047
Advanced first-order second-moment method, 1029
Age-based policy, 825–827, 832, 833
Age-dependence model, 793
Age-dependent repair, 1154
Age replacement, 760, 790
Agenda, 65, 862
Aging, 1143
Akaike information criterion (AIC), 1196
ALARP, 729
Aleatory uncertainty 477–478, 486
Algorithm, 309–315, 321, 323, 333, 337–339
    Doyle, Dugan & Patterson (DDP), 324, 333, 334
    k-out-of-n system, 339
    Simple and efficient (SEA), 324, 336
Algorithmic statistical process control (ASPC), 220
Algorithmic techniques (ABFT), 1094
All-terminal reliability, 1049
Allowable stress design, 1026
Amorphous hydrogenated carbon, 967
Analysis phase, 1195
Analysis phase, 1013–1019
Antithetic variates vrt, 1038
Approximate method, 278, 506, 509, 510
    Geometric programming, 510, 516
Approximations, 318, 319, 324
    MTTF, 314
    Harmonic number, 316
    With repair, 316
        Reliability, 318
        Failure rate, 316
Arithmetic codes, 1091
Arrhenius, 569
Arrhenius relationship, 548, 549, 550
Artificial neural networks, 1041
Assertion, 1094
Associativity, 99
Asymmetrical cluster 1098
ATM, 1184
Atomic hydrogen, 970–971
Attribute test, 535
Auto-covariance matrix, 830, 836
Availability, 76, 81–88, 309, 314, 499, 501, 513, 514, 767, 782, 790–792, 1135, 789–791, 793, 799, 814, 815, 816, 1151
    Average up-time availability, 87
    Indices, 848
    Inherent availability, 87
    Instantaneous availability, 87
    Interval availability, 767
    Operational availability, 87–89
    Point availability, 87
Availability measures, 309
    Steady-state, 309
        Availability, 309, 314
        Expected down-time (ED), 311
        Expected up-time (EU), 311
        Failure frequency, 309
        Mean cycle time (MCT), 309
        Mean down time (MDT), 309
        Mean time to failure (MTTF), 309, 312
        Mean time to repair (MTTR), 311, 314

Mean up time (MUT), 309
Number of system failures (NSF), 309
Number of system repairs (NSR), 309
Time-specific, 315
Availability, 315
Failure frequency, 315
Availability of a semi-Markov system, 372
Asymptotic normality of the estimator, 375
Estimator of, 375
Explicit form of, 374
Strong consistency of the estimator, 376
Availability trade offs, 767
Average availability, 790
Average factorial effects, 241
Average number of failures, 791
Average voting, 1094

Back propagation algorithm, 513
Back up server, 1095
Ballast cleaning, 1126
Ballast pressure, 1130
Barrier modeling, 1132
Baseline hazard function, 837
Bathtub curve, 1127, 1128
Bayesian analysis, 540, 586–592
Bayesian analysis of launch vehicle, 589
Bayesian generalized models, 591
Bayesian model for count data, 580
Reliability, 583
Formulation of priors, 587
Maximum entropy, 588
Maximum likelihood, 588
Method of moments, 588
Pre-prior updating, 389
Behavioral decomposition, 323
Benefit, 1147–1148
Best available techniques, 859, 863
Best practicable environmental option, 863
Bias-voltage, 959, 968
Bilateral contracts, 1163, 1165, 1170, 1172–1173
Bill Gates, 95, 103
Binary decision diagram (BDD), 344, 347–348, 353–356, 365, 381, 603–608, 616
Boolean algebra, 350, 352, 357
Conversion, 604
Data Structure, 381
Else edge, 603
If-then-else (ite) format, 603
Logical operations, 384
Multi-state, 362
Ordered, 604
Recursive algorithm, 606
Reduced ordered, 604, 605
Reduction rule, 604
Isomorphic, 603
Shannon decomposition, 603
Then edge, 603
Useless node, 605
Variable ordering heuristics, 394
Zero-suppressed BDD, 384
Binary, 335
Binary-state model, 432
Binomial, 312, 314
Bio-informatics, 935
Biotechnology, 852, 920
Block maintenance policy, 796, 797
Block replacement, 790
BMW, 888
Boltzman's constant, 550
Boolean algebra, 350, 352, 357, 367, 387
Boolean reduction, 706
Bounded feedback adjustment, 214
Branch and bound, 506
Breakage process, 1211
Bring-back rewards, 133
British standard BS5760, 38
Broadband, 570
Broadcast, many-to-one, multicast, unicast, 1049
Broadcast (s,T), 1033, 1049
Brown Bovery company, 167
Brundtland report, 12, 81
BT, 876
Bug, 256
Burn-in, 500, 573
Bus cycle level synchronization, 1095
Business models, 127, 128, 130, 132, 134, 137, 138, 885
Business models and strategies, 885
Business strategies, 131
B_X life, 535
Byzantine faults, 1087, 1094, 1095

Calendar time function, 398, 406, 409
CALREL, 1041
Capacitively coupled, 969
Capacity of repair, 791
Carrying capacity of earth, 3
Cascading failure, 620, 637
Case study, 996
Causes of failure, 31
Cautionary principle, 729
CBM model building, 836
CCF models, 821
Alpha factor, 631
Basic parameter, 631
Beta-factor, 621

Binomial failure rate, 630
C-factor model, 627
Explicit, 625
Implicit, 625
Markov, 625
Multiple beta-factor, 630
Multiple Greek letter, 630, 631
Unified partial, 629
Circuit stability design, 239
Common Cause Failure (CCF), 349–350, 353, 357, 363–365, 612, 620–622
CCF event, 622
Common cause (CC), 363–365, 612–613
Common cause event (CCE), 363, 612
Common cause group (CCG), 363, 606, 613
Defense, 623
Efficient decomposition and aggregation (EDA), 363, 612
Central limit theorem (CLT), 1210
Alternative conditions, 1210
Applied to software rates, 1210
Multiplicative forms, 1210
CE mark, 37
Characteristic life, 808
Characteristics, 1048
Checking point, 1030
Checkpointing, 1093
Checking programming technique 1094
Chemical inertness 967
Chloride corrosion, 1158
Chloride penetration, 1150, 1152
Classical perturbation, 1039
Classical regression models for count data, 580
Generalized additive models, 580
Generalized linear mixed models, 580
Generalized linear models, 580
Ordinary least squares regression, 580
Zero-inflated models, 582
Cleaner production, 139, 856
Definition, 139
Dissemination, 141
Lessons learned, 151
Closed loop supply chain, 875, 881
CLT, *see* Central limit theorem
Clustering, 1210
CNG Fire hazard, 710
Gas dispersion, 712
Ignition likelihood, 712
Code coverage, 1209
Coding, 1091
COGEM, 939
Collision accident, 684
Combinatorial approaches, 323, 349, 351, 355, 367
Combined code, 861
Commercial off the shelf (COTS), 83, 103
Common mode failures, 1092
Communication network, 1047
Complexity, 309–311, 313–315, 317
Components, 309–312, 314, 316, 317
Identical, 309, 310
Non-identical, 309–312
Repairable, 311, 312, 314, 316, 317
Non-repairable, 309, 310
Component failure models, 1047
Component improvement program, 500
Components of risk, 716, 746
Ambiguity, 746
Complexity, 746
Uncertainty, 746
Component mixing, 509
Component reliability, 414, 416, 418
Component-state, 334, 339
Component state probability, 435
Component state space, 433
Composite indicators, 905
Composite sustainability indicators, 906
Definition, 905
Examples, 906
Pros and cons, 907
Composition operators, 450
Compounding of noise factors, 240
Computational complexity, 502
Computational time, 506, 511, 515
Computer-based robust engineering, 235
Computer communication network design, 529
Computer system, 807, 819–821, 1193
Computer-integrated manufacturing (CIM), 48
Computerized maintenance management system (CMMS), 765
Computing link availability, 1052
Concept design, 236
Concurrent engineering, 48, 169
Concurrent optimization, 48
Condition monitoring, 757, 774–775, 783–787, 825, 828, 834
Off line, 835
Online, 785
Confidence level, 86
Conditional expectation VRT, 1037
Conditional sojourn times distributions,
Definition, 369
Estimator, 375, 376
Condition-based maintenance, 825, 835, 840, 1108, 1156
Confidence level, 533
Consequence characteristics, 737

Constant failure rate, 86
Construction of composite sustainability indicators, 905
  Data envelopment analysis, 905
    Efficiency measure, 911
    Environmental dea technology, 911
    Environmental performance index, 911
    Production technology, 911
    Radial environmental index, 911
    Slacks-based environmental index, 912
  MCDA-DEA approach, 12
    Models, 912
    Properties, 913
Continual improvement process, 245, 247, 249
Control charts, 182, 183, 187
Control charts for attributes, 194
  Cumulative conformance count, 197
  Defects per unit, 196
  Non-conformities, 188, 195, 196
  Number of demerits, 196
Control charts for variables, 190
  ACUSUM, 192
  CUSUM, 192, 195, 199
  EWMA, 192, 195
  Mean and range, 190
  Mean and standard deviation, 191
  Moving average, 192, 193, 195, 197
  Moving range, 191, 192
  Multivariate, 193, 194, 197
  Trend, 188, 192–194
Control factors, 237, 239
Control function for safety, 684–686, 689–695
Control limits, 188–193, 195–197
Corporate responsibility, 866
Corporate social responsibility, 876, 897
Corrective action, 573
Corrective maintenance, 790, 807, 819
Corrective replacement, 808
Correlated variables, 1035
Correlation coefficient, 1032
Correlation matrix, 819, 820, 823, 827, 828, 830, 831, 836, 837
Corrosive wear, 956
COSSAN, 1041
Cost analysis, 1132
Cost-benefit analysis, 726
Cost-effectiveness analysis, 727
Cost modeling, 1204
Cost models, 793, 794, 801
Costs of quality, 27,
Coupling factor, 621, 623, 624
Covariance matrix, 827, 829, 830, 831, 836
Covariates, 1200
Coverage, 321, 324, 1088
  Definition, 321
  Model, 324,
    Element level (ELC), 324
    Fault level (FLC), 324
    One-on-one level (OLC), 326
    Perfect, 324
C_p,C_{pk}, C_{pm},C_{pmk}, 198, 199
Cradle-to-cradle, 133
Creativity, 54
Creep, 953
Crisp set, 1041
Critical failure, 1131, 1134, 1135, 1138
Critical-to-quality characteristics (CTQS), 1013, 1014
Criticisms, 119
  Opportunity cost, 118
  Strategic implications, 120
Cross-covariance matrix, 830, 836
Crystallographic defect, 953
Cumulative damage, 807, 808, 813, 817
Cumulative damage model, 807
Customer-center, 431, 439, 440, 441, 444
Customer driven quality, 235
Cut set, 610, 642, 694, 706
  Inclusion-exclusion (I-E), 603
  Minimal, 601–603, 605, 608, 610, 614, 706
  Sum of disjoint products (SDP), 603, 608
  Top-down approach, 601–602, 614
  Truncate, 706
Cyclic codes, 1091

Dangling bond, 971
Data diversity techniques, 1093
Data fusion, 482
Data mapping, 634
  Mapping-down, 637
  Mapping-up, 637
Debugging of software, 244
Decision rules, 190, 191, 195
Decision variables, 1042
Decoding, 1091
Decomposition method, 47
Deductive methods, 596
Defect, 256
Defect rates, 1194
Defense, 623, 625, 628
Defence standards 00-40 and 00-41, 38
Define phase, 1015, 1017, 1018
Degradation degree models, 793, 794
Degradation model, empirical, 1123, 1124
Degradation model, stochastic, 1123, 1127
Degradation of dielectrics, 953
Dehydrogenation, 970
Delphi method, 97
Demand-critical electronics, 84
Deming, W. E., 26–28, 30, 40, 115

Deming's funnel experiment, 205, 211
Dependence, 622
  Negative, 622
  Positive, 622
Dependencies, 1141
Dependent failures, 595, 613, 705
  Cascading, 613
  Negative, 613
  Positive, 613
  Propagating, 613
Dependent maintenance policy, 796, 797
Deposition mechanism, 967
Deposition method, 967–969
Deriving explanations of human failures, 650
Design adequacy, 75
Design for Six Sigma (DFSS), 174, 177
Design for environment, 57, 58, 62–65, 67–69, 872, 924
Design for safety, 80
Design for Society, 924
Design for Six Sigma, 231
Design optimization, 481, 484, 486–488
  Evidence-based design optimization (EBDO), 486–487
  Possibility-based design optimization (PBDO), 487–488
  Reliability-based design optimization (RBDO), 487–488
  Robust design, 488
Design refresh planning, 92, 94, 101
  Porter's approach, 93
Detecting information-dependent, 796, 797
Deterioration function, 1148
  Phase, 1150
Deterioration with usage and age, 789
Development cycle, 534
Dimensionality reduction, 825, 826, 840
Diminishing manufacturing sources and, material shortages (DMSMS), 90
Directed acyclic graph (DAG), 603
Direction cosines, 1032
Discounting, 1153
Discrete Lognormal, 1210
  Discrete lognormal distribution, 1210
  Lognormal, 1209
Discrete software reliability growth models, 1239
  Exponential, 1239
  Modified exponential, 1242
  Delayed S-shaped, 1242
  With change point, 1251
Discriminant analysis, 1228, 1236
Disjoint paths, 1053, 1055, 1063, 1064, 1065
Disk duplexing, 1101
Disk mirroring, 1101
Disordered carbon, 967
Dissociation pattern, 970
Distance-learning, 868, 871
Distributed systems, 1085
Distribution 34, 292, 294–296, 299, 301, 308, 310, 312–317, 1147, 1148
  Baseline, 229
  Binomial, 312, 314, 535
  Bivariate, 292
  Chi-squared, 538
  Erlang, 298, 301
  Exponential, 298–319
  Gamma, 294, 298, 299
  General, 297–299, 301, 304
  Lognormal, 294, 1209, 11210
  Multivariate, 296
  Normal, 28, 296
  Poisson, 808
  Weibull, 294, 296, 302, 378, 536
Distribution (electricity), 1147, 1148
Distributions of components, 790
Disturbance, occurrences, 683, 684
Disutility function, 431, 436, 442
Diversity, 1092
Divide and conquer algorithm, 510
DMADV methodology, 231, 1012, 1013
DMAIC methodology, 226, 229–231, 1012, 1013
DNA, 934
DPCA covariates, 829, 831
Drucker, P.F., 28, 30, 40, 105, 106, 113–115
Duplication, 1089
DVAOV(define-visualize-analyze-optimize-verify), 1014–1016, 1018
  Key features, 1000
  Key outputs from each phase, 1001
  Key phases and objectives, 1014
    Define phase, 999–1014, 1015
    Visualize phase, 101
    Analyze phase, 1014, 1017
    Optimize phase, 1014, 1017
    Verify phase, 1014, 1018
  Key tasks of each phase, 1014
Dynamic principal component analysis, 825, 826, 841
Dynamic redundancy, 1089, 1090, 1093
Dynamic reliability measure, 431, 444
Dynamic source routing, 1063

Eco-efficiency, 860
Ecological risk assessment, 845
Ecomarketing, 131
Economic instruments, 860
Economic segregation, 1164
Economics of sustainability, 850
Ecoproducts, 131
Education, Engineering in Society, 109

Effect of load history, 294, 295
Cumulative damage model, 295
Cumulative exposure (CE) model, 295
Eigenvalue, 827, 1032
Eigenvector, 1032
Elastic modulus, 967
Electric related failure, 953
Electric utility, 1163
Electricity,
Distribution, 1163, 1164
Generation, 1163, 1164
Pricing, 1163, 1164
Transmission, 1163, 1164
Electron energy distribution, 970
E-maintenance, 781, 784
Framework, 781, 785
Embedded Markov chain, 371
Embeddedness, 142
Types, 142
Cognitive, 145
Cultural, 145
Political, 146
Spatial and temporal, 146
Structural, 145
Emergency planning, 857, 864, 868
Encoding, 1091
End-of-life decisions, 1118
End of life options, 9
Energy consumption, 1051, 1065, 1066
Energy distribution, 968, 970
Energy transformation, 236
Engineered quality, 235
Engineering design,
Bottom-up approach, 18
Top-down approach, 18
Engineering process control (EPC), 162, 183, 198, 203
Enhanced interior gateway protocol, 1096
Enterprise and the environment, 873
Environmental costs, 889
Environmental factors, 254, 1193
Environmental goods and services market, 858
Environmental management, 858–861, 867, 876, 877, 884, 887
Environmental movement, 112
Environmental performance indicators, 903
Environmental Protection Act 1990, 859
Environmental report, 860, 867, 872, 873, 895
Environmental risk assessment, 844
Hazard identification, 844
Dose-response assessment, 844
Exposure assessment, 845
Risk charaterization, 845
Environmental sustainability, 81, 876, 883, 887
Environmentally induced failure, 953
Environmentally responsible product development (ERPD), 58–60, 62–65, 67, 68
Epistemic uncertainty, 477–478, 480.
Equivalence class, 434, 441
Equivalent load, 414
Equivalent normal mean, 1031
Equivalent normal standard deviation, 1015, 1031
Erdös-Rényi graphs, 1056
ERP (enterprise resource planning) system, 800
Error, 256
Error-detection, correction, 1091
Etching rate, 971
Ethernet, 1096, 1097
EU Lisbon objectives, 128
Evaluation factors/methods, 801
Evaluative criteria, 43
Event, 595
Basic, 595
Dependent, 595
Disjoint, 595, 601– 608
Top, 396
Undesired, 595
Undeveloped, 595
Event tree, 381, 590, 594, 596, 601, 607, 614, 617, 682, 683, 697, 703
Branch point, 704
Functional, 704
Systemic, 704
Evidence theory, 477, 478, 479, 480, 481, 483, 486
Evolvability, 99
Exact algorithms, 800
Exact method, 506, 507, 509
Branch and bound process, 506, 507, 508
Cutting plan technique, 506
Dynamic programming, 506, 507, 509
Implicit enumeration search technique, 500, 502–504, 506, 508–510
Lawler and Bell's algorithm, 502, 508
MIP algorithm, 508, 513
Partial enumeration search technique, 500, 502, 503, 506, 508, 509
Surrogate constraints algorithm, 509
EXAKT software, 828
Expected cost, 807–821
Expected disutility, 443
Expected down-time (ED), 311
Expected hop count, 1050
Expected number of failures, 808
Expected total utility for experience (ETUE), 439
Expected up-time (EU), 311
Expected utility theory, 726
Expected values, 726
Experimental design, 171, 173, 178, 180, 237
Experimental design cycle, 283

Explicit limit state function, 1031
Exponential distribution, 820
Exponential time-to-failure distribution, 607, 612
Extended healthcare delivery systems, 1011
External event, 703
Externalizing the costs, 128
Extreme value failure, 1150
Exxon Valdez, 869, 871
Eyring relationship, 548, 552

Factor time, 133
Fail-silent, 1087
Failure, 159, 323, 331, 334, 341, 343, 616, 1167
  Analysis, 586
  Cost, 1143
  Covered -, 324, 328, 331, 334, 337, 345
  Event, 694
  Near coincident -, 323
  Single point -, 323, 331
  Uncovered -, 323, 331, 334, 341, 343
  States, 371
  Frequency, 309, 610, 611, 617, 791, 798
  Cascading, 637
  Common cause- , 1184
  Corrosion -, 258
  Dependent -, 257
  Hidden -, 622
  Individual -, 622
  Mechanism, 256
  Metallugical -, 257
  Mode, 256, 954
  Mode and effect analysis (FMEA), (126), 596, 1183
  Multiple -, 616, 617
  Multiplicity, 623
  Pattern, 942
  Rate, 85, 89, 292–295, 297, 299, 300, 302, 310–312, 413, 800–803, 807, 811, 812
    Baseline, 294, 295, 299, 301, 302
    Constant, 298, 300
    Cumulative, 299
    Time-varying, 295
Failure-critical, 609
Failure mode approach, 1044
Failure mode effect and criticality analysis (FMECA), 596
Failure precursors, 1109
Failure prevention, 826, 834, 838
Failure rate of a semi-Markov system,
  Asymptotic normality of the estimator, 376, 378
  Estimator of, 376
  Explicit form of, 374
  Strong consistency of the estimator, 378
Failure-critical, 609
Failure time distribution, 1200
FAR (fatal accident rate), 733
Fatigue failure probability, 425
Fatigue life, 569
Faults, 321, 322, 323, 325, 327, 328, 331, 335, 337
  Models, 321, 322, 327, 328
    Multi-fault, 322, 327
    Near coincident, 323, 330
    Single-fault, 322, 326
  Propagation, 335, 337
    Global, 337
    Local, 338
    Probabilistic, 338
  State, 326, 327, 332, 338
    Active, 327, 328
    Latent, 327
  Types, 322, 323
    Intermittent, 325
    Permanent, 325
    Transient, 325
Fault density, 1194
Fault detection, 819, 820, 825, 826, 832–834, 1088, 1090
Fault detection capability, 834
Fault error handling model (FEHM), 322, 323
  All-inclusive near coincident, 330
    Exponentially distributed recovery time, 330
    Extended models, 331
    Fixed recovery time, 331
    General recovery time, 331
    Phase recovery process, 331
      k-out-of-n system, 339
      Identical components, 340
      Non-identical components, 340
    Optimal system design, 345
    Probability, 324, 331, 332, 334
      Component state, 334, 339
      Conditional, 325, 336
      Exit, 325
    Reliability, 333, 334, 338–341
      Conditional, 339, 340, 343
    SAME-type near coincident, 330
    Unconditional, 339, 343
  Combinatorial approaches, 322–323 333, 335, 338, 339–341
    Binary decision diagram, 344
    Conversion rule, 605, 606
    DDP algorithm, 323
    Implicit common cause failure Method, 343
    Inclusion-exclusion, 341
    SEA-algorithm, 324, 336
    SDP method, 334
    Truth table, 341, 342

Exits, 325
Near coincident failure, 325
Permanent coverage, 325
Single-point failure, 325
Transient restoration, 325
General structure, 325
Multi-fault model, 330, 339
Single-fault model, 326
ARIES, 329
CARE III basic, 328
CARE III transient fault, 328
CAST recovery, 328
Continuous time, 327
Discrete time, 327
HARP, 329
Phase type, 327

State space models, 323, 331
Markov models, 331
System, 334–339
Configuration, 340, 341
k-out-of-n, 337–339
Modular, 339
General, 339
Type, 334–336
Binary, 335
Multi-state, 335
Hierarchical, 338
Phased mission, 338
Total probability theorem, 336
Fault injection, 1088, 1092
Fault masking, 1090
Fault tolerant software, 1201
Fault tree, 348–350, 353–355, 364, 381, 595–605, 697, 1180
Coherent, 286, 595
Dynamic 355, 365, 592–594
Multistate, 615
Noncoherent, 350, 598
Static, 355, 595, 598
Subtree, 602
Fault tree analysis (FTA), 596, 690, 1183
Combinatorial, 602, 607, 608
Galileo, 617
Modular, 602, 607
Qualitative, 601
Quantitative, 601–604
Relex, 595, 617
Software tools, 595, 617
State space, 602, 607, 613
Static, 596
Fault tree model, 1044
FDA, 998, 999, 1003, 1004, 1007
FDA regulations, 38
Field environment, 577
Field programmable gate array, 1104
Film density, 970
Finite difference approach, 1039
Finite interval., 810, 822
Finite renewal times, 1148, 1155
Firewall, 1097
First-order mean, 1038
First-order reliability method (FORM), 1028
First-order second-moment method (FOSM), 1028
First-order variance, 1028
First passage time, (113) 1147, 1148
Lower bound, 1149
FMEA (failure mode effect analysis), 690
Failure modes, mechanisms, and effects (FMMEA), 1111
Food and drug administration, 868
FORM/SORM, 1028
FRACAS/CAPA 988, 1000, 1004
Fracture, 953
Frameworks, 1012–1014
Full distribution approach, 1028
Functional block diagram, 702
Functional dependency gate, 599
Functional product, 779
Functional service economy, 128, 130, 135, 136, 138
Fuses and canaries, 1109
Futuristic system designs, 8
Fuzzy approach, 800
Fuzzy chance-constraint programming, 512
Fuzzy multi-objective optimization, 513
Fuzzy reliability theory, 491
Fuzzy set, 1041
Fuzzy simulation, 512
Fuzzy voting, 1094

Gain model, 1204
Gate, 349, 596
AND, 351, 356
Cold spare (CSP), 356, 599
Common cause failure (CCF), 1012
Dynamic, 356, 599
Exclusive OR, 350, 600, 608
Functional dependence (FDEP), 355, 599
Hot spare (HSP), 599
Inverse, 600
k-out-of-n, 351, 356, 616
NOT, 350, 600
OR, 348, 350, 351, 354, 356, 592, 599
Priority AND, 356, 599, 600
Sequence enforcing (SEQ), 600
Spare, 599
Warm spare (WSP), 356, 599
General log-linear model, 555

Generalized block diagram method, 447
Gene therapy, 927
Genetic algorithms, 800
Genetically modified organisms (GMO), 939
Generation (electricity), 1147, 1148 ??
Global computing, 1094
Globalization, 124, 921
GMW3172, 534
GNP, 129, 130
Goal theoretic basis for Six Sigma, 1011
Goel-Okumoto model, 1240
Grain boundaries, 958, 967
Graphite electrode, 968
Graphs, Probabilistic, 1048
Green engineering, 112
Greenpeace, 112
Global reporting initiative (GRI), 878
Grid, 1069, 1070
Grid computing, 987, 1069
  Failure analysis, 1071
Grid clusters, 1095
Grid service reliability, 1070
Grinding, 1126, 1127
GRMS, 573
Growth rate, 969–971

HALT, 540, 542, 544
Hamming codes, 1091
Happiness, 115
Hardware redundancy, 1088
Harmonic number, 316
HASA, 572
HASS, 559
Hazard and hazard analysis, 664, 665
Hazard and operability studies (HAZOP), 673
Hazard evaluation methods, 641
Health assessment and monitoring, 1042
Healthcare industry, 1012
Healthcare publications with Six Sigma, 1013
Healthcare technologies, 1011
Health delivery system, 986
Heuristic, 506, 507, 510–515
  HKRRA (Ha Kuo Reliability-Redundancy Algorithm), 511
Hidden factory, 26
Hierarchical control structure, 685
High hardness, 967
Hippocratic oath, 114
Hot standby router protocol, 1097
Human error, 256, 683
Human factors, 1184
Human failure modes and effects analysis, 648
Human hazard and operability analysis method, 648
Human reliability analysis, 642
  Definition, 642
  Event tree, 642
  Fault tree, 637
  Human error, 642
  Qualitative perspective, 642
  Quantitative perspective, 642
Humphrey's method, 627
Hybrid redundancy, 1088, 1090
Hydrogen content, 967, 971, 972, 974
Hydrogenated tetrahedral amorphous carbon, 968

ICDE database, 634
Ideal function, 238
Identifying consequences of human failures, 650
Identifying human failure modes, 648
IDOV (identify-design, optimize-validate), 1012, 1013
Impact vector, 636
Imperfect and perfect repair, 792
Imperfect coverage, 347, 348, 353, 357, 358 360, 367, 606, 611
  Covered failure, 358, 359, 360, 606
  Single-point failure, 362
  Uncovered failure, 358, 359, 360, 606
Imperfect maintenance, 804, 807, 822, 823
Importance analysis, 609–611
  Measures, 609–611
  Birnbaum, 603, 605, 609, 611, 700, 708
  Component criticality, 609
  Conditional probability (CP), 611
  Criticality importance factor (CIF), 611
  Diagnostic importance factor (DIF), 611
  Fussell-Vesely, 619, 708
  Improvement potential (IP), 605, 611
  Initiator and enabler, 609
  Reliability importance, 617
  Risk achievement worth (RAW), 611
  Structure importance, 611
Importance factor, 388
  Critical IF, 389
  Diagnostic IF, 389
  Differential importance measure, 390
  Marginal IF, 389
  Risk achievement worth, 388, 700 n.gef.
  Risk reduction worth, 611, 708
Importance measure, 708
  Absolute, 709
  Relative, 709
Imprecise reliability theory, 481
Improper integration, 315
Independent system operator (ISO), 991
Inductive methods, 596
  Failure mode and effect analysis (FMEA), 596
  Failure mode effect and criticality analysis (FMECA), 596

Fault hazard analysis (FHA), 596
Preliminary Hazards analysis (PHA), 596
Industrial biotechnology, 1261
Industrial ecology, 9, 139, 882, 919
Definition, 139
Dissemination, 141
Lessons learned, 151
Performance, 147
Industrial economy, 128, 129, 130, 133
Information and communication technologies, 781
Information redundancy, 1091
Information technology, 110
Infrared (IR) thermography, 763
Infrastructural operating issues, 887
Initial distribution, 372
Initiating event, 696
Operational, 696
Non-operational, 696
Initiation phase, 1150
Innovative multifunctional products, 130
Input energy, 238
Inspection, 803, 807, 808, 812, 819, 1132, 1135
Inspection interval, 1134, 1141, 1143
Inspection models, 793, 794, 795
Instantaneous degradation rate, 436, 438, 439
Integrated healthcare delivery system (IDS), 986
Integrated pollution prevention & control, *see* IPPC
Integrated safety, health and environmental management, 868
Integration, 315, 316
Improper, 315
Reliability, 318, 319
Intensity function, 808, 816, 817, 821
Intermittent faults, 800, 807, 813, 819, 820, 1078
Internal control, 857
International Risk Governance Council, 743, 754
International Standards Organization (ISO), 860, 861
Interval availability, 767
Interval graphs, 1053
Interventions and barriers, 651
In-use stiction, 955
Inventory spares, 800
Inverse power law relationship, 548, 556
Inverse transformation technique, 1036
Ion beam assisted deposition, 968, 976
Ion beam deposition, 967, 976
Ion bombardment, 968, 970, 974
Ion source, 968
Ionization energy, 969
IPPC, 859
I-R framework, 120
Ishikawa (or fishbone) diagram, 1021
ISO certification, 166
ISO 0603000, 38
ISO 09000, 36–38
ISO 14000, 112, 864
ISO 14001, 924
ISO 14063, 861, 864, 867
ISO/IEC 61508, 38
IT, *see* Information technology, 110
Iterative perturbation, 1039

Job creation, 128, 134, 137
Johnson & Johnson, 869
Just in time, 169, 232

Kaizen, 169
Kalman filter, 1043
Kaufman source, 968
Kelvin, Lord, 108
Kiss principle, 36
Kleinrock's independence approximation, 1213
Knowledge management, 247
k-out-of-n system, 297, 298, 301, 309–317, 337, 339
Non-repairable, 309, 310, 313
Failure rate, 311, 312, 313
MTTF, 314, 315
Repairable, 298, 313, 315–317
Identical components, 298
Non-identical components, 302
k-terminal or source-to-many terminals (SMT), 1049

Lab-on-a-chip, 137
Laplace transform, 1154
Incomplete, 1155
Modified, 1154
Larger the better quality characteristics, 179, 180
Latent (defect), 574
Least square approach, 509, 517
Parametric programming, 528
Least square estimation, 835
Left censoring, 409
Legal obligations, 875, 885
Liability loops, 131
Life cycle, 99, 100
Monitoring, 97
Roadmapping, 100, 101
Sustainability, 81–83, 101
Life cycle activities, 12
Life cycle assessment (LCA), 6, 860, 861, 878
Life cycle costs, 77, 84, 87, 95, 133, 263, 767, 770, 781, 782
Analysis, 776
Life cycle design, 49
Life cycle management, 879, 881
Life-stress relationships, 546, 547
Life test ratio, 540

Lifetime buy, 93, 94
Lifetime of the system, 373
Limit availability, 790
Limit average availability, 790
Limit state, 1025
Linear codes, 1091
Linear production system, 921
Linear thinking, 129
Lipson equality, 539
Liquid nitrogen, 562
Load and resistance factor design, 1026
Load balancing, 1085, 1096
Load-life relationship, 293, 294
  Accelerated failure time model (AFTM), 294
    Exponential law, 294
    Power law, 294
  Proportional hazards model (PHM), 294
Load pattern, 293
  Constant, 293
  Time varying, 293
Load sharing, 291- 296
  Models, 294
    Freund, 296
    Static, 295
    Time dependent, 296
Load-strength interference, 413
Lognormal,
  Operational profile, 1211
  Operational sequences, 1212
  Software defect,
    Imperfect repair, 1222
    Failure rate model, 1213
    Occurrence time model, 1214
Lognormal parameters,
  Location parameter, μ,
    Software interpretation, 1222
  Shape parameter, σ,
    Function of depth of conditionals, 1210
    Software interpretation, 1210
  Total defects, N
    Estimation, 1215
    Software interpretation, 1215
Lognormal, origin in software,
  Event rate distribution, 1210
  Fault detection process, 1213
  Operational profile, 1211
  Program control flow, 1212
  Queuing network models, 1212
  Sequences of operations, 1212
  System state vectors, 1213
Lognormal, software reliability models,
  Advantages, 1221
  Code coverage growth, 1220
  Failure rate distribution, 1213
  Failure time distribution, 1214
  Limiting distribution, 1218
  Reliability growth, 1214
Lognormal, validation in software,
  Code block execution rate data, 1217
  Code coverage growth data, 1220
  Defect occurence count data, 1220
  Failure rate data, 1216
  Reliability growth data, 1218
Long-term ownership, 134
Loop economy, 129, 133, 138
Lower boundary points, 433, 434
Low friction coefficient, 967, 974, 975

Machine structures, 51
Magnetic storage disk, 967
Magnetron sputtering, 968, 975
MAIC (T), 176
Maintainability, 75, 84, 758, 769, 772, 776
Maintained system design, 280
Maintenance, 83–85, 611, 765, 781, 1131
  Action distributions, 790
  Approaches, 759
  Corrective, 87, 759
  Cost, 765
  Definition, 796
  Degree, 790
  Design for, 780
  Design out, 780
  Failure-finding, 765
  Indexes, 790
  Management, 770
  Models, 789–800
  Optimization, 789, 790, 798
  Performance indicator, 772, 780
  Performance measure, 780
  Philosophy, 756
  Polices, 789, 790
  Predictive, 755
  Preventative, 84, 759
  Quantitative analysis, 789
  Reliability centred (RCM), 768
  Requirements, 780
  Scope and classification, 756, 757
  System, 747, 765
  Total productive (TPM), 769
  Trends, 773, 775
Maintenance cost analysis, 833
Maintenance cost comparison, 832
Maintenance cost savings, 840
Maintenance interval, 1133
Maintenance interval optimization, 1133
Majority voting, 1094
Malcolm Baldridge, 225

Manageability, 737, 739
Management commitment, 245
Management process factor, 1231, 1233, 1234
Management systems, 859, 860
Managerial review and judgment, 721
Managing performance over time, 128, 137
MANET, 987
MANET path recovery, 1063
MANET routing protocols, 1063
Manufacturing cost, 44–46, 48, 50, 52, 53, 56
Many-source-to-terminal (MST), 1049
Many-to-one (S,t), 1033
Marginal pricing system,
  Nodal, 1163
  Uniform, 1167
  Zonal, 1167
Market models,
  Bilateral contracts, 1163, 1165, 1167, 1170
  Hybrid, 1163–1165, 1170
  Poolco, 1163, 1165, 1166, 1169
Markov chain, 303–305, 312, 316, 323, 328, 351–354, 358, 370
Markov chain model, 1141, 1223
Markov model, 607, 608, 612, 618, 1048
  Absorbing state, 607
  Differential equation, 607, 612
  Laplace transform, 607
  State explosion, 602, 612, 613, 614
  State transition, 607
Markov process, 436, 437
Markov renewal chain, 370, 371
Markov renewal equation, 373
  semi-Markov transition function, 373
Marks and Spencer, 897
Masking redundancy, 1093
Master tasks list, 997 n.gef.
Material loops, 129, 131
Material risk index (MRI), 92
Matrix convolution product,
  Definition, 371
  Identity element, 371
  Left inverse, 371
Maximal (minimal) objective functions, 799
Maximization of:
  Failure frequency and downtime, 798
  Mean down time MDT, 791
  Mean time between failures (MTBF) 791
  Mean time to failure (MTTF), 791
  Mean time to first failure MTTFF, 791
  Mean up time (MUT), 791
  System reliability/availability, 790, 792, 794, 795, 798
MDZ figure, 1131
Mean cumulative function, 402
  Age, 404
  Anomalous machine, 404
  Comparisons, 408
  Cost Function, 411
  Cumulative Plot, 402
  Downtime Function, 410
Mean cycle time (MCT), 311
Mean down time (MDT), 87, 311, 790, 791
Mean supply delay time (MSD), 88
Mean time between failure (MTBF), 32, 33, 85, 535, 569, 782, 791
Mean time between maintenance (MTBM), 87
Mean time to first failure (MTTFF), 8–10, 315, 790
Mean time to failure (MTTF), 314, 315–317, 535, 790, 1102, 1139
Mean time to repair (MTTR), 311, 314, 1137
Mean up time (MUT), 790
Mean value first-order second-moment method, 1027
Mean value function, 808, 814, 816, 817
Mechanical properties, 965, 967
Medical device, 985–987, 997, 998, 1001, 1002
  Classes, 999
  Classification, 999
  Reliability standards, 998, 1008
Memory scrubbing, 1101
MEMS, 945, 953
Mental satisfaction level, 44
Meshless methods, 1025
Metaheuristic algorithms, 800, 802
Metastable, 967
Metrics, 128, 137
Metrics of sustainability, 848
  Emery sustainability index, 850
  Gross domestic product, 849
  Happy planet index, 849
  Human development index, 850
  Living planet index, 849
M-for-N diversity coding, 1064
Micro-electromechanical devices, 967
Micro-electromechanical systems, 953
Micropartitioning, 1099
MIL-HDBK- 268, 535
Military handbook, 32
Military standard for quality, MIL-Q-9858, 36
Miner's criterion, 569
Minimal cutsets, 385
  Decomposition theorems, 387
  Definition, 385
Minimal repair, 800–804, 808–811, 816, 817
Minimal task spanning tree (MTST), 1080
MIP algorithm, 521, 522, 523, 525, 527
Mission life, 533
Mitigation of obsolescence cost analysis,
MOCA, 93

Mixed time and deteriorating degree, 796
Mobile ad hoc network (MANET), 1047
  Computing link availability, 1052
  Critical values, 1061
  Phase changes, 1061
  Routing protocols, 1063
Model order determination, 829, 830, 835
Modulated excitation, 574
Molecular manufacturing, 853
Monitoring, 560
Monitoring environmental and usage loads, 1109
Monoradical, 970
Morgan's law, 615
Motor current analysis, 762
MST reliability, 1049
MSV (Misra, Sharma, Venkateswaran), 510
MTBF calculation, 1000, 1004, 1005, 1006
  Failure terminated, 1006
  Time terminated, 1006
MTBF, *see* Mean time between failure
MTTF, *see* Mean time to failure
MTTR, *see* Mean time to repair
Multi-attribute analysis, 729
Multi-criteria redundancy optimization, 529
Multi-objective optimization problem, 45
Multicast (s, T_i), 1095
Multicast routing protocols, 1095
Multidisciplinary optimization, 47
Multinormal integral, 1150
Multi-objective function, 799
  Without constraints, 799
  With constraints, 799
Multi-path iterative heuristic, 511
  XKL (Xu, Kuo, Lin), 511
Multi-path routing protocol, 1063
Multiphase design optimization procedures, 49
Multiple regression analysis, 1227, 1236
Multiple-valued decision diagrams (MDD), 606, 616
Multi-state model, 432, 440
Multi-state system, 441, 459
Multistate, 595, 606, 607
Multi-unit systems, 790, 795, 798, 822
Multi-variable inversion (MVI), 1053
Multivariable relationships, 555
Multivariate adaptive regression splines, 580
  Model fit criteria, 584
Multivariate CM data modeling, 825, 826
Multivariate control charts, 825, 826
Multivariate linear analysis, 1227
Multivariate Markov process, 837
Multivariate time series modeling, 835–837
Mutually disjoint terms (MDT), 1053
Mutually exclusive, 358, 359, 362, 363, 433, 612–614
Nano carbon tubes, 138
Nanoelectromechanical systems, 953
Nanomaterials, 944
Nanotechnology, 853
Natural environment, 44
Natural resources, 44
N-copy programming, 1093
NEMS, 953
NESSUS, 1040
Net present value, 725
Network reliability, 441
New products from waste, 131
New strategy for dynamic globalization, 124
NGO, 919, 927, 931
NHPP model, 1190, 1196
Nodal price, 1163–1177
Nodal reliability, 1165, 1167, 1168
Noise factors, 235–237, 239, 243
Non parametric, 397
Non-composite indicators, 905
  Definition, 905
  Examples, 905
Non-dominated solution, 801
Non-homogeneous continuous time Markov process (NHCTMP), 438, 442, 444
Non-homogeneous poisson process, 808, 814, 816
Normal distribution, 28
N-tier systems, 1091
Nuclear power plant, 1179
NUREG, 617
N-version programming, 1093

Obsolescence mitigation, 91–95
  Aftermarket sources, 91
  Alternative part, 91
  Bridge buy, 93
  Emulation foundries, 91
  Lifetime buy, 92
Obsolescence, 81, 84, 91, 96
  Electronic part obsolescence, 90, 91
  Forecasting, 92
  Functional obsolescence, 95
  Inventory obsolescence, 90
  Logistical obsolescence, 95
OC curve, 189
OHSAS 18001, 864
Oil analysis, 762
Oil data histories, 825, 827, 828, 829, 834, 835
Omission fault, 1095
One-unit system, 808, 815
On-line decision-making, 835, 840
On-line quality engineering, 236
Open university, 868, 874

OPENSEES, 1041
Operation mode, 702
  Normal, 702
  Off-normal, 702
Operational limit, 561
Operational performance, 883, 886, 896
Operational readiness, 74
Operations, 875, 878
Operations design, 885
Operations improvement, 896
Operations management, 875–877, 879–881 883, 885
Operations planning and control, 894
Operations strategy, 883
Optical transparency, 967
Optical window, 967, 975
Optimal feedback controllers/minimum mean squared error (MMSE) controllers, 209
Optimal maintenance policies, 791
  Problems, 791
  Solution, 799
Optimization, 465
  Algorithm, 465, 469
Optimization criteria, 790, 802
Optimum quality, 26, 27
Orthogonal arrays, 236, 242–244
OSPF protocol, 1096
Output response, 237, 239
Outsourcing, 777
  Full, 779
  Partial, 778
  Partnering, 779
Overlay networks, 1098
Overstress acceleration, 544
Oversupply, 129, 130

Packaging reliability, 955
Parallel system, 807, 808
Parameter design, 173, 177, 178, 180, 184, 236, 237, 239, 241
Parameter diagram, 237
Parametric binomial, 535
Parametric optimization, 528
Pareto optimum solution line, 53
Pareto optimum solution set, 45, 46
Parity codes, 1091
Partial likelihood function, 1200
Partition method, 810
Partitioning, 1099
Passive redundancy, 1088
Patent, 562
Path/pathset, 1048, 1049, 1053
Path recovery, 1063
Path delay faults, 1104
Pathways to sustainability, 852
PC scores, 827, 831, 832, 840
Percentile point, 809
Perceptions of risk, 865
Percolation theory, 1056
Performability, 10, 11, 857, 858, 860, 861, 866, 1046, 1085
  Dependability, 11
  Engineering, 11
  Quality, 11
  Reliability, 11
  Maintainability, 11
  Safety, 11
  Sustainability, 11
  Survivability, 11
Performance, 1066, 1069, 1070, 1072, 1073, 1080, 1085
Performance based design, 1027
Performance based logistics (PBL), 87
Performance criterion, 1027
Performance economy, 127, 128, 136, 138
Performance management systems, 887
Performance objectives and indicators, 886
Periodic repair model, 793
Periodic replacement, 807, 808
Perrier, 868, 869
Petri net, 350, 353–355, 367
PF interval, 1129
Pham-Nordmann-Zhang model, 1193
Pham-Zhang model, 1193
Phase changes, 1058
Phase changes phenomenon, 1061
Phased mission, 595, 611
Phased-mission system (PMS), 349–367
  Coherent, 350, 357
  Combinatorial phase requirement (CPR), 349, 351, 358–360
  Dynamic, 349, 351, 365
  Mini-component, 351, 352, 356, 357
  Noncoherent, 350
  Non-repairable system, 349–351
  Phase algebra, 352, 357, 358, 360
  Phase dependent operation (PDO), 353, 357
  Phase modular, 349, 355, 367
  Sequential, 351
  Static, 347–349, 351, 355, 367
Physical asset management, 138
Piper alpha, 869
Planning and control, 883
Plant accidents, 78
Plant specific beta-factor, 621
Plasma enhanced chemical vapor deposition, 967, 969
Plasma polymerization, 970
Plasma source, 968
Plasma sputtering, 968
Plasma-surface interaction, 970

Pointwise availability, 791
Busy probability of repairmen, 791
Poisson distribution, 86
Poisson probability, 86
Poisson process, 397, 814
Generalized renewal process, 401
Homogeneous, 397
MTBF, 398
Non-homogeneous, 401
Renewal process, 401
Poissonian disturbances, 1148
Poisson-lognormal, *see* Discrete lognormal
Polymerization, 970
Poolco, 1163–1167
Population pressure, 1
Possibility theory, 477–479, 482
Potters bar, 870
Power cycling, 563
Power flow,
Model, 1148
Optimization, 1148
Power system,
Deregulated, 1164
Operation, 1164, 1169, 1174
Planning, 1152, 1164
Reliability, 1149, 1150, 1160
Restructured, 1163–1167
Power temperature cycling, 534
PRA, *see* Probablistic risk assessment
Pratt & Witney, 134
Precautionary principle, 729
Preferred solution, 801
Preliminary Hazard Analysis (PHA), 673
Prevention performance check, 839
Preventive maintenance (PM), 790, 793, 795, 796, 807
Preventive replacement, 807
Price volatility, 1163
Pricing, (electricity), 1163, 1164
PRIFO, 1134
Primary failures, 597, 598
Prime implicant, 608–610, 615
Principal component analysis, 825, 826, 1227–1230
Principle-centered quality, 171, 174, 175, 184
Priority maintenance policy, 796, 798
Probabilistic connectivity matrix, 1057
Probabilistic graph, 1048
Probabilistic risk assessment, 667, 676, 992, 1179
Data, 700
Event identification, 701
Information assembly, 701
Interpretation, 700
Logic modeling, 704
Objectives, 701
Possibilistic approach, 677
Quantification, 706
Risk assessment, 1179
Risk ranking, 708
Scenario development, 700
Sensitivity analysis, 700
Standard, 1168
System response, 1183
Uncertainty analysis, 700
Probabilistic safety assessment, 1180
Probability, 324, 331, 333, 334, 388, 714, 1170
Aggregation, 1171
Conditional, 325, 326
Probability density function (PDF), 311, 312
Probability of failure on demand, 621
Probability of intersections, 1157
PROBAN, 1041
Process assets, 247
Process baseline, 246
Process capability, 44, 176, 198, 199
Process data, 1228, 1230, 1232, 1233, 1236
Process map, 246
Process ownership, 247
Process quality, 1227
Process tailoring, 248
Process variation, 188, 198
Assignable causes, 188, 189, 191
Chance causes, 188
Process variation, 29
Producibility, 99
Producing performance, 128, 137
Product and process design, 889
Product development processes, 57–60, 62–65, 67–69
Product life cycle, 44, 879
Product life-cycle management, (PLM), 168
Product manufacturing, 43
Product performance, 43
Product quality, 43, 1213, 1127–1230
Product take-back, 1118
Product-life extension, 132
Product-service system, 885, 887
Prognostics and health monitoring, 1107
Definition, 1107
Framework, 1108
Condition-based maintenance, 1108
Benefits, 1122
Built-in test, 1109
Approaches for PHM of electronics, 1109
Fuses and canaries, 1109
Failure precursor, 1111
Monitoring environmental and uses loads, 1114
Implementation, 1111
FMMEA, 1111
Sensors, 1112
Project specific process, 248

Proportional hazards modeling, 825, 834, 840
Prostate cancer, 441, 442
Protective coating, 967, 973–975
Proteogenomics, 934
Pseudo random numbers, 1036

Q-statistic, 826
Qualitative accelerated testing, 543
Quality,
  Assurance, 163, 174
  Chronological developments, 160
  Circles, 169
  Control, 159
    Off-line, 159
    On-line, 160
  Costs, 164
  Definitions, 158
  Improvement, 164
  Management, 171, 173, 174, 184, 867, 868, 870, 876, 877
  Planning, 162, 174
  Policy, 246
  Prediction, 1219, 1223–1225, 1221, 1222
Quality and reliability, 159
Quality assurance process factor, 1231, 1234
Quality engineering, 157
  Off-line, 171–173, 177, 180, 181, 184
  On-line, 171–173, 180, 182, 184
Quality function deployment (QFD), 171, 174–177, 184, 1016, 1017, 1023
  CSQFDs, 1016, 1017
  CTQs, 1016, 1017
  House of Quality (HOQ), 1016
Quality loss function, 172, 179, 182, 236, 237
Quality management system (QMS), 164
Quality manuals, 249
Quality of life, 441–444
Quality of service (QoS), 1047
Quality policy deployment, 250
Quantifying reliability, 31
Quantitative accelerated testing, 543
Quantitative risk assessment, 672
Quasi renewal process, 1205
Queuing methodologies, 1016, 1018
  Little's Theorem, 1014, 1019
  M/G/1 Queue System, 1020, 1021
  M/G/S Queue System, 1020, 1021
  M/M/1 Queue System, 1019
  M/M/s Queue System, 1019, 1021
Queuing network, 1019, 1020

RAID, 1100, 1101
Rail degradation, 1125
Rail safety and standards board, 870
Railway track, 1123–1125
Railway track configuration, 1124
Railway track settlement, 1124, 1125, 1127
Random field environments, 1204
Random graph, 1050
Random processes methods, 447
Random replacement, 807, 808
Random vibration, 566
Range limited graph, 1058
RDF2000, 535
REACH (European Chemicals Policy), 938
Reactive sputtering, 968
Real-time control system, 1196
Rebuilding strategy, 1153
Reconfiguration, 1088, 1089
Reconstruction, 1147
Recovery block (RB), 1093, 1203
Recovery options, 892
Recurrence rate, 404
Recyclability/dissembly rating, 62
Recycling and reuse of structural steel sections, 882
Redesign, 91, 92, 99
Reduced coordinates, 1014, 1030
Redundancy, 264, 289, 294–296, 298, 300, 301
Redundancy allocation, 516
Refresh, *see* Design refresh
Regionalisation of economy, 137
Rejuvenation technique, 1094
Release-related stiction, 955
Reliability, 5, 10, 38, 44, 295, 298, 302, 310, 311, 313, 314, 315, 333, 334, 338, 339, 340, 341, 462–467, 527, 589, 767, 774, 782, 953, 1012, 1094
  Allocation, 465
  Alternative approaches, 279
  Binary, 462, 465, 468
  Computation, 467
  Conditional, 336, 343
  Demonstration, 533, 535
  Design procedure, 280
  Expert systems, 278
  Failures,
    Classification, 260
    Data, 265
    Electrical, 257
    Genesis, 258
    Mechanical, 257
  Growth, 283
  IEC definition, 253
  Index, 1029, 1149
  Modelling, 275, 1067
    Structures, 276
  Multi-state, 461, 466
  Prediction, 531

Parts count method, 271
Parts stress method, 271
Program, 533
Requirements, 53
Standards for prediction, 267
IEEE STD 493-1997, 271
MIL-HDBK 217, 268
NPRD-95, 270
NSWC-98/LE1, 270
Physics of failure, 271
PRISM, 269
Telcordia SR-332, 268
Some hard facts, 255, 256
Testing, 280, 531
Unconditional, 339, 343
Reliability analysis, 477–480, 483, 484, 485–487
Evidential reasoning, 493–495
Possibilistic analysis, 484, 497
Probabilistic analysis, 477
Reliability-based design, 1026
Reliability block diagram (RBD), 596, 1048
Reliability centred maintenance, 768
Reliability degradation, 413
Reliability engineering, 261, 262
Strategy, 256
Reliability measures, 1049, 1053, 1055
Reliability/availability models, 807, 808
Reliability prediction for mechanical and structural members, 273
Reliability network, 1163, 1170
Reliability of a semi-Markov system,
Asymptotic confidence intervals, 378
Asymptotic normality of the estimator, 376, 377
Asymptotic variance, 377, 378
Estimator, 375
Explicit form, 374
Strong consistency of the estimator, 377, 379
Reliability process, 953
Reliability program, 1000
Concept phase, 1000
Design phase, 1000, 1001
Manufacturing phase, 1000, 1001
Prototype phase, 1000, 1003
Reliability special gadgets, 277
Reliability tools, 997, 1000, 1004
Benchmarking, 1000
Derating analysis/component selection, 1000
Fault tree analysis, 1000
FMECA, 1002
Gap analysis, 1001
Human factors analysis, 1000
Modeling and predictions, 1000
Software reliability analysis, 1000
Thermal analysis, 1000
Worst case circuit analysis, 1000
Renewal density, 808–812
Renewal function, 808–812, 1150
Renewal intensity, 1151
Renewal process, 813
Repair, 1134, 1135, 1141, 1147, 1152, 1214, 1222
Imperfect, 1152, 1222
Repair duration, 374
Repair limit, 807, 815
Repairability, 75
Repairable semi-Markov system, 373, 374
Repairable system, 397, 513, 791–795, 798, 802
Repair-critical, 609
Replacement, 806–821
Replacement cost-rate, 799
Replication, 1087, 1091
Residual life, 422
Resistance to sustainability, 851
Resources,
Non-renewable, 2
Renewable, 2
Resource consumption, 128, 129, 130, 137
Resource efficiency, 129, 130, 131, 133
Response surface approach, 1039
Response surface methodology (RSM), 1018
Restart, 821, 823
Restructuring, 1163, 1164
Retry blocks, 1093
Reverse supply chain, 881, 883, 885, 889
Richard Feynman, 943
Risk, 714, 772, 851, 856, 857, 1163
Analysis, 665, 715, 717, 771, 1153
Appraisal, 743
Assessment, 712, 738, 883, 1163
Aversion, 726
Based decision, 776
Communication, 667, 743
Concern assessment, 745
Consequences, 768, 769
Evaluation, 673, 718, 741, 1163
Goal, 1187
Governance, 678, 743
Informed approach, 1180
Management, 136, 667, 672, 677, 678, 719
Management process, 677, 720, 1187
Perception, 667
Pre-assessment, 743
Treatment, 718
Risk acceptance criteria, 719, 733
Risk averse, 443
Risk-based design, 1026
Risk neutral, 443
Risk prone, 443
Robust design, 171, 178, 180, 184

Robustness, 235
Robust engineering, 235, 237–239, 242, 244
  Experimental design, 237, 244
  Parameter design, 236, 237, 239, 241
  Parameter diagram (PD), 237, 239
  Signal to noise (S/N) ratio, 238, 241
  Software testing, 242–244
    Orthogonal arrays, 243–245
    Debugging, 244
Robust optimization, 1042
ROCOX, 1139
Root cause, 561, 577, 621, 623
Root cause analysis, 1003, 1021, 1022
Routing protocols, 1096, 1097
Run to run control, 215

Safety, 35, 38, 44, 78, 1179
Safety case, 38
Safety constraint, 684
Safety control function, 684
  Failure, 684
Safety factor, 273
Safety index, 1029
Safety instrumented system, 626
Safety integrity level, 621
Safety management, 722
Safety margins, 264
Safety-critical systems, 458
Sainsbury, 895
Sample size, 189–192, 195–197, 534
Sandoz, 869
Sanity-based, 1094
Satisfying solution, 801, 802
Scientific management, 105, 106
Scree test, 831, 836
Scorecard model, 63
SEC-DED, 1091, 1103, 1104
Secondary failure, 598, 599
Second-order reliability method (SORM), 1027
Security, 1052, 1062, 1066
Self maintenance, 768
Self-bias voltage, 969
Selling goods, 132
Selling performance, 128, 132, 135, 137, 138
Selling results, 132
Selling shared services, 132
Selling use, 132
Semiconductor, 958, 962
Semi-Markov chain, 299, 305, 370
Semi-Markov kernel, 370–376
  Cumulative, 371
  Definition, 370, 371
  Estimator, 376, 377
Sensitivity, 239, 241
Sensitivity analysis, 611, 1016
Sensitivity index, 1035
Sensitivity-based analysis, 1039
Sensors, 1112
Sensor to business, 783
Sensor to sensor, 783
Sequence dependence, 599, 607
Sequential maintenance, 815, 817
Series-parallel systems, 458
Service economy, 127, 128, 130–136, 137
Service reliability, 1070, 1072, 1074, 1075
Service unbundling, 1164
Serviceability, 75
Serviceability limit state, 1043
Setup adjustment problem, 214
  Grubb's harmonic rule, 215
Shareholder value, 868–870
Sheath, 969
Shewhart, W.A., 30
Shock, 813–815, 817
Shock models, 792–794, 802
Shut-off rules, 790, 793
Signal factors, 237, 239, 243
Simulation, 1012
Simulation based experiments, 239
Single point of failure, 1092
Single-point failure, 602
Single-unit systems, 790
Single-variable inversion (SVI), 1053
Six Sigma, 39, 166, 171, 174–177, 184, 226–234, 1011
  Case-engineering tank, 230
  DFSS (design for Six Sigma), 1012
  Execution (sequential and iterative), 1014
  Frameworks, 1012, 1013
    DMADV, 1012, 1013
    DMAIC, 1012, 1013
    DVAOV, 1014
    IDOV, 1012, 1013
  Lean, 232
  Origin of Six Sigma, 1012
SKI data, 634
Smaller the better quality characteristics, 179, 180
Smart materials, 138
Social amplification of risk, 865, 874
Social responsibility, 861
Soft computing, 1041
Soft errors, 1091
Soft failure, 562
Software attacks, 1105
Software defect,
  Failure rate model, 1213
  Occurrence counts model, 1214
  Occurrence time model, 1213
Software development process, 1193

Software failure, 1236
Software failure rate model, 1224
Software faults, 1194, 1227
Software fault tolerance, 1088
Software metrics, 1224
Software obsolescence, 95
  Sudden obsolescence, 90
Software quality assurance plan, 248
Software quality management, 1228, 1233
Software reliability, 1185, 1193
Software reliability growth models (SRGM), 994, 1196, 1198, 1239–1249
Software reliability modeling, 1196
Software tool, 595, 617, 618
Sojourn times distributions, 369
Source-to-many terminals (SMT), 1049
Space redundancy, 1092
Spanning tree, 1080
Spanning tree protocol (STP), 1096
Sparing, 81, 84
  Item-level sparing, 84
  System-level sparing, 87
Spatial redundancy, 1104
SPC, *see* Statistical process control
Spectrometric analysis of engine oil, 817, 821
Sputter yield, 968
Squared prediction error, 828
Stable configuration approach, 1044
Stakeholder, 721, 864, 865, 874, 875, 877, 879, 880, 884
Stakeholder capitalism, 880
Stakeholder engagement processes, 885, 892
Stakeholder involvement, 743
  Design discourse, 750
  Epistemic discourse, 748
  Participatory discourse, 750
  Reflective discourse, 748
Stakeholder value, 879, 880
Standardization 118
  Assumptions 119, 120
  Criticisms 119, 120
  Opportunity cost, 118
  Strategic implications, 120
Star topology grid architecture, 1075
State classification, 433
Statistical inferences, 792, 803
Statistical process control (SPC), 29, 161, 826, 828, 832, 833, 840, 1018, 1019
Statistical quality control, 161, 171, 173
Statistical quality engineering, 1012
Statistical sampling techniques, 1016
Steady-state availability, 309-315
Steady-state busy probability of repairmen, 791
Sticking coefficient, 971
Stiction, 953
Stochastic dependency models, 292–296
  Bivariate, 296
  Common-cause failure, 292
  Load-sharing, 291, 293
  Multi-variate, 296
  Shock, 292
Stochastic finite element method, 1039
Stochastic optimization, 1041
Stochastic process, 791, 794, 795, 797, 801
Strength degradation, 417
Strength limit state, 1043
Stress loading, 548
Stress screen, 559
Stroke study, 440
Structural maintenance, 1043
Structural operating issues, 886
Structural state function, 1148
Structure function, 431–435, 441, 443, 448
Structured task oriented strategies and well-defined goals, 1012
Subjective probabilities, 740
Subplantation, 967, 970, 971
Subsurface reaction, 970
Success factors, 1012, 1015
Success run testing, 533
Sum of disjoint products (SDP), 603, 608, 1053
Supply chain perspective, 875
Supply network perspective, 879
Supportability, 99
Survivability, 11, 71
Suspended animation, 309, 318, 319
Sustainability, 81, 82, 98, 128, 843, 846, 875, 876, 878, 880, 887, 898
  Assessment, 843, 905
  Definition, 905
  Economic and performance aspects, 7
  Indicators, 896
  Business sustainability, 82
  Environmental sustainability, 81
  End of life options, 9
  Management, 875–877, 880, 883, 886
  Metrics, 848
  Social dimension, 847
  Technology can help, 4
  Technology sustainability, 82
Sustainable development, 874
Sustainable operations design, 889, 891
Sustainable operations management, 82, 891, 899
Sustainable operations strategy, 885
Sustainable products and systems, 5
Sustainment, 81, 82, 98
  Cost avoidance, 92
  Engineering, 82
  Dominated systems, 90

Vicious circle, 83
Symmetrical cluster, 1098
Synchronization, 1095, 1100
System,
Concept and definition, 14
Classification, 15
Characterization, 15
Design, 173, 177
Design characteristics, 17
Design process, 19
Conceptual design, 21, 66
Preliminary design, 21
Detail design and development, 22
Design evaluation, 22
Elements, 15
Hierarchy, 16
Identification, 1013, 1014, 1042
Inputs and outputs, 16
Reliability, 420, 1043
Testing, 22
Worth, 78
System control for safety, 683
System control loop, 684
System effectiveness, 73
Attributes, 74
Systems engineering tools (*see* DVAOV), 1014–1016, 1018
Cause and effect matrix, 1016
Current and future reality trees (CRT), 1017
Design of experiments (DOE), 1012–1016
Exploratory data analysis (EDA), 1016
FMEA, 1016
Goal programming, 1018
Linear models, 1016
Linear programming (LP), 1017, 1018
Multiple objective linear programming (MOLP), 1018
Monte Carlo simulation, 1024, 1036, 1132
Multi-vari studies, 1016
Process capability analysis, 1016
Process mapping, 1016
Project management, 1016
Systems modeling and optimization, 1012
System reliability evaluation, 274
System solutions, 130, 131, 133
System performances, 755, 773, 780, 798
System perspective, 1011
System safety, 668
System state space, 433

Taguchi, Genichi, 30
Taguchi method (TM), 235, 236, 239, 244
Tampered failure rate (TFR) model, 292, 297
Tamping, 1126
Target the best quality characteristics, 179, 180
Task analysis, 644
Hierarchical task analysis, 644
Taylor series, 1029
Taylor, F.W., 105
TBL, *see* Triple bottom line, 82, 876
Team based execution strategy, 1014
Technological obsolescence, 95
Technological progress and risk, 668
Technology and culture, 925
Technology and risk, 926
Technology upgrading, 132
Technology insertion, 96
Technology lock-in, 922
Telcordia, 535
Temperature-humidity relationship, 548, 554
Temperature-non-thermal relationship, 548, 554
Temporal redundancy, 1104
Ternary decision diagram (TDD), 362
Ternary phase diagram, 967
Tests, 34
Acceptance test, 1005
Capability, 534
Development/growth test, 1005
Durability, 534
Duration, 534
DVT, 1003, 1004
Environmental, 533
HALT, 1000, 1003, 1004
ORT, 1004
Performance, 1000, 1001
Qualification, 1005
RDT, 1000, 1003, 1004
Robustness, 534
Screening, 1000–1004
Sequential, 1005
To a bogey, 535
Testing, 996, 1000, 1003
Theory of constraints, 1017
Theory of inventive problem solving (TRIZ), 167, 170, 236,
Thermal conductivity, 967
Thermal uprating, 91
Throughput, 1098
Throw-away products, 84
Time,
Active repair, 76
Administrative, 77
Down, 76
Free, 77
Logistic, 76
Operating, 76
Storage, 77
Time compression, 562

Time dependent analyses, 391
Availability, 391
Failure intensity, 392
Failure rate, 392
Reliability, 391
Time-dependent stress, 549
Time-independent stress, 548
Time model, 793
Time redundancy, 1092
Time series modeling, 206
Autoregressive AR(p), Moving Average MA(q), Autoregressive Moving Average ARMA(p q), 207
Autoregressive Integrated Moving Average ARIMA(p d q) Models, 207
Integrated Moving Average IMA (0 1 1) Models, 208
Time to failure, 85
Time-between failures, 1196
Time-dependent maintenance policy, 796
Time-dependent reliability, 416, 422
Times ten rule, 26
TMR, 1088
Token ring, 1097
Tolerance design, 173, 177, 178, 180, 184, 236, 239
Total experience, 431, 439, 440
Total probability theorem, 612
Total productive maintenance (TPM), 769
Total product system, 881
Total quality control, 162
Total quality management, 28, 39, 165, 225, 226
Double EWMA controllers, 217
EWMA controllers, 216
Grubb's harmonic rule, 215
Initial intercept iteratively adjusted (IIIA) controllers, 203, 223
Variable EWME controllers, 219
TQM, *see* Total quality management
Transformation matrix, 1032
Transient failures, 1092
Transition function, 372
Maximum likelihood estimators, 375
Transition matrix, 1136, 1139
Transition probabilities, 820
Transition rate, 1135, 1136
Transmission (electricity), 1163, 1164
Tree topology grid architecture, 1079
Service MTST, 1080
Reliability indices, 1084
Parameterization and monitoring, 1084
Triple bottom line, 82, 876
Truck transmission, 825, 826, 828
Turnbull report, 861, 862
Two approaches,
Mechanism, 13
Reductionism, 13
Analytic vs. synthetic thinking, 14
Two-factor combinations, 243
Two-terminal or (s,t) reliability, 1049
Two types of failure, 819
Two-step optimization, 236
Two-stress models, 553
Two-unit system, 807, 808, 815, 816
Two-way tables, 243
Type I error, 189, 194
Type II error, 189

Ultimate strength design, 1027
Ultrasonic inspection, 1127, 1129
Unavailability, 86, 608–610, 617
Unbalanced magnetron, 968
Uncertainties, 719, 724, 1180
Uncertainty management, 722
Uncertainty measure, 482
Uncertainty ranking, 709
Uncertainty theory, 478–480
Unicast (s,t), 1049
Unicast routing protocols, 1095, 1096
Union carbide, 869
Universal generating function, 447, 1069
Universal moment generating function, 616
Unreliability, 602, 603
Upgrade trap, 83
Upper boundary points, 431–435, 443
Usage rate acceleration, 544
User conditions, 242
User-designer interaction, 23
Utilities,
Distribution companies (Disco), 991
Generation companies (Genco), 991
Transmission companies (Transco), 991
Restructuring, 1163, 1164
Vertically integrated, 1163, 1164
Utility function, 431, 439, 442, 443
Utilization of goods, 131

Validation and replication, 1018
Validation, 533, 534
Cost, 536
Value metrics, 96
Value stream analysis (VSA), 1016
Muda, 1017
Value stream mapping (VSM), 1017–1019
Voice of the customer (VOC), 1016
Wastes, 1017
Variable EWMA controllers, 219
Variables and attributes, 188, 190

Variance reduction techniques, 1037
Variation, 25, 28–31, 108
Variation in engineering, 28–30
Variational method, 506, 509
Vector autoregressive model, 825, 827
Viability, 98
Vibration measurement and analysis, 762
Virtual private networks (VPN), 1096
Virtual routers, 1097
Volume of resource flows, 129, 131
Voluntary standards, 887
Volvo, 889
Von Clausewitz, Carl, 114
VRRP protocol, 1097
Vulnerability, 724

Wald statistic, 829, 830
Warranty models, 793, 795
Warranty, 88
  Pro-rata warranty, 89
  Two-dimensional warranty, 90
  Unlimited free replacement warranty, 89
  Warranty cost analysis, 89
Waste management costs, 129
Waste minimization, 859
Watchdog timer, 1092
Wear, 953
Wearability, 967
Weibull analysis, 537
Weibull distribution, 536
WEEE directives, 11
What-if analysis, 651
Wireless communication network (WCN), 987, 1047
Wireless sensor network (WSN), 1047
World Nuclear Association (WNA), 992
Working state, 790
Working states, 373

Xerox, 130, 132, 134

Yamada exponential model, 1198
Yield losses, 769
Yule-walker estimation method, 829

Zero failure substantiation test, 535

100% inspection, 181, 183, 184