

Alessandro Birolini

Reliability Engineering

Theory and Practice

Seventh Edition



Springer

Reliability Engineering

Alessandro Birolini

Reliability Engineering

Theory and Practice

Seventh Edition

With 190 Figures, 60 Tables, 140 Examples,
and 70 Problems for Homework

 Springer

Prof. Dr. Alessandro Birolini*
Centro Storico—Bargello
I-50122 **Firenze**
Tuscany, Italy

birolini@emeritus.ethz.ch
www.ethz.ch/people/whoiswho,
www.birolini.ch

*Ingénieur et penseur, Ph.D., Professor Emeritus of Reliability Eng.
at the Swiss Federal Institute of Technology (ETH), Zurich

ISBN 978-3-642-39534-5 ISBN 978-3-642-39535-2 (eBook)

DOI 10.1007/978-3-642-39535-2

Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013945800

© Springer-Verlag Berlin Heidelberg 1994, 1997, 1999, 2004, 2007, 2010, 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law. The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

"La chance vient à l'esprit qui est prêt à la recevoir." 1)

Louis Pasteur

"Quand on aperçoit combien la somme de nos ignorances dépasse celle de nos connaissances, on se sent peu porté à conclure trop vite." 2)

Louis De Broglie

"One has to learn to consider causes rather than symptoms of undesirable events and avoid hypocritical attitudes."

Alessandro Birolini

1) "Opportunity comes to the intellect which is ready to receive it."

2) "When one recognizes how much the sum of our ignorance exceeds that of our knowledge, one is less ready to draw rapid conclusions."

Preface to the 7th Edition

The large interest granted to the 6th edition (over 2000 on-line requests per year) incited me for a 7th and last edition of this book (11 editions with the 4 German editions 1985 - 97).

The book shows how to build in, evaluate, and demonstrate reliability, maintainability, and availability of components, equipment, and systems. It presents the state-of-the-art of reliability engineering, both in theory and practice, and is based on the author's more than 30 years experience in this field, half in industry (part of which in setting up the Swiss Test. Lab. for VLSI, 1979 - 83 in Neuchâtel) and half as Professor of Reliability Engineering at the Swiss Federal Institute of Technology (ETH), Zurich. Considering that performance, dependability, cost, and time to market are key factors for today's products and services, but also that failure of complex systems can have major safety consequences, reliability engineering becomes a necessary support in developing and producing complex equipment and systems.

The structure of the book has been conserved through all editions, with main Chapters 1 to 8 and Appendices A1 to A11 (A10 & A11 since the 5th Edition 2007). Chapters 2, 4, and 6 deal carefully with analytical investigations, Chapter 5 with design guidelines, Chapters 3 and 7 with tests, and Chapter 8 with activities during production. Appendix A1 defines and comment on the terms commonly used in reliability engineering. Appendices A2-A5 have been added to support managers in answering the question of *how to specify and achieve high reliability (RAMS) targets for complex equipment and systems*. Appendices A6- A8 are a compendium of probability theory, stochastic processes, and mathematical statistics, as necessary for Chapters 2, 4, 6, and 7, consistent from a mathematical point of view but still with reliability engineering applications in mind (demonstration of established theorems is referred, and for all other propositions or equations, sufficient details for complete demonstration are given). Appendix A9 includes statistical tables, Laplace transforms, and probability charts. Appendix A10 resumes basic technological component's properties, and Appendix A11 gives a set of 70 problems for homework.

This structure makes the book *self contained* as a text book for postgraduate students or courses in industry (Fig. 1.9 on p. 24), allows a rapid access to practical results (as a desktop reference), and offers to theoretically oriented readers all mathematical tools to continue research in this field.

The book covers many aspects of reliability engineering using a common language, and has been improved step by step. Methods & tools are given in a way that they can be tailored to cover different reliability requirement levels, and be used for safety analysis too. A large number of tables (60), figures (190), and examples (210 of which 70 as problems for homework), as well as comprehensive reference list and index, amply support the text. This last edition reviews, refines, and extends all previous editions. New in particular includes:

- A strategy to mitigate *incomplete coverage* (p.255), yielding new models (Table 6.12c & d, p. 256).
- A comprehensive introduction to *human reliability* with a set of design guidelines to avoid human errors (pp. 158-159) and new models combining human errors probability and time to accomplish a task, based on semi-Markov processes (pp. 294-298).
- An improvement of the design guidelines for maintainability (pp. 154-158).
- An improvement of *reliability allocation* using Lagrange multiplier to consider cost aspects (p. 67).
- A comparison of four *repair strategies* (Table 4.4, p. 141).
- A comparison of basic models for *imperfect switching* (Table 6.11, p. 248).
- A refinement of *approximate expressions*, of concepts related to *regenerative processes*, and of the *use and limitations* of stochastic processes in modeling reliability problems (e.g. Table 6.1, p.171).
- New is also that relevant statements and rules have been written cursive and centered on the text.

Furthermore,

- Particular importance has been given to the selection of *design guidelines and rules*, the development of *approximate expressions* for large series-parallel systems, the *careful simplification of exact results* to allow in-depth trade off studies, and the *investigation of systems with complex structure* (preventive maintenance, imperfect switching, incomplete coverage, elements with more than one failure mode, fault tolerant reconfigurable systems, common cause failures).

- The central role of *software quality assurance* for complex equipment and systems is highlighted.
- The use of *interarrival times* starting by $x=0$ at each occurrence of the event considered, instead of the variable t , *giving a sense to MTBF* and allowing the introduction of a failure rate $\lambda(x)$ and a mean time to failure *MTTF* also for *repairable systems*, is carefully discussed (pp. 5-6, 41, 175, 316, 341, 378, 380) and consequently applied. Similar is for the *basic difference* between failure rate, (probability) density, and renewal density or intensity of a point process (pp. 7, 378, 426, 466, 524). In this context, the assumption *as-good-as-new* after repair is critically discussed wherever necessary, and the historical distinction between nonrepairable and repairable items is scaled down (removed for reliability function, failure rate, *MTTF*, and *MTBF*); national and international standards should better consider this fact and avoid definitions intrinsically valid only for constant (time independent) failure rates.
- Also valid is the introduction since the 1st edition of indices S_i for *reliability figures at system level* (e. g. $MTTF_{S_i}$), where S stands for system and i is the state entered at $t=0$ (system referring to the highest integration level of the item considered, and $t=0$ being the beginning of observations, $x=0$ for interarrival times). This is mandatory for judicious investigations at the system level.
- In agreement with the practical applications, *MTBF* is reserved for $MTBF = 1 / \lambda$.
- Important *prerequisites for accelerated tests* are carefully discussed (pp. 329-334), in particular to transfer an acceleration factor A from the *MTTF* ($MTTF_1 = A \cdot MTTF_2$) to the (random) failure-free time τ ($\tau_1 = A \cdot \tau_2$).
- *Asymptotic & steady-state* is used for *stationary*, by assuming *irreducible embedded chains*; *repair for restoration*, by neglecting administrative, logistical, technical delays; *mean for expected value*. For reliability applications, pairwise independence assures, in general, totally (mutually, statistically, stochastically) independence, *independent* is thus used for *totally independent*.

The book has growth from about 400 to 600 pages, with main improvements in the 4th to 7th Editions.

- 4th Edition: Complete review and general refinements.
- 5th Edition: Introduction to phased-mission systems, common cause failures, Petri nets, dynamic FTA, nonhomogeneous Poisson processes, and trend tests; problems for homework.
- 6th Edition: Proof of Eqs. (6.88) & (6.94), introduction to network reliability, event trees & binary decision diagrams, extensions of maintenance strategies and incomplete coverage, refinements for large complex systems and approximate expressions.

The launching of the 6th Edition of this book coincided with my 70th anniversary, this was celebrated with a special Session at the 12th Int. Conf. on Quality and Dependability CCF2010 held in Sinaia (RO), 22-24 September 2010. My response to the last question at the interview [1.0] given to Prof. Dr. Ioan C. Bacivarov, Chairman of the International Scientific Committee of CCF2010, can help to explain the acceptance of this book:

"Besides more than 15 years experience in the industry, and a predisposition to be a self-taught man, my attitude to life was surely an important key for the success of my book. This is best expressed in the three sentences given on the first page of this book. These sentences, insisting on generosity, modesty and responsibility apply quite general to a wide class of situations and people, from engineers to politicians, and it is to hope that the third sentence, in particular, will be considered by a growing number of humans, now, in front of the ecological problems we are faced and in front of the necessity to create a federal world wide confederation of democratic states in which freedom is primarily respect for the other."

The comments of many friends and the agreeable cooperation with Springer-Verlag are gratefully acknowledged. Looking back to all editions (1st German 1985), thanks are due, in particular, to K.P. LaSala for reviewing the 4th & 6th Editions [1.17], I.C. Bacivarov for reviewing the 6th Edition [1.0], book reviewers of the German editions, P. Franken and I. Kovalenko for commenting Appendices A6-A8, A. Bobbio F. Bonzanigo, M. Held for supporting numerical evaluations, J. Thalhammer for supporting the edition of all figures, and L. Lambert for reading final manuscripts.

Contents

1	Basic Concepts, Quality & Reliability (RAMS) Assurance of Complex Equip. & Systems . . .	1
1.1	Introduction	1
1.2	Basic Concepts	2
1.2.1	Reliability	2
1.2.2	Failure	3
1.2.3	Failure Rate, <i>MTTF</i> , <i>MTBF</i>	4
1.2.4	Maintenance, Maintainability	8
1.2.5	Logistic Support	8
1.2.6	Availability	9
1.2.7	Safety, Risk, and Risk Acceptance	9
1.2.8	Quality	11
1.2.9	Cost and System Effectiveness.	11
1.2.10	Product Liability	15
1.2.11	Historical Development	16
1.3	Basic Tasks & Rules for Quality & Rel. (RAMS) Assurance of Complex Eq. & Systems .	17
1.3.1	Quality and Reliability (RAMS) Assurance Tasks	17
1.3.2	Basic Quality and Reliability (RAMS) Assurance Rules	19
1.3.3	Elements of a Quality Assurance System.	21
1.3.4	Motivation and Training	24
2	Reliability Analysis During the Design Phase (Nonrepairable Elements up to System Failure) . . .	25
2.1	Introduction	25
2.2	Predicted Reliability of Equipment and Systems with Simple Structure	28
2.2.1	Required Function	28
2.2.2	Reliability Block Diagram	28
2.2.3	Operating Conditions at Component Level, Stress Factors	33
2.2.4	Failure Rate of Electronic Components	35
2.2.5	Reliability of One-Item Structures	39
2.2.6	Reliability of Series-Parallel Structures	41
2.2.6.1	Systems without Redundancy	41
2.2.6.2	Concept of Redundancy	42
2.2.6.3	Parallel Models	43
2.2.6.4	Series - Parallel Structures	45
2.2.6.5	Majority Redundancy	49
2.2.7	Part Count Method	51
2.3	Reliability of Systems with Complex Structure	52
2.3.1	Key Item Method	52
2.3.1.1	Bridge Structure	53
2.3.1.2	Rel. Block Diagram in which Elements Appear More than Once	54
2.3.2	Successful Path Method	55
2.3.3	State Space Method	56
2.3.4	Boolean Function Method	57
2.3.5	Parallel Models with Constant Failure Rates and Load Sharing	61
2.3.6	Elements with more than one Failure Mechanism or one Failure Mode	64
2.3.7	Basic Considerations on Fault Tolerant Structures	66
2.4	Reliability Allocation and Optimization	67

2.5	Mechanical Reliability, Drift Failures	68
2.6	Failure Modes Analyses	72
2.7	Reliability Aspects in Design Reviews	77
3	Qualification Tests for Components and Assemblies	81
3.1	Basic Selection Criteria for Electronic Components	81
3.1.1	Environment	82
3.1.2	Performance Parameters	84
3.1.3	Technology	84
3.1.4	Manufacturing Quality	86
3.1.5	Long-Term Behavior of Performance Parameters	86
3.1.6	Reliability	86
3.2	Qualification Tests for Complex Electronic Components	87
3.2.1	Electrical Test of Complex ICs	88
3.2.2	Characterization of Complex ICs	90
3.2.3	Environmental and Special Tests of Complex ICs	92
3.2.4	Reliability Tests	101
3.3	Failure Modes, Mechanisms, and Analysis of Electronic Components	101
3.3.1	Failure Modes of Electronic Components	101
3.3.2	Failure Mechanisms of Electronic Components	102
3.3.3	Failure Analysis of Electronic Components	102
3.3.4	Present VLSI Production-Related Reliability Problems	106
3.4	Qualification Tests for Electronic Assemblies	107
4	Maintainability Analysis	112
4.1	Maintenance, Maintainability	112
4.2	Maintenance Concept	115
4.2.1	Fault Detection (Recognition) and Localization	116
4.2.2	Equipment and Systems Partitioning	118
4.2.3	User Documentation	118
4.2.4	Training of Operation and Maintenance Personnel	119
4.2.5	User Logistic Support	119
4.3	Maintainability Aspects in Design Reviews	121
4.4	Predicted Maintainability	121
4.4.1	Calculation of $MTTR_S$	121
4.4.2	Calculation of $MTTPM_S$	125
4.5	Basic Models for Spare Parts Provisioning	125
4.5.1	Centralized Logistic Support, Nonrepairable Spare Parts	125
4.5.2	Decentralized Logistic Support, Nonrepairable Spare Parts	129
4.5.3	Repairable Spare Parts	130
4.6	Maintenance Strategies	134
4.6.1	Complete renewal at each maintenance action	134
4.6.2	Block replacement with minimal repair at failure	138
4.6.3	Further considerations on maintenance strategies	139
4.7	Basic Cost Considerations	142
5	Design Guidelines for Reliability, Maintainability, and Software Quality	144
5.1	Design Guidelines for Reliability	144
5.1.1	Derating	144

- 5.1.2 Cooling 145
- 5.1.3 Moisture 147
- 5.1.4 Electromagnetic Compatibility, ESD Protection 148
- 5.1.5 Components and Assemblies 150
 - 5.1.5.1 Component Selection 150
 - 5.1.5.2 Component Use 150
 - 5.1.5.3 PCB and Assembly Design 151
 - 5.1.5.4 PCB and Assembly Manufacturing 152
 - 5.1.5.5 Storage and Transportation 153
- 5.1.6 Particular Guidelines for IC Design and Manufacturing 153
- 5.2 Design Guidelines for Maintainability 154
 - 5.2.1 General Guidelines 154
 - 5.2.2 Testability 155
 - 5.2.3 Connections, Accessibility, Exchangeability 157
 - 5.2.4 Adjustment 158
 - 5.2.5 Human, Ergonomic, and Safety Aspects 158
- 5.3 Design Guidelines for Software Quality 159
 - 5.3.1 Guidelines for Software Defect Prevention 162
 - 5.3.2 Configuration Management 165
 - 5.3.3 Guidelines for Software Testing 166
 - 5.3.4 Software Quality Growth Models 166
- 6 Reliability and Availability of Repairable Systems 169**
 - 6.1 Introduction, General Assumptions, Conclusions 169
 - 6.2 One-Item Structure 175
 - 6.2.1 One-Item Structure New at Time $t = 0$ 176
 - 6.2.1.1 Reliability Function 176
 - 6.2.1.2 Point Availability 177
 - 6.2.1.3 Average Availability 178
 - 6.2.1.4 Interval Reliability 179
 - 6.2.1.5 Special Kinds of Availability 180
 - 6.2.2 One-Item Structure New at Time $t = 0$ and with Constant Failure Rate λ 183
 - 6.2.3 One-Item Structure with Arbitrary Conditions at $t = 0$ 184
 - 6.2.4 Asymptotic Behavior 185
 - 6.2.5 Steady-State Behavior 187
 - 6.3 Systems without Redundancy 189
 - 6.3.1 Series Structure with Constant Failure and Repair Rates 189
 - 6.3.2 Series Structure with Constant Failure and Arbitrary Repair Rates 192
 - 6.3.3 Series Structure with Arbitrary Failure and Repair Rates 193
 - 6.4 1-out-of-2 Redundancy (Warm, one Repair Crew) 196
 - 6.4.1 1-out-of-2 Redundancy with Constant Failure and Repair Rates 196
 - 6.4.2 1-out-of-2 Redundancy with Constant Failure and Arbitrary Rep. Rates 204
 - 6.4.3 1-out-of-2 Red. with Const. Failure Rate in Reserve State & Arbitr. Rep. Rates . 207
 - 6.5 k -out-of- n Redundancy (Warm, Identical Elements, one Repair Crew) 213
 - 6.5.1 k -out-of- n Redundancy with Constant Failure and Repair Rates 214
 - 6.5.2 k -out-of- n Redundancy with Constant Failure and Arbitrary Repair Rates . . . 218
 - 6.6 Simple Series - Parallel Structures (one Repair Crew) 220
 - 6.7 Approximate Expressions for Large Series - Parallel Structures 226
 - 6.7.1 Introduction 226
 - 6.7.2 Application to a Practical Example 230

6.8	Systems with Complex Structure (one Repair Crew)	238
6.8.1	General Considerations	238
6.8.2	Preventive Maintenance	240
6.8.3	Imperfect Switching	243
6.8.4	Incomplete Coverage	249
6.8.5	Elements with more than two States or one Failure Mode	257
6.8.6	Fault Tolerant Reconfigurable Systems	259
6.8.6.1	Ideal Case	259
6.8.6.2	Time Censored Reconfiguration (Phased-Mission Systems)	259
6.8.6.3	Failure Censored Reconfiguration	266
6.8.6.4	Reward and Frequency /Duration Aspects	270
6.8.7	Systems with Common Cause Failures	271
6.8.8	Basic Considerations on Network-Reliability	275
6.8.9	General Procedure for Modeling Complex Systems	277
6.9	Alternative Investigation Methods	280
6.9.1	Systems with Totally Independent Elements	280
6.9.2	Static and Dynamic Fault Trees	280
6.9.3	Binary Decision Diagrams	283
6.9.4	Event Trees	286
6.9.5	Petri Nets	287
6.9.6	Numerical Reliability and Availability Computation	289
6.9.6.1	Numerical Computation of System's Reliability and Availability	289
6.9.6.2	Monte Carlo Simulations	290
6.9.7	Approximate expressions for Large, Complex Systems: Basic Considerations	293
6.10	Human Reliability	294
7	Statistical Quality Control and Reliability Tests	299
7.1	Statistical Quality Control	299
7.1.1	Estimation of a Defective Probability p	300
7.1.2	Simple Two-sided Sampling Plans for Demonstration of a Def. Probability p	302
7.1.2.1	Simple Two-sided Sampling Plan	303
7.1.2.2	Sequential Test	305
7.1.3	One-sided Sampling Plans for the Demonstration of a Def. Probability p	306
7.2	Statistical Reliability Tests	309
7.2.1	Reliability and Availability Estimation & Demon. for a given fixed Mission	309
7.2.2	Availability Estimation & Demonstration for Continuous Operation (steady-state)	311
7.2.2.1	Availability Estimation (Erlangian Failure-Free and/or Repair Times)	311
7.2.2.2	Availability Demonstration (Erlangian Failure-Free and/or Repair Times)	313
7.2.2.3	Further Availability Evaluation Methods for Continuous Operation	314
7.2.3	Estimation and Demonstration of a Const. Failure Rate λ (or of $MTBF=1/\lambda$)	316
7.2.3.1	Estimation of a Constant Failure Rate λ	318
7.2.3.2	Simple Two-sided Test for the Demonstration of λ	320
7.2.3.3	Simple One-sided Test for the Demonstration of λ	324
7.3	Statistical Maintainability Tests	325
7.3.1	Estimation of an $MTTR$	325
7.3.2	Demonstration of an $MTTR$	327
7.4	Accelerated Testing	329
7.5	Goodness-of-fit Tests	334
7.5.1	Kolmogorov-Smirnov Test	334
7.5.2	Chi-square Test	338

7.6	Statistical Analysis of General Reliability Data	341
7.6.1	General considerations	341
7.6.2	Tests for Nonhomogeneous Poisson Processes	343
7.6.3	Trend Tests	345
7.6.3.1	Tests of a HPP versus a NHPP with increasing intensity	345
7.6.3.2	Tests of a HPP versus a NHPP with decreasing intensity	348
7.6.3.3	Heuristic Tests to distinguish between HPP and Monotonic Trend	349
7.7	Reliability Growth	351
8	Quality & Reliability (RAMS) Assurance During Production Phase (Basic Considerations)	357
8.1	Basic Activities	357
8.2	Testing and Screening of Electronic Components	358
8.2.1	Testing of Electronic Components	358
8.2.2	Screening of Electronic Components	359
8.3	Testing and Screening of Electronic Assemblies	362
8.4	Test and Screening Strategies, Economic Aspects	364
8.4.1	Basic Considerations	364
8.4.2	Quality Cost Optimization at Incoming Inspection Level	367
8.4.3	Procedure to handle first deliveries	372
 <i>Appendices (A1 -A11)</i>		
A1	Terms and Definitions	373
A2	Quality and Reliability (RAMS) Standards	387
A2.1	Introduction	387
A2.2	General Requirements in the Industrial Field	388
A2.3	Requirements in the Aerospace, Railway, Defense, and Nuclear Fields	390
A3	Definition and Realization of Quality and Reliability (RAMS) Requirements	391
A3.1	Definition of Quality and Reliability (RAMS) Requirements	391
A3.2	Realization of Quality & Reliability (RAMS) Requirements for Complex Eq. & Syst.	393
A3.3	Elements of a Quality and Reliability (RAMS) Assurance Program	398
A3.3.1	Project Organization, Planning, and Scheduling	398
A3.3.2	Quality and Reliability (RAMS) Requirements.	399
A3.3.3	Reliability, Maintainability, and Safety Analysis	399
A3.3.4	Selection and Qualification of Components, Materials, Manuf. Processes	400
A3.3.5	Software Quality Assurance	400
A3.3.6	Configuration Management	401
A3.3.7	Quality Tests	402
A3.3.8	Quality Data Reporting System	404
A4	Checklists for Design Reviews	405
A4.1	System Design Review	405
A4.2	Preliminary Design Reviews	406
A4.3	Critical Design Review (System Level)	409
A5	Requirements for Quality Data Reporting Systems	410
A6	Basic Probability Theory	413
A6.1	Field of Events	413
A6.2	Concept of Probability	415

A6.3	Conditional Probability, Independence	418
A6.4	Fundamental Rules of Probability Theory	419
A6.4.1	Addition Theorem for Mutually Exclusive Events	419
A6.4.2	Multiplication Theorem for Two Independent Events	420
A6.4.3	Multiplication Theorem for Arbitrary Events	421
A6.4.4	Addition Theorem for Arbitrary Events	421
A6.4.5	Theorem of Total Probability	422
A6.5	Random Variables, Distribution Functions	423
A6.6	Numerical Parameters of Random Variables	429
A6.6.1	Expected Value (Mean)	429
A6.6.2	Variance	432
A6.6.3	Modal Value, Quantile, Median	434
A6.7	Multidimensional Random Variables, Conditional Distributions	434
A6.8	Numerical Parameters of Random Vectors	436
A6.8.1	Covariance Matrix, Correlation Coefficient	437
A6.8.2	Further Properties of Expected Value and Variance	438
A6.9	Distribution of the Sum of Indep. Positive Random Variables and of τ_{\min}, τ_{\max}	438
A6.10	Distribution Functions used in Reliability Analysis	441
A6.10.1	Exponential Distribution	441
A6.10.2	Weibull Distribution	442
A6.10.3	Gamma Distribution, Erlangian Distribution, and χ^2 -Distribution	444
A6.10.4	Normal Distribution	446
A6.10.5	Lognormal Distribution	447
A6.10.6	Uniform Distribution	449
A6.10.7	Binomial Distribution	449
A6.10.8	Poisson Distribution	451
A6.10.9	Geometric Distribution	453
A6.10.10	Hypergeometric Distribution	454
A6.11	Limit Theorems	454
A6.11.1	Laws of Large Numbers	455
A6.11.2	Central Limit Theorem	456
A7	Basic Stochastic-Processes Theory	460
A7.1	Introduction	460
A7.2	Renewal Processes	463
A7.2.1	Renewal Function, Renewal Density	465
A7.2.2	Recurrence Times	468
A7.2.3	Asymptotic Behavior	469
A7.2.4	Stationary Renewal Processes	471
A7.2.5	Homogeneous Poisson Processes (HPP)	472
A7.3	Alternating Renewal Processes	474
A7.4	Regenerative Processes with a Finite Number of States	478
A7.5	Markov Processes with a Finite Number of States	480
A7.5.1	Markov Chains with a Finite Number of States	480
A7.5.2	Markov Processes with a Finite Number of States	482
A7.5.3	State Probabilities and Stay Times in a Given Class of States	491
A7.5.3.1	Method of Differential Equations	491
A7.5.3.2	Method of Integral Equations	495
A7.5.3.3	Stationary State and Asymptotic Behavior	496
A7.5.4	Frequency / Duration and Reward Aspects	498
A7.5.4.1	Frequency / Duration	498
A7.5.4.2	Reward	500

A7.5.5	Birth and Death Process	501
A7.6	Semi-Markov Processes with a Finite Number of States	505
A7.7	Semi-regenerative Processes with a Finite Number of States.	510
A7.8	Nonregenerative Stochastic Processes with a Countable Number of States	515
A7.8.1	General Considerations	515
A7.8.2	Nonhomogeneous Poisson Processes (NHPP)	516
A7.8.3	Superimposed Renewal Processes	520
A7.8.4	Cumulative Processes	521
A7.8.5	General Point Processes	523
A8	Basic Mathematical Statistics	525
A8.1	Empirical Methods	525
A8.1.1	Empirical Distribution Function	526
A8.1.2	Empirical Moments and Quantiles	528
A8.1.3	Further Applications of the Empirical Distribution Function	529
A8.2	Parameter Estimation	533
A8.2.1	Point Estimation	533
A8.2.2	Interval Estimation	538
A8.2.2.1	Estimation of an Unknown Probability p	538
A8.2.2.2	Estimation of Param. λ for Exp. Distrib.: Fixed T , instant. repl.	542
A8.2.2.3	Estimation of Param. λ for Exp. Distrib.: Fixed n , no repl.	543
A8.2.2.4	Availability Estimation (Erlangian Failure-Free and/or Repair Times)	545
A8.3	Testing Statistical Hypotheses	547
A8.3.1	Testing an Unknown Probability p	548
A8.3.1.1	Simple Two-sided Sampling Plan	549
A8.3.1.2	Sequential Test	550
A8.3.1.3	Simple One-sided Sampling Plan	551
A8.3.1.4	Availability Demonstr. (Erlangian Failure-Free and/or Rep. Times)	553
A8.3.2	Goodness-of-fit Tests for Completely Specified $F_0(t)$	555
A8.3.3	Goodness-of-fit Tests for $F_0(t)$ with Unknown Parameters	558
A9	Tables and Charts	561
A9.1	Standard Normal Distribution	561
A9.2	χ^2 -Distribution (Chi-Square Distribution)	562
A9.3	t -Distribution (Student distribution)	563
A9.4	F -Distribution (Fisher distribution)	564
A9.5	Table for the Kolmogorov-Smirnov Test	565
A9.6	Gamma Function	566
A9.7	Laplace Transform	567
A9.8	Probability Charts (Probability Plot Papers)	569
A9.8.1	Lognormal Probability Chart	569
A9.8.2	Weibull Probability Chart	570
A9.8.3	Normal Probability Chart	571
A10	Basic Technological Component's Properties	572
A11	Problems for Homework	576
	Acronyms	582
	References	583
	Index	605

1 Basic Concepts, Quality and Reliability (RAMS) Assurance of Complex Equipment and Systems

Considering that complex equipment and systems are generally repairable, contain redundancy and must be safe, the term *reliability* appears often for *reliability, maintainability, availability & safety*. RAMS (in brackets) is used to point out this wherever necessary in the text. The purpose of *reliability (RAMS) engineering* is to develop methods and tools to *evaluate and demonstrate* reliability, maintainability, availability, and safety of components, equipment & systems, as well as to *support* development and production engineers in *building in* these characteristics. In order to be cost and time effective, reliability (RAMS) engineering must be integrated in the project activities, support quality assurance and concurrent engineering efforts, and be performed without bureaucracy. This chapter introduces basic concepts, shows their relationships, and discusses the tasks necessary to assure quality and reliability (RAMS) of complex equipment & systems with *high quality and reliability (RAMS) requirements*. A comprehensive list of definitions is given in Appendix A1. Standards for quality and reliability (RAMS) assurance are discussed in Appendix A2. Refinements of *management* aspects are given in Appendices A3 - A5.

1.1 Introduction

Until the nineteen-sixties, quality targets were deemed to have been reached when the item considered was found to be free of *defects* or *systematic failures* at the time it left the manufacturer. The growing complexity of equipment and systems, as well as the rapidly increasing cost incurred by loss of operation as a consequence of failures, have brought to the forefront the aspects of *reliability, maintainability, availability, and safety*. The expectation today is that complex equipment and systems are not only *free from defects and systematic failures* at time $t = 0$ (when they are put into operation), but also *perform the required function failure free* for a stated time interval and *have a fail-safe behavior in case of critical or catastrophic failures*. However, the question of whether a given item will operate without failures during a stated period of time cannot be simply answered by *yes* or *no*, on the basis of a compliance test. Experience shows that *only a probability* for this occurrence can be given. This probability is a measure of the *item's*

reliability and can be *interpreted* as follows:

If n statistically identical and independent items are put into operation at time $t = 0$ to perform a given mission and $\bar{v} \leq n$ of them accomplish it successfully, then the ratio \bar{v} / n is a random variable which converges for increasing n to the true value of the reliability (Appendix A6.11).

Performance parameters as well as *reliability, maintainability, availability, and safety* have to be *built in* during design & development and retained during production and operation of the item. After the introduction of some important concepts in Section 1.2, Section 1.3 gives basic tasks and rules for quality and reliability assurance of *complex equipment and systems with high quality and reliability requirements* (see Appendix A1 for a comprehensive list of definitions and Appendices A2 - A5 for a refinement of management aspects).

1.2 Basic Concepts

This section introduces important concepts used in reliability engineering and shows their relationships (see Appendix A1 for a more complete list).

1.2.1 Reliability

Reliability is a *characteristic* of the item, expressed by the *probability* that it will perform its *required function* under *given conditions* for a *stated time interval*. It is generally designated by R . From a qualitative point of view, reliability can be defined as the *ability of the item to remain functional*. Quantitatively, reliability specifies the *probability that no operational interruptions* will occur during a stated time interval. This does not mean that *redundant* parts may not fail, such parts can fail and be repaired (without operational interruption at item (system) level). The concept of reliability thus applies to *nonrepairable* as well as to *repairable* items (Chapters 2 and 6, respectively). To make sense, a numerical statement of reliability (e. g. $R = 0.9$) must be accompanied by the definition of the *required function*, the *operating conditions*, and the *mission duration*. In general, it is also important to know whether or not the item can be considered new when the mission starts.

An *item* is a functional or structural *unit* of arbitrary complexity (e.g. component, assembly, equipment, subsystem, system) that can be considered as an *entity* for investigations.⁺⁾ It may consist of hardware, software, or both and may also include human resources. Often, *ideal* human aspects and logistic support are assumed, even if (for simplicity) the term *system* is used instead of *technical system*.

^{+) System refers in this book, and often in practical applications, to the highest integration level of the item considered.}

The *required function* specifies the item's task. For example, for given inputs, the item outputs have to be constrained within specified tolerance bands (performance parameters should always be given with tolerances). The definition of the required function is the *starting point for any reliability analysis*, as it defines *failures*.

Operating conditions have an important influence on reliability, and must therefore be specified with care. Experience shows for instance, that the failure rate of semiconductor devices will double for operating temperature increase of 10 to 20°C.

The required function and/ or operating conditions can be *time dependent*. In these cases, a *mission profile* has to be defined and all reliability figures will be related to it. A representative mission profile and the corresponding reliability targets should be given in the *item's specifications*.

Often the mission duration is considered as a parameter t , the *reliability function* is then defined by $R(t)$. $R(t)$ is the probability that no failure at item level will occur in the interval $(0, t]$. The item's condition at $t=0$ (new or not) influences final results. To consider this, in this book reliability figures at system level will have indices S_i (e. g. $R_{S_i}(t)$), where S stands for system and i is the state entered at $t=0$ (Tab. 6.2). State 0, with all elements new, is often assumed at $t=0$, yielding $R_{S_0}(t)$.

A distinction between *predicted* and *estimated* or *assessed* reliability is important. The first one is calculated on the basis of the item's reliability structure and the failure rate of its components (Sections 2.2 & 2.3), the second is obtained from a statistical evaluation of reliability tests or from field data by known environmental and operating conditions (Section 7.2).

The concept of reliability can be extended to processes and services as well, although *human aspects* can lead to modeling difficulties (Sections 1.2.7, 5.2.5, 6.10).

1.2.2 Failure

A *failure* occurs when the item stops performing its required function. As simple as this definition is, it can become difficult to apply it to complex items. The *failure-free time* (hereafter used as a synonym for *failure-free operating time*) is generally a *random variable*. It is often reasonably long; but it can be very short, for instance because of a failure caused by a transient event at turn-on. A general assumption in investigating failure-free times is that at $t=0$ the item is free of *defects* and *systematic failures*. Besides their *frequency*, failures should be classified (as far as possible) according to the mode, cause, effect, and mechanism:

1. *Mode*: The mode of a failure is the *symptom* (local effect) by which a failure is observed; e. g., opens, shorts, or drift for electronic components (Table 3.4); brittle rupture, creep, cracking, seizure, fatigue for mechanical components.
2. *Cause*: The cause of a failure can be *intrinsic*, due to weaknesses in the item and/ or wear out, or *extrinsic*, due to errors, misuse or mishandling during the design, production, or use. Extrinsic causes often lead to *systematic failures*, which are *deterministic* and should be considered like *defects* (dynamic

defects in software quality). *Defects are present at $t = 0$* , even if often they can not be discovered at $t = 0$. *Failures appear always in time*, even if the time to failure is short as it can be with systematic or early failures.

3. *Effect*: The effect (consequence) of a failure can be different if considered on the item itself or at higher level. A usual classification is: *non relevant, partial, complete, and critical failure*. Since a failure can also cause further failures, distinction between *primary and secondary failure* is important.
4. *Mechanism*: Failure mechanism is the physical, chemical, or other process resulting in a failure (see Table 3.5 (p. 103) for some examples).

Failures can also be classified as *sudden and gradual*. In this case, sudden and complete failures are termed *cataleptic failures*, gradual and partial failures are termed *degradation failures*. As failure is not the only cause for the item being down, the general term used to define the down state of an item (not caused by a preventive maintenance, other planned actions, or lack of external resources) is

1.2.3 Failure Rate, *MTTF*, *MTBF*

The *failure rate* plays an important role in reliability analysis. This Section introduces it heuristically, see Appendix A6.5 for an analytical derivation.

Let us assume that n *statistically identical*, new, and independent items are put into operation at time $t = 0$, under the same conditions, and at the time t a subset $\bar{v}(t)$ of these items have not yet failed. $\bar{v}(t)$ is a right continuous decreasing step function (Fig. 1.1). t_1, \dots, t_n , measured from $t = 0$, are the *observed* failure-free times (operating times to failure) of the n items considered. They are independent realizations of a *random variable* τ (hereafter identified as failure-free time) and must not be confused with arbitrary points on the time axis (t_1^*, t_2^*, \dots). The quantity

$$\hat{E}[\tau] = \frac{t_1 + \dots + t_n}{n} \quad (1.1)$$

is the *empirical mean* (empirical expected value) of τ . Empirical quantities are statistical estimates, marked with $\hat{}$ in this book. For $n \rightarrow \infty$, $\hat{E}[\tau]$ converges to the true mean $E[\tau] = \text{MTTF}$ given by Eq. (1.8) (Eqs. (A6.147), (A8.7)). The function

$$\hat{R}(t) = \frac{\bar{v}(t)}{n} \quad (1.2)$$

is the *empirical reliability function*, which converges to $R(t)$ for $n \rightarrow \infty$ (Eq. (A8.5)).

For an arbitrary time interval $(t, t + \delta t]$, the *empirical failure rate* is defined as

$$\hat{\lambda}(t) = \frac{\bar{v}(t) - \bar{v}(t + \delta t)}{\bar{v}(t)\delta t}. \quad (1.3)$$

$\hat{\lambda}(t)\delta t$ is the ratio of the items failed in the interval $(t, t + \delta t]$ to the number of items

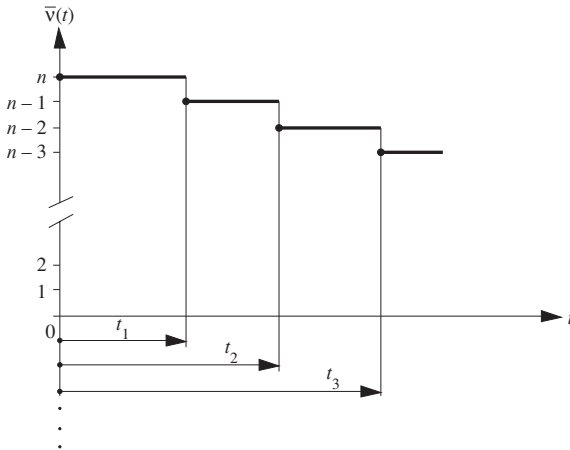


Figure 1.1 Number $\bar{v}(t)$ of (nonrepairable) items still operating at time t

still operating (or surviving) at time t . Applying Eq. (1.2) to Eq. (1.3) yields

$$\hat{\lambda}(t) = \frac{\hat{R}(t) - \hat{R}(t + \delta t)}{\delta t \hat{R}(t)}. \tag{1.4}$$

For $R(t)$ derivable, $n \rightarrow \infty$ & $\delta t \rightarrow 0$, $\hat{\lambda}(t)$ converges to the (instantaneous) failure rate

$$\lambda(t) = \frac{-d R(t) / dt}{R(t)}. \tag{1.5}$$

Considering $R(0) = 1$ (at $t = 0$ all items are new), Eq. (1.5) leads to

$$R(t) = e^{-\int_0^t \lambda(x) dx}, \quad (\text{for } R(0) = 1). \tag{1.6}$$

The failure rate $\lambda(t)$ given by Eqs. (1.3) - (1.5) applies in particular to nonrepairable items (Figs. 1.1 & 1.2). However,

considering Eq. (A6.25) $\lambda(t)$ can also be defined for repairable items which are as-good-as-new after repair (renewal), taking instead of t the variable x starting by $x = 0$ at each renewal (as for interarrival times); this is important when investigating repairable systems, and holds in particular for $\lambda(x) = \lambda$ (see remarks on pp. 6, 40-41, 378, 380).

If a repairable system cannot be restored to be as-good-as-new after repair (with respect to the state considered), i.e., if at least one element with time dependent failure rate has not been renewed at every repair, failure intensity $z(t)$ has to be used (see pp. 378, 426, 524 for comments). The use of hazard rate for $\lambda(t)$ should be avoided.

In many practical applications, $\lambda(t) = \lambda$ can be assumed. Eq. (1.6) then yields

$$R(t) = e^{-\lambda t}, \quad (\text{for } \lambda(t) = \lambda), \quad (1.7)$$

and the failure-free time $\tau > 0$ is *exponentially distributed* ($F(t) = \Pr\{\tau \leq t\} = 1 - e^{-\lambda t}$);

for this, and only in this case, the failure rate λ can be estimated by $\hat{\lambda} = k/T$, where T is a given (fixed) cumulative operating time and k the total number of failures during T (Eqs. (7.28) and (A8.46)).

The *mean* (expected value) of the failure-free time $\tau > 0$ is given by (Eq. (A6.38))

$$MTTF = E[\tau] = \int_0^{\infty} R(t) dt, \quad (1.8)$$

where *MTTF* stands for *mean time to failure*. For $\lambda(t) = \lambda$ it follows $E[\tau] = 1/\lambda$.

A constant (time independent) failure rate λ is often considered also for *repairable items*. Assuming that the item is *as-good-as-new after each repair*, successive failure-free times are then *independent random variables, exponentially distributed with the same parameter λ , and with mean*

$$MTBF = 1/\lambda, \quad (\text{for } \lambda(x) = \lambda, x \text{ starting at } 0 \text{ after each repair}). \quad (1.9)$$

MTBF stands for *mean operating time between failures*. Also because of the statistical estimate $\hat{MTBF} = T/k$ used in practical applications (p.318), *MTBF* should be confined to the case of repairable items with *constant failure rate*. However, at component level $MTBF = 10^8$ h for $\lambda = 10^{-8} \text{h}^{-1}$ has no practical significance. For systems with >2 states, MUT_{ζ} (system mean up time) is used (p. 278, Table 6.2). Finally,

it must be pointed out that for a repairable item, the only possibility to have successive statistically identical and independent operating times after each repair (interarrival times), giving a sense to a mean operating time between failures (MTBF), is to re-establish at each repair an as-good-as-new situation, replacing all parts with non constant failure rates.

The failure rate of a *large population of statistically identical and independent items* exhibits often a typical bathtub curve (Fig. 1.2) with the following 3 phases:

1. *Early failures*: $\lambda(t)$ decreases (in general) rapidly with time; failures in this phase are attributable to *randomly distributed weaknesses* in materials, components, or production processes.
2. *Failures with constant (or nearly so) failure rate*: $\lambda(t)$ is approximately constant; failures in this period are *Poisson distributed* and often cataleptic.
3. *Wear out failures*: $\lambda(t)$ increases with time; failures in this period are attributable to aging, wear out, fatigue, etc. (e.g. corrosion, electromigration).

Early failures are *not deterministic* and appear in general randomly distributed in time and over the items. During the early failure period, $\lambda(t)$ must not necessarily decrease as in Fig. 1.2, in some cases it can oscillate. To eliminate early failures,

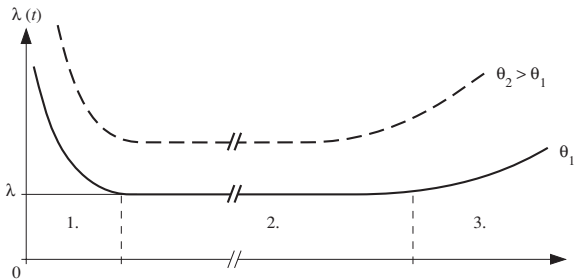


Figure 1.2 Typical shape for the failure rate of a *large population of statistically identical and independent (nonrepairable) items* (dashed is a possible shift for a higher stress, e. g. ambient temperature)

burn-in or *environmental stress screening* is used (Chapter 8). Early failures must be distinguished from *defects* and *systematic failures*, which are present at $t = 0$, deterministic, caused by *errors* or *mistakes*, and whose elimination requires a *change* in design, production process, operational procedure, documentation or other. Length of early failure period varies in practice from few h to some 1'000h. The presence of a period with *constant* (or nearly so) *failure rate* $\lambda(t) \approx \lambda$ is realistic for many equipment & systems, and useful for calculations. The *memoryless property*, which characterizes this period, leads to exponentially distributed failure-free times and to a time homogeneous *Markov process* for the time behavior of a repairable system if also *constant repair rates* can be assumed (Chapter 6). An *increasing failure rate* after a given operating time (> 10 years for many electronic equipment) is typical for most items and appears because of degradation phenomena due to wear out.

A possible explanation for the shape of $\lambda(t)$ given in Fig. 1.2 is that the population contains np_f weak elements and $n(1-p_f)$ good ones. The distribution of the failure-free time can then be expressed by a *weighted sum* of the form $F(t) = p_f F_1(t) + (1-p_f)F_2(t)$, where $F_1(t)$ can be a gamma ($\beta < 1$) and $F_2(t)$ a shifted Weibull ($\beta > 1$) distribution (Eqs. (A6.34), (A6.96), (A6.97)), see also pp. 337, 355 & 467 for alternative possibilities.

The failure rate strongly depends upon the item's *operating conditions*, see e. g. Figs. 2.4-2.6 and Table 2.3. Typical figures for λ are 10^{-10} to 10^{-7} h^{-1} for electronic components at 40°C , doubling for a temperature increase of 10 to 20°C .

From Eqs. (1.3) - (1.5) one recognizes that for an *item new at* $t = 0$ and $\delta t \rightarrow 0$, $\lambda(t)\delta t$ is the *conditional probability* for failure in $(t, t + \delta t]$ *given that the item has not failed in* $(0, t]$. Thus, $\lambda(t)$ is *not a density* as defined by Eq. (A6.23) and must be clearly distinguished from the density $f(t)$ of the failure-free time ($f(t)\delta t$ is the *unconditional probability* for failure in $(t, t + \delta t]$), from the *failure intensity* $z(t)$ of an arbitrary point process, and from the *intensity* $h(t)$ or $m(t)$ of a renewal or Poisson process (Eqs. (A7.228), (A7.24), (A7.193)); this also in the case of a homogeneous Poisson process, see pp. 378, 426, 466, 524 for further considerations.

The concept of failure rate applied to humans yields a shape as in Fig. 1.2.

1.2.4 Maintenance, Maintainability

Maintenance defines the set of actions performed on the item to *retain* it in or to *restore* it to a specified state. Maintenance is thus subdivided into *preventive maintenance*, carried out at predetermined intervals to reduce wear out failures, and *corrective maintenance*, carried out after failure detection and intended to put the item into a state in which it can again perform the required function. Aim of a preventive maintenance is also to detect and repair *hidden failures*, i.e., failures in *redundant elements* not detected at their occurrence. Corrective maintenance is also known as *repair*, and can include any or all of the following steps: *detection*, *localization* (isolation), *correction*, *checkout*. *Repair* is used in this book as a synonym for *restoration*, by neglecting logistic and administrative delays. To simplify calculations, it is generally assumed that *the element in the reliability block diagram* for which a maintenance action has been performed is *as-good-as-new* after maintenance. This assumption is *valid for the whole equipment or system in the case of constant failure rate* for all elements which have not been repaired or replaced.

Maintainability is a *characteristic* of the item, expressed by the *probability* that a *preventive maintenance* or a *repair* of the item will be performed within a stated *time interval* for given *procedures and resources* (skill level of personnel, spare parts, test facilities, etc.). From a qualitative point of view, maintainability can be defined as the *ability of the item to be retained in or restored to a specified state*. The *mean* (expected value) of the repair time is denoted by *MTTR* (mean time to repair (restoration)), that of a preventive maintenance by *MTTPM*. Maintainability has to be *built into* complex equipment and systems *during design and development* by realizing a *maintenance concept*. Due to the increasing maintenance cost, maintainability aspects have grown in importance. However, maintainability achieved in the field largely depends on the resources available for maintenance (human and material), as well as on the correct installation of the equipment or system, i.e. on the *logistic support* and *accessibility*.

1.2.5 Logistic Support

Logistic support designates all actions undertaken to provide effective and economical use of the item during its operating phase. To be effective, logistic support should be integrated into the *maintenance concept* of the item under consideration and include after-sales service.

An emerging aspect related to maintenance and logistic support is that of *obsolescence management*, i.e., how to assure functionality over a long operating period (e. g. 20 years) *when technology is rapidly evolving* and components need for maintenance are no longer manufactured. Care has to be given here to *design aspects*, to assure *interchangeability* during the equipment's useful life without important redesign (standardization has been started [1.5, 1.11, A2.6 (IEC 62402)]).

1.2.6 Availability

Availability is a broad term, expressing the ratio of delivered to expected service. It is often designated by A and used for the stationary & steady-state value of the point and average availability ($PA = AA$). *Point availability* ($PA(t)$) is a characteristic of the item expressed by the *probability* that the item will perform its *required function* under *given conditions* at a stated *instant of time* t . From a qualitative point of view, *point availability* can be defined as the *ability of the item to perform its required function under given conditions at a stated instant of time (dependability)*.

Availability evaluations are often difficult, as *logistic support* and *human factors* should be considered in addition to reliability and maintainability. *Ideal* human and logistic support conditions are thus often assumed, yielding to the *intrinsic* (inherent) *availability*. In this book, *availability* is used as a synonym for *intrinsic availability*. Further assumptions for calculations are continuous operation and *complete renewal of the repaired element* in the reliability block diagram (assumed as-good-as-new after repair). For a given item, the point availability $PA(t)$ rapidly converges to a *stationary & steady-state value*, given by (Eq. (6.48))

$$PA = MTF / (MTF + MTTR) . \quad (1.10)$$

PA is also the stationary & steady-state value of the *average availability* (AA) giving the *mean* (expected value) of the *percentage of the time* during which the item performs its required function. PA_S and AA_S is used for considerations at system level. Other availability measures can be defined, e.g. *mission availability*, *work-mission availability*, *overall availability* (Sections 6.2.1.5, 6.8.2). Application specific figures are also known, see e.g. [6.12]. In contrast to reliability analyses for which *no failure at item (system) level* is allowed (only redundant parts can fail and be repaired on line), availability analyses *allow failures at item (system) level*.

1.2.7 Safety, Risk, and Risk Acceptance

Safety is the ability of the item not to cause injury to persons, nor significant material damage or other unacceptable consequences during its use. Safety evaluation must consider the following two aspects: Safety when the item functions and is operated correctly and safety when the item, or a part of it, has failed. The first aspect deals with *accident prevention*, for which a large number of national and international regulations exist. The second aspect is that of *technical safety* which is investigated in five steps (identify *potential hazards*, identify their *causes*, determine their *effect*, *classify* their effect as per Fig. 2.13, investigate possibilities to *avoid* the hazard or at least to *mitigate its effect*), using similar tools as for reliability. However, a distinction between technical safety and reliability is necessary. While safety assurance examines measures which allow the item to be brought into a *safe state* in the case of failure (*fail-safe behavior*), reliability assurance deals with measures for minimizing

the total number of failures. Moreover, for technical safety the effects of *external influences* like human errors, catastrophes, sabotage, etc. are of great importance and must be considered carefully. The safety level of the item influences the number of *product liability claims*. However, increasing in safety can reduce reliability.

Closely related to the concept of safety are those of *risk*, *risk management*, and *risk acceptance*; including risk analysis & assessment [1.3, 1.9, 1.21, 1.23, 1.26, 1.28]. Risk problems are often *interdisciplinary* and have to be solved in *close cooperation between engineers and sociologists* to find common solutions to controversial questions. An appropriate weighting between *probability of occurrence* and *effect* (consequence) of a given accident is important. The *multiplicative rule* is one among different possibilities. Also it is necessary to consider the different *causes* (machine, machine & human, human) and *effects* (location, time, involved people, effect duration) of an accident. Statistical tools can support *risk assessment*. However, although the behavior of a homogenous human population is often known, experience shows that the reaction of a *single person* can become unpredictable (see Section 6.10 for basic considerations on *human reliability*). Similar difficulties also arise in the evaluation of *rare events* in complex systems. Risk analyses are basically performed with tools used for failure modes and effect analysis (Section 2.6). However, for high-risk systems, refinements are often necessary, for instance, using the *risk priority number concept* with logarithmic scale [2.82].

Quite generally, considerations on risk and risk acceptance should take into account that the probability p_1 for a given accident which can be caused by one of n statistically identical and *independent* items, each of them with occurrence probability p , is for np small ($n \rightarrow \infty, p \rightarrow 0$) nearly equal to np as per

$$p_1 = np(1-p)^{n-1} \approx np e^{-np} \approx np(1-np) \approx np. \quad (1.11)$$

Equation (1.11) follows from the binomial distribution and the Poisson approximation (Eqs. (A6.120) & (A6.129)). It also applies with $np = \lambda_{tot} T$ to the case in which one assumes that the accident occurs randomly in the interval $(0, T]$, caused by one of n *independent* items (systems) with failure rates $\lambda_1, \dots, \lambda_n$, where $\lambda_{tot} = \lambda_1 + \dots + \lambda_n$. This is because the *sum of n independent Poisson processes is again a Poisson process* (Eq. (7.27)) and the probability $\lambda_{tot} T e^{-\lambda_{tot} T}$ for one failure in the interval $(0, T]$ is nearly equal to $\lambda_{tot} T$. Thus, for $np \ll 1$ or $\lambda_{tot} T \ll 1$ it holds that

$$p_1 \approx np \approx (\lambda_1 + \dots + \lambda_n) T. \quad (1.12)$$

Also by assuming a reduction of the individual occurrence probability p (or failure rate λ_i), one recognizes that in the future it will be necessary either to *accept greater risks* p_1 or to keep the spread of high-risk technologies under *tighter control*. Similar considerations apply to *environmental stresses* caused by mankind. Aspects of *ecologically acceptable* production, use, disposal, *recycling, reuse* of products should become subject for international regulations (*sustainable development*).

In the context of a *product development*, risks related to *feasibility* and *time to market* within the given cost constraints must also be considered during all development phases (*feasibility checks* in Fig. 1.6 and Tables A3.3 & 5.3).

Mandatory for *risk management* are psychological aspects related to *risk awareness* and *safety communication*. As long as a *danger for risk* is not perceived, people often do not react. Knowing that a *safety behavior* presupposes a risk awareness, *communication* is an important tool to avoid that the risk related to a given system will be underestimated, see e.g. [1.23, 1.26].

1.2.8 Quality

Quality is understood as the *degree to which a set of inherent characteristics fulfills requirements*. This definition, given now also in the ISO 9000: 2000 family [A1.6], follows closely the traditional definition of quality, expressed by *fitness for use*, and applies to products and services as well.

1.2.9 Cost and System Effectiveness

All previously introduced concepts are interrelated. Their relationship is best shown through the concept of cost effectiveness, as given in Fig. 1.3. *Cost effectiveness* is a measure of the ability of the item to meet a service demand of stated quantitative characteristics, with the best possible usefulness to life-cycle cost ratio. It is often referred also to as *system effectiveness*. Figure 1.3 deals essentially with technical and cost aspects. Some management aspects are considered in Appendices A2- A5. From Fig. 1.3, one recognizes the central role of *quality assurance*, bringing together all assurance activities (Section 1.3.3), and of *dependability* (collective term for availability performance and its influencing factors).

As shown in Fig. 1.3, *life-cycle cost* (LCC) is the sum of cost for acquisition, operation, maintenance, and disposal of the item. For complex systems, higher reliability leads in general to higher acquisition cost and lower operating cost, so that the optimum of life-cycle cost seldom lies at extremely low or high reliability figures. For such a system, per year operating & maintenance cost often exceeds 10% of acquisition cost, and experience shows that up to 80% of the life-cycle cost is frequently generated by decisions early in the design phase. To be complete, life-cycle cost should also take into account *current and deferred damage to the environment* caused by production, use, and disposal of the item. Life-cycle cost optimization falls within the framework of *cost effectiveness* or *systems engineering*. It can be positively influenced by *concurrent engineering* [1.16, 1.22]. Figure 1.4 shows an example of the influence of the attainment level of quality and reliability targets on the sum of cost of quality and operational availability assurance for two systems with different mission profiles [2.2 (1986)], see Example 1.1 for an introduction.

Example 1.1

An assembly contains n independent components each with a *defective probability* p . Let c_k be the cost to replace k defective components. Determine (i) the mean (expected value) $C_{(i)}$ of the total replacement cost (no defective components are allowed in the assembly) and (ii) the mean of the total cost (test and replacement) $C_{(ii)}$ if the components are submitted to an incoming inspection which reduces defective percentage from p to p_0 (test cost c_t per component).

Solution

- (i) The solution makes use of the *binomial distribution* (Appendix A6.10.7) and question (i) is also solved in Example A6.19. The probability of having exactly k defective components in a lot of size n is given by (Eq. (A6.120))

$$p_k = \binom{n}{k} p^k (1-p)^{n-k}. \quad (1.13)$$

The mean $C_{(i)}$ of the total cost (deferred cost) caused by the defective components follows then from the weighted sum

$$C_{(i)} = \sum_{k=1}^n c_k p_k = \sum_{k=1}^n c_k \binom{n}{k} p^k (1-p)^{n-k}. \quad (1.14)$$

- (ii) To the cost caused by the defective components, calculated from Eq. (1.14) with p_0 instead of p , one must add the incoming inspection cost nc_t

$$C_{(ii)} = nc_t + \sum_{k=1}^n c_k \binom{n}{k} p_0^k (1-p_0)^{n-k}. \quad (1.15)$$

The difference between $C_{(i)}$ and $C_{(ii)}$ gives the gain (or loss) obtained by introducing the incoming inspection, allowing thus a *cost optimization* (see also Section 8.4 for a deeper discussion).

Using Eq. (A7.42) instead of (A6.120), similar considerations to those in Example 1.1 yield for the *mean* (expected value) of the total repair cost C_{cm} during the cumulative operating time T of an item with failure rate λ and cost c_{cm} per repair

$$C_{cm} = \lambda T c_{cm} = \frac{T}{MTBF} c_{cm}. \quad (1.16)$$

(In Eq. (1.16), the term λT gives the mean value of the number of failures during T (Eq. (A7.42)), and $MTBF$ is used as $MTBF = 1/\lambda$.)

From the above considerations, the following equation expressing the *mean* C of the sum of the cost for quality assurance and for the assurance of reliability, maintainability, and logistic support of a system can be obtained

$$C = C_q + C_r + C_{cm} + C_{pm} + C_l + \frac{T}{MTBF_S} c_{cm} + (1-OA_S) T c_{off} + n_d c_d. \quad (1.17)$$

Thereby, q is used for quality, r for reliability, cm for corrective maintenance, pm for preventive maintenance, l for logistic support, off for down time & d for defects.

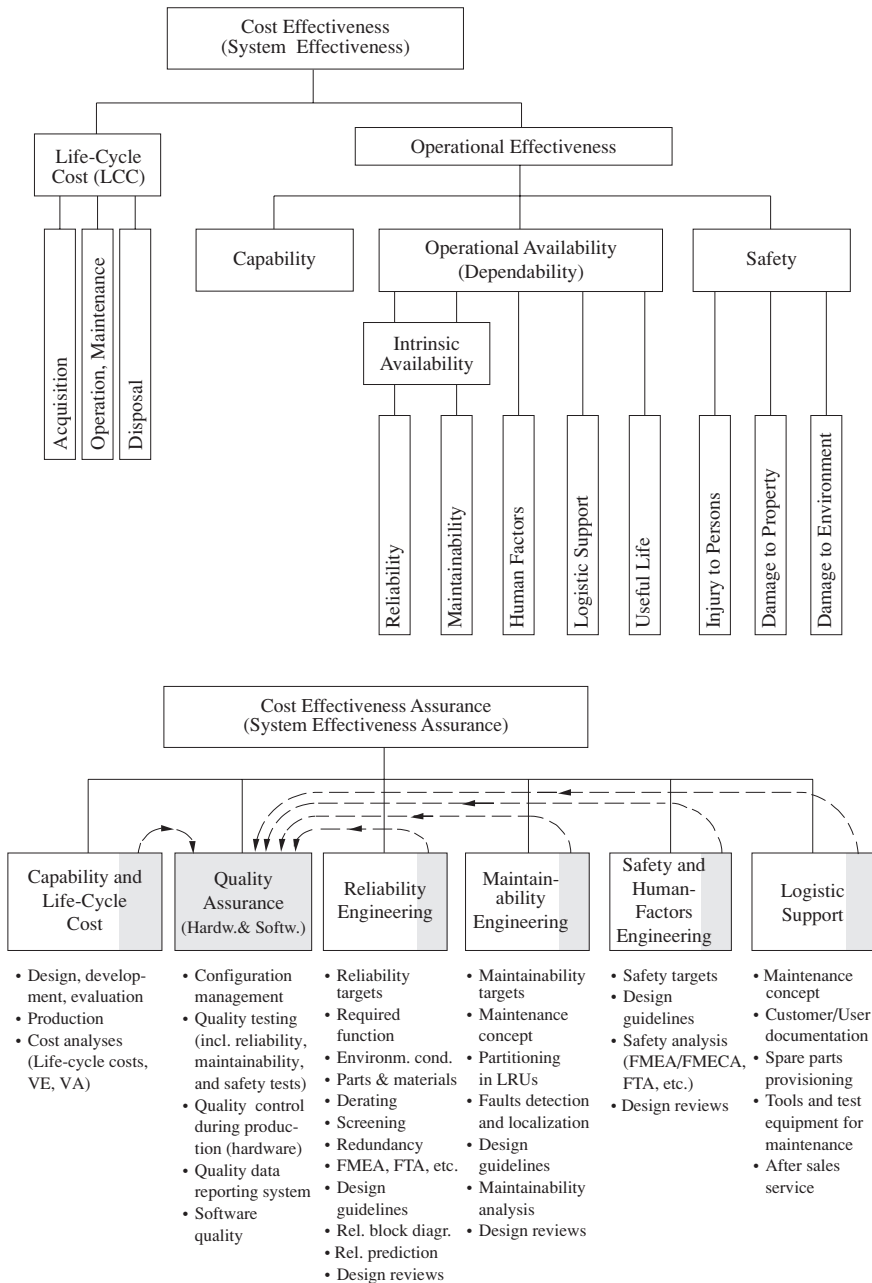


Figure 1.3 Cost Effectiveness (System Effectiveness) for *complex equipment & systems with high quality and reliability (RAMS) requirements* (see Appendices A1 - A5 for definitions & management aspects; dependability can be used instead of operational availability, for a qualitative meaning)

$MTBF_S$ and OA_S are the system mean operating time between failures (assumed here $= 1/\lambda_S$) and the system steady-state *overall availability* (Eq. (6.196) with T_{pm} instead of T_{PM}). T is the total system operating time (useful life) and n_d is the number of *hidden defects* discovered (and eliminated) in the field. C_q , C_r , C_{cm} , C_{pm} , and C_l are the cost for quality assurance and for the assurance of reliability, repairability, serviceability, and logistic support, respectively. c_{cm} , c_{off} , and c_d are the cost per repair, per hour down time, and per hidden defect, respectively (preventive maintenance cost are scheduled cost, considered here as a part of C_{pm}). The first five terms in Eq. (1.17) represent a part of the *acquisition cost*, the last three terms are *deferred cost* occurring during field operation. A model for investigating the cost C according to Eq. (1.17) was developed in [2.2 (1986)], by assuming C_q , C_r , C_{cm} , C_{pm} , C_l , $MTBF_S$, OA_S , T , c_{cm} , c_{off} , c_d , and n_d as parameters and investigating the variation of the total cost expressed by Eq. (1.17) as a function of the level of attainment of the specified targets, i.e., by introducing the variables $g_q = QA/QA_g$, $g_r = MTBF_S / MTBF_{Sg}$, $g_{cm} = MTTR_{Sg} / MTTR_S$, $g_{pm} = MTTPM_{Sg} / MTTPM_S$, and $g_l = MLD_{Sg} / MLD_S$, where the subscript g denotes the specified target for the corresponding quantity. A power relationship

$$C_i = C_{ig} g_i^{m_i} \quad (1.18)$$

was assumed between the actual cost C_i , the cost C_{ig} to reach the specified target (goal) of the considered quantity, and the *level of attainment* of the specified target ($0 < m_i < 1$ and all other $m_i > 1$). The following relationship between the number of hidden defects discovered in the field and the ratio C_q / C_{qg} was also included in the model

$$n_d = \frac{1}{(C_q / C_{qg})^{m_d}} - 1 = \frac{1}{g_q^{m_d}} - 1. \quad (1.19)$$

The final equation for the cost C as function of the variables g_q , g_r , g_{cm} , g_{pm} , and g_l follows then as (using Eq. (6.196) for OA_S)

$$C = C_{qg} g_q^{m_q} + C_{rg} g_r^{m_r} + C_{cmg} g_{cm}^{m_{cm}} + C_{pmg} g_{pm}^{m_{pm}} + C_{lg} g_l^{m_l} + \frac{T c_{cm}}{g_r MTBF_{Sg}} + \left(1 - \frac{1}{1 + \frac{1}{g_r g_{cm}} \cdot \frac{MTTR_{Sg}}{MTBF_{Sg}} + \frac{1}{g_r g_l} \cdot \frac{MLD_{Sg}}{MTBF_{Sg}} + \frac{MTTPM_{Sg}}{g_{pm} T_{pm}}}\right) T c_{off} + \left(\frac{1}{g_q^{m_d}} - 1\right) c_d. \quad (1.20)$$

The relative cost C / C_g given in Fig. 1.4 is obtained by dividing C by the value C_g from Eq. (1.20) with all $g_i = 1$. Extensive analyses with different values for m_i , C_{ig} , $MTBF_{Sg}$, $MTTR_{Sg}$, MLD_{Sg} , $MTTPM_{Sg}$, T_{pm} , T , c_{cm} , c_{off} , and c_d have shown that the value C / C_g is only moderately sensitive to the parameters m_i .

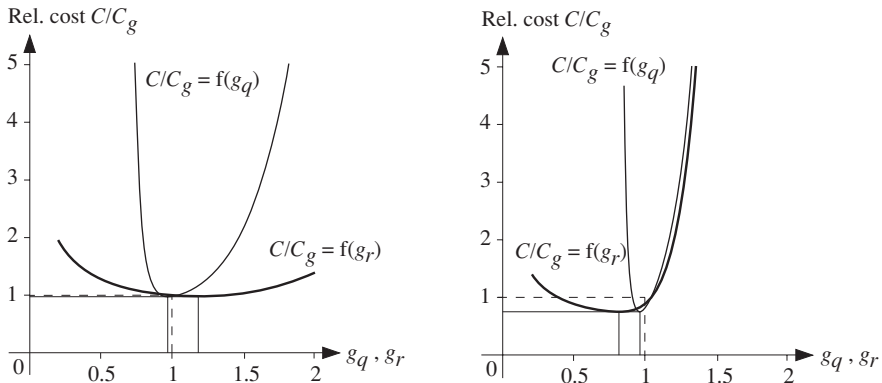


Figure 1.4 Basic shape of the relative cost C/C_g per Eq. (1.20) as function of $g_q = QA/QA_g$ and $g_r = MTBF_S / MTBF_{Sg}$ (quality assurance and reliability assurance as in Fig. 1.3) for two complex systems with different mission profiles (the specified targets $g_q = 1$ and $g_r = 1$ are dashed)

1.2.10 Product Liability

Product liability is the onus on a manufacturer (producer) or others to compensate for losses related to injury to persons, material damage, or other unacceptable consequences caused by a product (item). The manufacturer *has to specify a safe operational mode* for the product (user documentation). In legal documents related to product liability, the term *product* often indicates *hardware* only and the term *defective product* is in general used instead of *defective* or *failed product*. Responsible in a product liability claim are all those people involved in the design, production, sale, and maintenance of the product (item), inclusive suppliers. Often, *strict liability* is applied (the manufacturer has to demonstrate that the product was free from defects). This holds in the USA and increasingly in Europe [1.10]. However, in Europe the causality between damage and defect has still to be demonstrated by the user (see p. 382 for further considerations).

The rapid increase of product liability claims (alone in the USA, 50,000 in 1970 and over one million in 1990) cannot be ignored by manufacturers. Although such a situation has probably been influenced by the peculiarity of US legal procedures, *configuration management* and *safety analysis* (in particular *causes-to-effects* analysis, i. e., FMEA/FMECA or FTA as introduced in Section 2.6) as well as considerations on risk management should be performed to *increase safety* and avoid product liability claims (see Sections 1.2.7, 2.6 & 6.10, and Appendix A.3.3).

1.2.11 Historical Development

Methods and procedures of quality assurance and reliability engineering have been developed extensively over the last 60 years. For indicative purpose, Table 1.1 summarizes major steps of this development and Fig. 1.5 shows the approximate distribution of the effort between quality assurance and reliability engineering during the same period of time. Because of the rapid progress of microelectronics, considerations on *redundancy*, *fault-tolerance*, *test strategy*, and *software quality* gains in importance. A skillful, allegorical presentation of the *story of reliability* is in [1.25].

Table 1.1 Historical development of quality assurance (management) and reliability engineering

before 1940	Quality attributes and characteristics are defined. In-process and final tests are carried out, usually in a department within the production area. The concept of <i>quality of manufacture</i> is introduced.
1940 - 50	Defects and failures are systematically collected and analyzed. <i>Corrective actions</i> are carried out. <i>Statistical quality control</i> is developed. It is recognized that quality must be <i>built into</i> an item. The concept <i>quality of design</i> becomes important.
1950 - 60	<i>Quality assurance</i> is recognized as a means for developing and manufacturing an item with a specified quality level. <i>Preventive measures</i> (actions) are added to tests and corrective actions. It is recognized that correct short-term functioning does not also signify <i>reliability</i> . <i>Design reviews</i> and systematic analysis of failures (failure data and failure mechanisms), performed often in the research & development area, lead to important reliability improvements.
1960 - 70	Difficulties with respect to reproducibility and change control, as well as interfacing problems during the integration phase, require a refinement of the concept of <i>configuration management</i> . Reliability engineering is recognized as a means of developing and manufacturing an item with specified reliability. <i>Reliability estimation methods and demonstration tests</i> are developed. It is recognized that reliability cannot easily be demonstrated by an <i>acceptance test</i> . Instead of a reliability figure (λ or $MTBF=1/\lambda$), contractual requirements are for a <i>reliability assurance program</i> . <i>Maintainability, availability, and logistic support</i> become important.
1970 - 80	Due to the increasing complexity and cost for maintenance of equipment and systems, the aspects of <i>man-machine interface</i> and <i>life-cycle cost</i> become important. Customers require demonstration of reliability and maintainability during the warranty period. Quality and reliability assurance activities are made <i>project specific</i> and carried out in <i>close cooperation</i> with all engineers involved in a project. Concepts like <i>product assurance, cost effectiveness</i> and <i>systems engineering</i> are introduced. <i>Human reliability</i> and <i>product liability</i> become important.
1980 - 90	<i>Testability</i> is required. <i>Test and screening strategies</i> are developed to reduce testing cost and warranty services. Because of the rapid progress in microelectronics, greater possibilities are available for <i>redundant and fault tolerant structures</i> . <i>Software quality</i> becomes important.
after 1990	The necessity to further shorten the development time leads to the concept of <i>concurrent engineering</i> . <i>Total Quality Management (TQM)</i> appears as a refinement to quality assurance as used at the end of the seventies. <i>RAMS</i> is used for <i>reliability, availability, maintainability & safety, reliability engineering</i> for <i>RAMS engineering</i> .

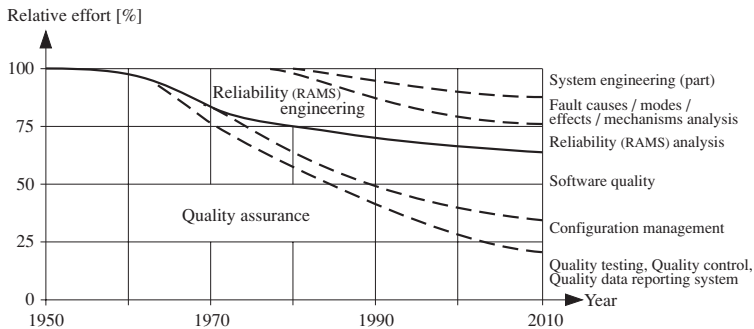


Figure 1.5 Approximate distribution of the effort between quality assurance and reliability (RAMS) engineering for *complex equipment & systems with high quality and reliability (RAMS) requirements*

1.3 Basic Tasks & Rules for Quality and Reliability (RAMS) Assurance of Complex Equip. & Systems

This section deals with some important considerations on the organization of quality and reliability assurance in the case of *complex repairable equipment and systems with high quality and reliability requirements*. In this context, the term *reliability* appears for *reliability, availability, maintainability, and safety* (RAMS). This minor part of the book aims to support managers in answering the question of *how to specify and realize high reliability (RAMS) targets for equipment and systems*. Refinements are in Appendix A3 for complex equipment and systems *for which tailoring is not mandatory*, with considerations on *quality management* and *total quality management* (TQM) as well. As a general rule, quality assurance and reliability (RAMS) engineering must avoid bureaucracy, be integrated in project activities, and support *quality management* and *concurrent engineering* efforts, as per *TQM*.

1.3.1 Quality and Reliability (RAMS) Assurance Tasks

Experience shows that besides the prevention of defects and systematic failures, *which remains the primary task of a quality assurance system,*

the development and production of complex repairable equipment and systems with high reliability (RAMS) targets requires *specific activities* during all life-cycle phases of the item considered. Figure 1.6 shows the *life-cycle phases* and Table 1.2 gives the *main tasks* for quality and reliability (RAMS) assurance. Depicted in Table 1.2 is also the period of time over which the tasks have to be performed. Within a project, the tasks of Table 1.2 must be refined in a project-specific quality and reliability (RAMS) *assurance program* (Appendix A3).

Table 1.2 Main tasks for quality and reliability (RAMS) assurance of *complex equipment & systems with high quality and reliability requirements* (the bar height is a measure of the relative effort)

Main tasks for quality and reliability (RAMS) assurance of <i>complex equipment and systems</i> , conforming to TQM (see Table A3.2 for greater details and a possible task assignment; software quality appears in tasks 4, 8-11, 14-16, see also Section 5.3)	Project-independent	Specific during					
		Conception	Definition	Design & Devel.	Evaluation	Production	Use
1. Customer and market requirements	■	■	■	■	■	■	■
2. Preliminary analyses		■	■	■	■	■	
3. Quality and reliability aspects in specs, quotations, contracts, etc.		■	■	■	■	■	
4. Quality and reliability (RAMS) assurance		■	■	■	■	■	
5. Reliability and maintainability analyses			■	■	■	■	■
6. Safety and human factor analyses			■	■	■	■	■
7. Selection and qualification of components and materials			■	■	■	■	
8. Supplier selection and qualification			■	■	■	■	
9. Project-dependent procedures and work instructions			■	■	■	■	
10. Configuration management		■	■	■	■	■	■
11. Prototype qualification tests			■	■	■	■	
12. Quality control during production				■	■	■	
13. In-process tests				■	■	■	
14. Final and acceptance tests		■	■	■	■	■	■
15. Quality data reporting system					■	■	■
16. Logistic support		■	■	■	■	■	■
17. Coordination and monitoring	■	■	■	■	■	■	■
18. Quality costs	■	■	■	■	■	■	■
19. Concepts, methods, and general procedures (quality and reliability)	■		■	■	■	■	
20. Motivation and training	■		■	■	■	■	

Conception, Definition, Design, Development, Evaluation		Production (Manufacturing)		Use	Disposal, Recycling
Preliminary study, Conception	Definition, Design, Full development, Prototype qualification	Pilot production	Series production	Installation, Operation	
<ul style="list-style-type: none"> • Idea, market requirements • Evaluation of delivered equipment and systems • Proposal for preliminary study 	<ul style="list-style-type: none"> • Feasibility check • System specifications • Interface definition • Proposal for the design phase 	<ul style="list-style-type: none"> • Feasibility check • Revised system specifications • Qualified and released prototypes • Technical documentation • Proposal for pilot production 	<ul style="list-style-type: none"> • Feasibility check • Production documentation • Qualified production processes • Qualified and released first series item • Proposal for series production 	<ul style="list-style-type: none"> • Series item • Customer documentation • Logistical support concept • Spare part provisioning 	

Figure 1.6 Basic life-cycle phases of *complex equipment and systems* (the output of a given phase is the input to the next phase), see Tab. 5.3 (p. 161) for software

1.3.2 Basic Quality and Reliability (RAMS) Assurance Rules

Performance, dependability, cost, and time to market are key factors for today's products and services. Taking care of the considerations in Section 1.3.1, the *basic rules* for a quality and reliability (RAMS) assurance optimized by considering cost and time schedule aspects (conforming to *TQM*) can be summarized as follows:

1. Quality and reliability (RAMS) targets should be just as high as necessary to satisfy real customer needs
 → *Apply the rule "as-good-as-necessary".*
2. Activities for quality & reliability (RAMS) assurance should be performed continuously throughout *all project phases*, from definition to operating phase
 → *Do not change the project manager before ending the pilot production.*
3. Activities must be performed in close cooperation between all engineers involved in the project (Table A3.2)
 → *Use TQM and concurrent engineering approaches.*
4. Quality and reliability (RAMS) assurance activities should be monitored by a central quality & reliability assurance department (Q & RA), which cooperates *actively* in all project phases (Fig. 1.7 and Table A3.2)
 → *Establish an efficient and independent quality & reliability assurance department (Q & RA) active in the projects.*

Figure 1.7 shows a basic organization which could embody the above rules and satisfy requirements of *quality management standards* (Appendix A2). As shown in Table A3.2, the assignment of quality and reliability (RAMS) assurance tasks should be such, that every engineer in a project *bears his/her own responsibilities* (as per *TQM*). A design engineer should for instance be responsible for all aspects of his/her own product (e.g. an assembly) including reliability, maintainability and safety, and the production department should be able to manufacture and test such an item within its own competence. The *quality & reliability (RAMS) assurance department* (Q & RA in Fig. 1.7) can be for instance responsible for (see also Tab. A3.2)

- setting targets for quality and reliability (RAMS) levels,
- preparation of guidelines and working documents (quality and reliability (RAMS) aspects),
- coordination of the activities belonging to quality and reliability (RAMS) assurance,
- reliability (RAMS) analyses at system level,
- qualification, testing, and screening of components and material (quality and reliability aspects),
- release of manufacturing processes (quality and reliability (RAMS) aspects),
- development and operation of the quality data reporting system,
- acceptance testing (with customers).

This central quality and reliability (RAMS) department should not be too small (credibility) nor too large (sluggishness).

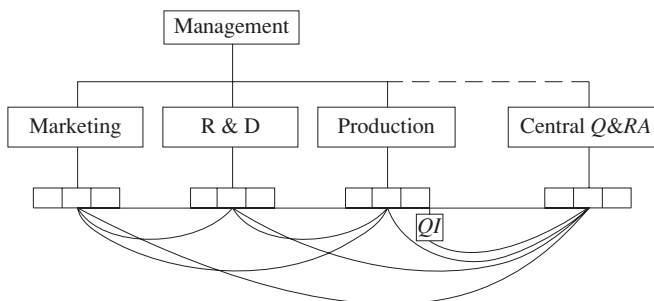


Figure 1.7 Basic organizational structure for quality and reliability (RAMS) assurance in a company producing *complex equipment and systems with high quality and reliability (RAMS) requirements* (connecting lines indicate close cooperation; A denotes assurance, I inspection, Q quality, R reliability (RAMS))

1.3.3 Elements of a Quality Assurance System

As stated in Sections 1.3.1, many of the tasks associated with *quality assurance* (in the sense of *quality management* as per *TQM*) are *interdisciplinary*. In order to have a minimum impact on cost and time schedules, their solution requires the *concurrent efforts (close cooperation) of all engineers involved in a project*. To improve coordination, it is useful to group the quality assurance activities (see also Fig. 1.3 and Appendix A3.3):

1. *Configuration Management*: Procedure used to specify, describe, audit & release the configuration of the item, as well as to control it during modifications or changes. Configuration management is an important tool for quality assurance. It can be subdivided into configuration *identification, auditing (design reviews), control, and accounting* (Appendix A3.3.6).
2. *Quality Tests*: Tests to verify whether the item conforms to specified requirements. Quality tests include incoming inspections, as well as qualification tests, production tests, and acceptance tests. They also cover reliability, maintainability, safety, and software aspects. To be cost effective, quality tests must be coordinated and integrated into a *test strategy*.
3. *Quality Control During Production*: Control (monitoring) of the production processes and procedures to reach a stated quality of manufacturing.
4. *Quality Data Reporting System (FRACAS)*: A system to collect, analyze & correct all defects and failures (faults) occurring during the production and test of the item, as well as to evaluate and feedback the corresponding quality and reliability (RAMS) data. Such a system is generally computer-aided. Analysis of failures and defects must be traced to the *cause*, to *avoid repetition* of the same problem, and be pursued at least during the warranty period (Fig. 1.8).
5. *Software quality*: Procedures and tools to specify, develop, and test software (appears in tasks 4, 8-11,14-16 of Tables 1.2 & A3.2, see also Section 5.3).

Configuration management spans from the definition up to the operating phase (Appendices A3 & A4). Quality tests encompasses technical and statistical aspects (Chapters 3, 7, and 8). The concept of a quality data reporting system is depicted in Fig. 1.8 (see Appendix A5 for basic requirements). Table 1.3 shows an example of data reporting sheets for PCBs evaluation.

The quality and reliability (RAMS) assurance system must be described in an appropriate *quality handbook* supported by the company management. A possible content of such a handbook for a company producing *complex equipment and systems with high quality & reliability (RAMS) requirements* is: •General, •Project Organization, •Quality Assurance (Management) system, •Quality & Reliability (RAMS) Assurance Program, •Reliability Engineering, •Maintainability Eng., •Safety & Human Eng., •Software Quality Assurance, •Logistic Support, •Motivation & Training.

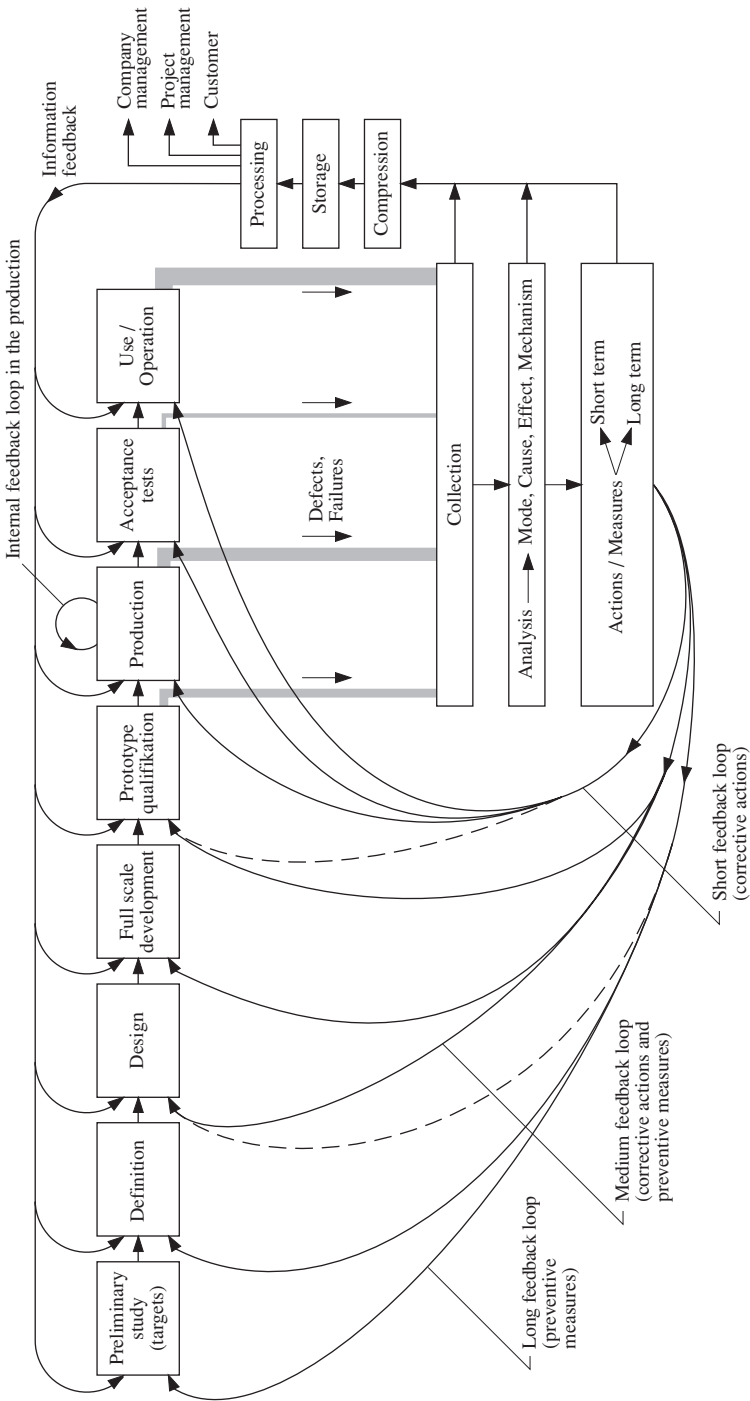


Figure 1.8 Basic concept for a quality data reporting system

1.3.4 Motivation and Training

Cost effective quality and reliability (RAMS) assurance / management can be achieved if every engineer involved in a project is made responsible for his / her assigned activities (e.g. as per Table A3.2). Figure 1.9 shows a comprehensive, practice oriented, *motivation and training* program in a company producing *complex equipment and systems with high quality and reliability (RAMS) requirements*.

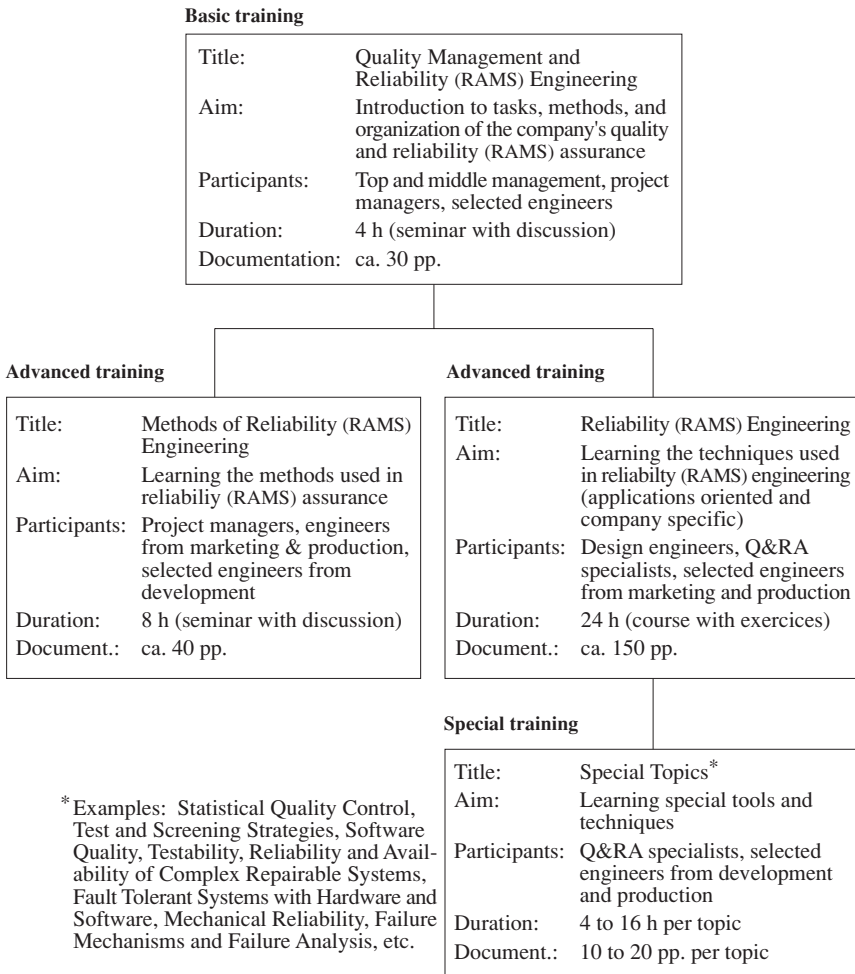


Figure 1.9 Example for a practical oriented training and motivation program in a company producing *complex equipment and systems with high quality and reliability (RAMS) requirements*

2 Reliability Analysis During the Design Phase (Nonrepairable Elements up to System Failure)

Reliability analysis during the design and development of complex components, equipment, and systems is important to detect and eliminate *reliability weaknesses* as early as possible and to perform *comparative studies*. Such an investigation includes *failure rate* and *failure mode* analysis, verification of the adherence to *design guidelines*, and cooperation in *design reviews*. This chapter presents methods and tools for failure rate and failure mode analysis of complex equipment and systems considered as *nonrepairable* up to system failure (except for Eq. (2.48)). After a short introduction, Section 2.2 deals with series - parallel structures. Complex structures, elements with more than one failure mode, and parallel models with *load sharing* are investigated in Section 2.3. Reliability allocation with cost considerations are discussed in Section 2.4, stress / strength and drift analysis in Section 2.5. Section 2.6 deals with failure mode and causes-to-effects analyses. Section 2.7 gives a checklist for reliability aspects in design reviews. Maintainability is considered in Chapter 4 and repairable systems are investigated in Chapter 6 (including complex systems for which a reliability block diagram does not exist, imperfect switching, incomplete coverage, reconfigurable systems, common cause failures, as well as an introduction to network reliability, BDD, ET, dynamic FT, Petri nets, and computer-aided analysis). Design guidelines are in Chapter 5, qualification tests in Chapter 3, reliability tests in Chapters 7 & 8. Theoretical foundations for this chapter are in Appendix A6.

2.1 Introduction

An important part of the reliability analysis during the design and development of complex equipment and systems deals with failure rate and failure mode investigation as well as with the verification of the adherence to appropriate design guidelines for reliability. *Failure modes* and *causes-to-effects* analysis is considered in Section 2.6, *design guidelines* are given in Chapter 5. Sections 2.2- 2.5 are devoted to *failure rate analysis*.

Investigating the failure rate of a complex equipment or system leads to the calculation of the *predicted reliability*, i.e., that reliability which can be calculated from the structure of the item and the reliability of its elements. Such a prediction is necessary for an *early detection of reliability weaknesses*, for *comparative studies*, for *availability* investigation taking care of *maintainability* and *logistic support*, and for the definition of *quantitative reliability targets* for designers and subcontractors. However, because of different kind of uncertainties, the predicted reliability can often be only given with a limited accuracy. To these uncertainties belong

- simplifications in the mathematical modeling (independent elements, complete and sudden failures, no flaws during design and manufacturing, no damages),
- insufficient consideration of faults caused by internal or external interference (switching, transients, EMC, etc.),
- inaccuracies in the data used for the calculation of the component failure rates.

On the other hand, the *true reliability* of an item can only be determined by *reliability tests*, performed often at the prototype's qualification tests, i.e., late in the design and development phase. Practical applications also shown that with an experienced reliability engineer, the predicted failure rate at equipment or system level often agree *reasonably well* (within a factor of 2) with field data. Moreover, relative values obtained by comparative studies generally have a much greater accuracy than absolute values. All these reasons support the efforts for a *reliability prediction* during the design of equipment and systems with specified reliability targets.

Besides theoretical considerations, discussed in the following sections, *practical aspects* have to be considered when designing reliable equipment and systems, for instance with respect to operating conditions and to the mutual influence between elements (input/output, load sharing, effects of failures, transients, etc.). Concrete possibilities for reliability improvement are

- reduction of thermal, electrical and mechanical stresses,
- correct interfacing of components and materials,
- simplification of design and construction,
- use of qualitatively better components and materials,
- protection against ESD and EMC,
- screening of critical components and assemblies,
- use of redundancy,

in that order. *Design guidelines* (Chapter 5) and *design reviews* (Tables A3.3, 2.8, 4.3, and 5.5, Appendix A4) are mandatory to support such improvements. This chapter deals with *nonrepairable* (up to system failure) equipment and systems. Maintainability is discussed in Chapter 4. Reliability and availability of repairable equipment and systems is considered carefully in Chapter 6.

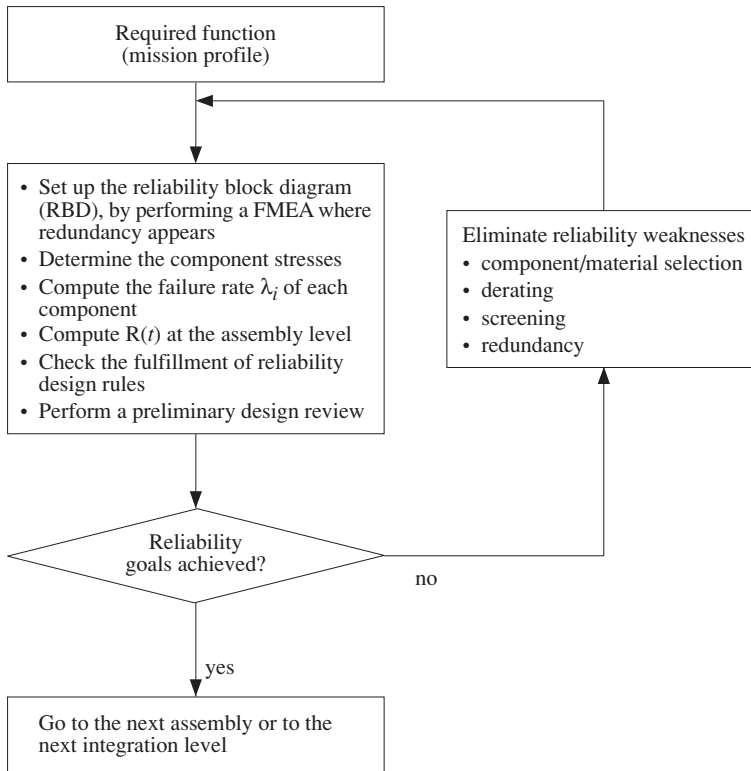


Figure 2.1 Reliability analysis procedure at assembly level

Taking account of the above considerations, Fig. 2.1 shows the reliability analysis procedure used in practical applications at assembly level. The procedure of Fig. 2.1 is based on the *part stress method* discussed in Section 2.2.4 (see Section 2.2.7 for the *part count method*). Also included are a failure modes and effects analysis (FMEA/ FMECA), to check the validity of the assumed *failure modes*, and a verification of the adherence to *design guidelines for reliability in a preliminary design review* (Section 5.1, Appendices A3.3.5 & A4). Verification of the assumed failure modes is *mandatory where redundancy appears*, in particular because of the *series element* in the reliability block diagram (see for instance Example 2.6, Sections 2.3.6 for elements with more than one failure mode & 6.8.7 for common cause failures, and Figs. 2.8- 2.9 & 6.17- 6.18 for a comparative investigation). To simplify the notation, in Chapters 2 and 6 *reliability* will be used for *predicted reliability* and *system* for *technical system* (i. e., for a system with ideal human factors and logistic support).

2.2 Predicted Reliability of Equipment and Systems with Simple Structure

Simple structures are those for which a reliability block diagram *exists* and can be reduced to a *series/parallel form* with *independent* elements. For such an item, the *predicted reliability* is calculated according to following procedure (Fig. 2.1):

1. Definition of the required function and of its associated mission profile.
2. Derivation of the corresponding reliability block diagram (RBD).
3. Determination of the operating conditions for each element of the RBD.
4. Determination of the failure rate for each element of the RBD.
5. Calculation of the reliability for each element of the RBD.
6. Calculation of the item (system) reliability function $R_S(t)$.
7. Performance of a preliminary design review.
8. Elimination of reliability weaknesses and return to step 1 or 2, as necessary.

This section discusses at some length steps 1 to 6, see Example 2.6 for the application to a simple situation. For the investigation of equipment and systems for which a reliability block diagram does not exist, one refers to Section 6.8.

2.2.1 Required Function

The *required function* specifies the item's (system's) task. Its definition is the starting point for any analysis, as it defines failures. For practical purposes, parameters should be defined with tolerances and not merely as fixed values.

In addition to the required function, *environmental conditions* at system level must also be defined. Among these, ambient temperature (e. g. +40°C), storage temperature (e. g. -20 to +60°C), humidity (e. g. 40 to 60%), dust, corrosive atmosphere, vibrations (e. g. 0.5 g_n , at 2 to 60 Hz), shocks, noise (e. g. 40 to 70 dB), and power supply voltage variations (e. g. $\pm 20\%$). From these global environmental conditions, the constructive characteristics of the system, and the internal loads, *operating conditions* (actual stresses) for each element of the system can be determined.

Required function and environmental conditions are often *time dependent*, leading to a *mission profile* (*operational profile* for software). A representative mission profile and the corresponding reliability targets should be defined in the system specifications (initially as a rough description and then refined step by step), see the remark on p. 38, as well as Section 6.8.6.2 for phased-mission systems.

2.2.2 Reliability Block Diagram

The *reliability block diagram* (RBD) is an *event diagram*. It answers the following question: *Which elements of the item under consideration are necessary for the*

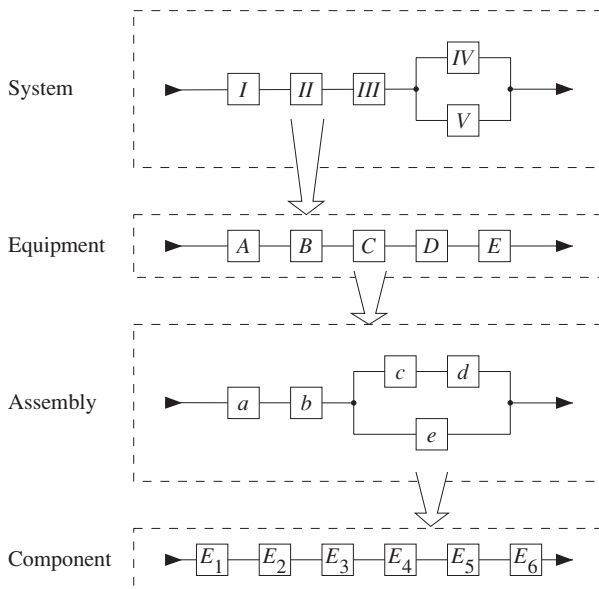


Figure 2.2 Procedure for setting up the *reliability block diagram* (RBD) of a system with four levels

fulfillment of the required function and which can fail without affecting it? Setting up a RBD involves, at first, *partitioning* the item into elements with clearly defined tasks. The elements which are necessary for the required function are connected *in series*, while elements which can fail with no effect on the required function (redundancy) are connected *in parallel*. Obviously, the ordering of the series elements in the reliability block diagram can be arbitrary. Elements which are not relevant for (or used in) the required function under consideration are removed (put into a reference list), *after having verified* (FMEA) that their failure does not affect elements involved in the required function. These considerations make it clear that for a given system, *each required function has its own reliability block diagram*.

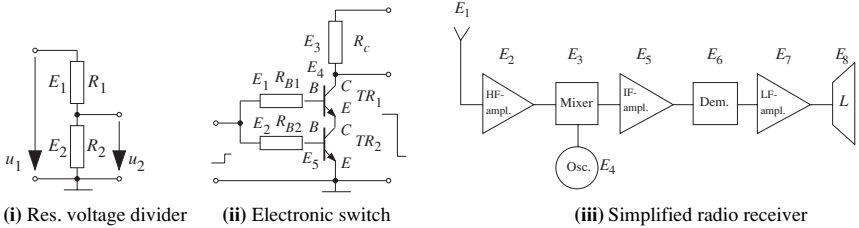
In setting up the reliability block diagram, care must be taken regarding the fact that only *two states* (good or failed) and *one failure mode* (e.g. opens or shorts) can be considered *for each element*. Particular attention must also be paid to the correct identification of the parts which appear *in series with a redundancy* (see e.g. Section 6.8). For large equipment and systems the reliability block diagram is derived top down as indicated in Fig. 2.2 (for 4 levels as an example). At each level, the corresponding required function is derived from that at the next higher level.

The technique of setting up reliability block diagrams is shown in the Examples 2.1 to 2.3 (see also Examples 2.6, 2.13, 2.14). One recognizes that a reliability block diagram basically differs from a *functional block diagram*. Examples 2.2, 2.3, 2.14 also show that one or more elements can appear *more than once* in a reliability

block diagram, while the corresponding element is physically present *only once* in the item considered. To point out the *strong dependence* created by this fact, it is mandatory to use a *box form other than a square* for these elements (in Example 2.2, if E_2 fails the required function for mission 1 & 2 is fulfilled *only* if E_1, E_3, E_5 work). To avoid ambiguities, each physically different element of the item should bear its own number. The typical structures of reliability block diagrams are summarized in Table 2.1 (see Sect. 6.8 for cases in which a reliability block diagram does not exist).

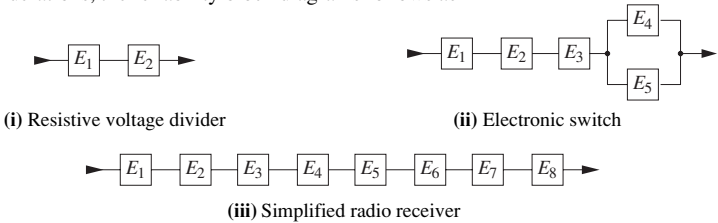
Example 2.1

Set up the reliability block diagrams for the following circuits:



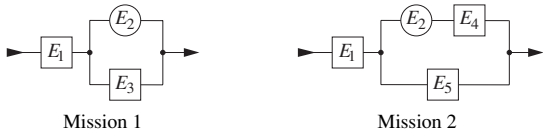
Solution

Cases (i) and (iii) exhibit no redundancy, i.e., for the required function (tacitly assumed here) all elements must work. In case (ii), transistors TR_1 and TR_2 are redundant if their failure mode is a *short* between emitter and collector (the failure mode for resistors is generally an open). From these considerations, the reliability block diagrams follows as



Example 2.2

An item is used for two different missions with the corresponding reliability block diagrams given in the figures below. Give the reliability block diagram for the case in which both functions are simultaneously required in a common mission.



Solution

The simultaneous fulfillment of both required functions leads to the *series connection* of both reliability block diagrams. Simplification is possible for element E_1 but not for element E_2 . A deeper discussion on phased-mission reliability analysis is in Section 6.8.6.2.

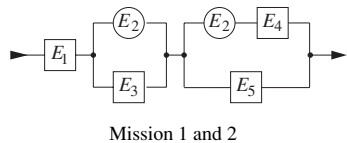
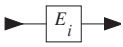
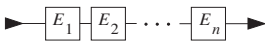
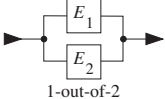
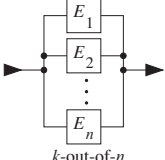
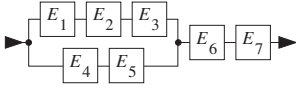
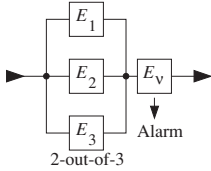
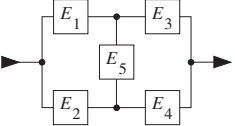
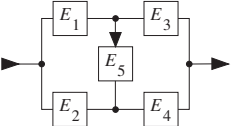
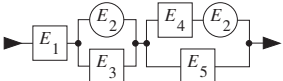
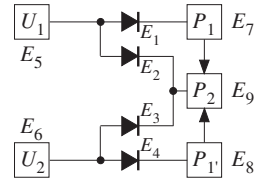


Table 2.1 Basic reliability block diagrams and associated reliability functions (nonrepairable up to system failure, new at $t=0$ ($R_{S0}(0)=1$), independent elements (except E_2 in 9), active redundancy, ideal failure detection & switch; 7-9 complex structures, can't be reduced to a series-parallel structure)

Reliability Block Diagram	Reliability Function ($R_S = R_{S0}(t)$; $R_i = R_i(t)$, $R_i(0)=1$)	Remarks
1 	$R_S = R_i$	One -item structure, $\lambda(t)=\lambda \Rightarrow R_i(t) = e^{-\lambda_i t}$
2 	$R_S = \prod_{i=1}^n R_i$	Series structure, $\lambda_S(t) = \lambda_1(t) + \dots + \lambda_n(t)$
3  1-out-of-2	$R_S = R_1 + R_2 - R_1 R_2$	1-out-of-2 redundancy, $R_1(t)=R_2(t) = e^{-\lambda t}$ $\Rightarrow R_S(t) = 2 e^{-\lambda t} - e^{-2\lambda t}$
4  k-out-of-n	$E_1 = \dots = E_n = E$ $\rightarrow R_1 = \dots = R_n = R$ $R_S = \sum_{i=k}^n \binom{n}{i} R^i (1-R)^{n-i}$	k-out-of-n redundancy for $k = 1$ $\Rightarrow R_S = 1 - (1-R)^n$ see p. 44 for $E_1 \neq \dots \neq E_n$
5 	$R_S = (R_1 R_2 R_3 + R_4 R_5 - R_1 R_2 R_3 R_4 R_5) R_6 R_7$	Series - parallel structure
6  2-out-of-3 Alarm	$E_1 = E_2 = E_3 = E$ $\rightarrow R_1 = R_2 = R_3 = R$ $R_S = (3 R^2 - 2 R^3) R_v$	Majority redundancy, general case (n + 1) - out - of - (2n + 1), n = 1, 2, ...
7 	$R_S = R_5 (R_1 + R_2 - R_1 R_2) \cdot (R_3 + R_4 - R_3 R_4) + (1 - R_5) \cdot (R_1 R_3 + R_2 R_4 - R_1 R_2 R_3 R_4)$	Bridge structure (bi-directional on E_5)
8 	$R_S = R_4 [R_2 + R_1 (R_3 + R_5 - R_3 R_5) - R_1 R_2 (R_3 + R_5 - R_3 R_5)] + (1 - R_4) R_1 R_3$	Bridge structure (unidirectional on E_5)
9 	$R_S = R_2 R_1 (R_4 + R_5 - R_4 R_5) + (1 - R_2) R_1 R_3 R_5$	The element E_2 appears twice in the reliability block diagram (not in the hardware)

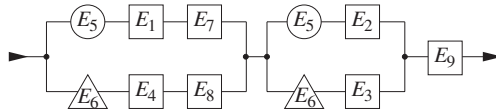
Example 2.3

Set up the reliability block diagram for the electronic circuit shown on the right. The required function asks for operation of P_2 (main assembly) and of P_1 or P_1' (control cards); E_1 to E_4 protect shorts at the input of P_1 and P_1' .



Solution

This example is not as trivial as Examples 2.1 and 2.2. A good way to derive the reliability block diagram is to consider the mission " P_1 or P_1' must work" and " P_2 must work" separately, and then to put both missions together as in Example 2.2 (see e. g. also Example 2.14 on pp. 68-69).



Also given in Table 2.1 are the associated reliability functions for the case of *non-repairable systems* (up to system failure) with *active redundancy* and *independent elements* except case 9 (Sections 2.2.5, 2.2.6, 2.3.1); see Section 2.3.5 for load sharing, Section 2.5 for mechanical systems, and Chapter 6 for repairable systems.

Table 2.2 Most important parameters influencing the failure rate of electronic components

Component	Ambient temp. (θ_A)	Junction temp. (θ_J)	Power stress (S)	Voltage stress (S)	Current stress (S)	Breakdown voltage	Technology	Complexity	Package	Application	Contact construction	Range	Production maturity	Environment (π_E)	Quality (π_Q)
Digital and linear ICs		D		x	x	x	x	x	x				x	x	x
Hybrid circuits	D	D	D	D	D	x	x	x	x	x	x	x	x	x	x
Bipolar transistors		D	D	x		x	x		x	x	x	x	x	x	x
FETs		D	D	x		x	x		x	x	x		x	x	x
Diodes		D	x	x	x	x	x		x	x	x	x	x	x	x
Thyristors		D	x	x	x	x	x		x		x	x	x	x	x
Optoelectronic components		D		x	x		x	x	x				x	x	x
Resistors	D		D				x					x	x	x	x
Capacitors	D			D			x		x	D		x	x	x	x
Coils, transformers	D		x	x			x						x	x	x
Relays, switches	D			x	x		x	x	x	x	D		x	x	x
Connectors	D				x		x		x	x	D	x	x	x	x

D denotes dominant, x denotes important

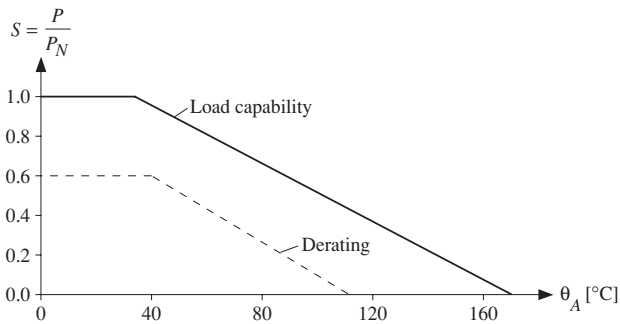


Figure 2.3 Load (power) capability and *typical derating curve* (dashed) for a bipolar Si-transistor as function of the ambient temperature θ_A (P =dissipated power, P_N =rated power at 40 °C)

2.2.3 Operating Conditions at Component Level, Stress Factors

The *operating conditions* of each element in the reliability block diagram influence the item's reliability and have to be considered. These operating conditions are function of the *environmental conditions* (Section 3.1.1) and *internal loads*, in operating and dormant state. Table 2.2 gives an overview of the most important parameters influencing electronic component failure rates.

A basic assumption is that components are in no way *over stressed*. In this context it is important to consider that the *load capability* of many electronic components decreases with increasing *ambient temperature*. This in particular for power, but often also for voltage and current. As an Example, Fig. 2.3 shows the variation of the power capability as function of the ambient temperature θ_A for a bipolar Si transistor (with constant thermal resistance R_{JA}). The continuous line represents the *load capability*. To the right of the break point the junction temperature is nearly equal to 175°C (max. specified operating temperature). The dashed line gives a typical *derating curve* for such a device. *Derating* is the designed (intentional) non utilization of the full load capability of a component with the purpose to reduce its failure rate. The *stress factor* (stress ratio, stress) S is defined as

$$S = \frac{\text{applied load}}{\text{rated load at } 40^\circ\text{C}}. \quad (2.1)$$

To give a touch, Figs. 2.4 - 2.6 show the influence of the temperature (ambient θ_A , case θ_C or junction θ_J) and of the stress factor S on the failure rate of some electronic components (from IEC 61709 [2.22]). Experience shows that for a good design and $\theta_A \leq 40^\circ\text{C}$ one should have $0.1 < S < 0.6$ for power, voltage, and current, $S \leq 0.8$ for fan-out, and $S \leq 0.7$ for U_{in} of lin. ICs (see Table 5.1 for greater details). $S < 0.1$ should also be avoided.

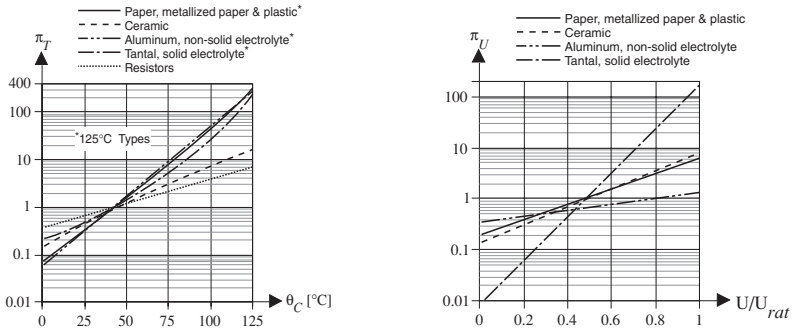


Figure 2.4 Factor π_T as function of the case temperature θ_C for capacitors and resistors, and factor π_U as function of the voltage stress for capacitors (examples from IEC 61709 [2.22])

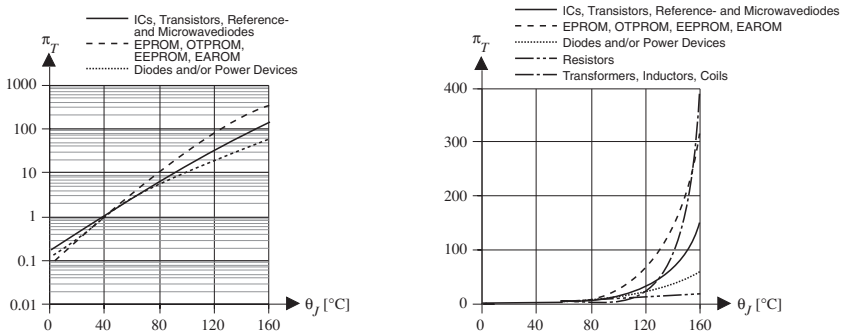


Figure 2.5 Factor π_T as function of the junction temperature θ_J (left, half log for semiconductors and right, linear for semiconductors, resistors and coils; examples from IEC 61709 [2.22])

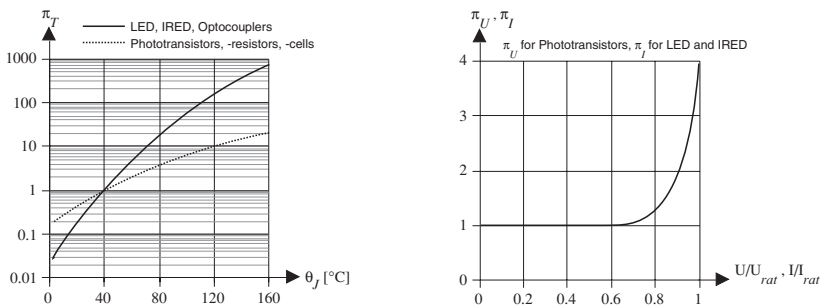


Figure 2.6 Factor π_T as function of the junction temperature θ_J and factors π_U and π_I as function of voltage and current stress for optoelectronic devices (examples from IEC 61709 [2.22])

2.2.4 Failure Rate of Electronic Components

The *failure rate* $\lambda(t)$ of an item is the conditional probability referred to δt of a failure in the interval $(t, t+\delta t]$ given that the item was new at $t=0$ and did not fail in the interval $(0, t]$, see Eqs. (1.5), (2.10), (A1.1), (A6.25). For a large population of statistically identical and independent items, $\lambda(t)$ exhibits often three successive phases: One of early failures, one with constant (or nearly so) failure rate and one involving failures due to wear out (Fig. 1.2). *Early failures* should be eliminated by a *screening* (Chapter 8). *Wear out failures* can be expected for some electronic components (electrolytic capacitors, power and optoelectronic devices, ULSI-ICs), as well as for mechanical and electromechanical components. They must be considered on a case-by-case basis in setting up a *preventive maintenance strategy* (Sections 4.6 & 6.8.2).

To simplify calculations, reliability prediction is often performed by assuming a *constant* (time independent) *failure rate* during the *useful life*

$$\lambda(t) = \lambda.$$

This approximation greatly simplify calculation, since a constant (time independent) failure rate λ leads to a flow of failures described by a homogeneous *Poisson process* with intensity λ (process with *memoryless property*, see Eqs. (2.14), (A6.29) & (A6.87), as well as Appendix A7.2.5).

The failure rate of components can be assessed *experimentally* by accelerated reliability tests or from field data (if operating conditions are sufficiently well known), with appropriate data analysis (Chapter 7). For established electronic and electromechanical components, models and figures for λ are often given in *failure rate handbooks* [2.20 - 2.30, 3.66, 3.67]. Among these, *FIDES Guide 2009 A* (2010) [2.21], *IEC 61709* (1996, Ed. 2 2011) [2.22], *IECTR 62380* (2004) [2.23], *IRPH 2003* [2.24], *MIL HDBK-217 G* (draft, Ed. H in preparation) [2.25], *RDF-96* [2.28], *RIAC-HDBK-217 Plus* (2008) [2.29], *Telcordia SR-332* (Rev. 3, 2011) [2.30]. *IEC 61709* gives *laws of dependency* of the failure rate on different stresses (temperature, voltage, etc.) and must be supported by a set of *reference failure rates* λ_{ref} for *standard industrial environment* (40°C ambient temperature θ_A , G_B as per Table 2.3, and steady-state conditions in field). *IRPH 2003* is based on *IEC 61709* and gives reference failure rates. Effects of thermal cycling, dormant state, and ESD are considered in *IEC TR 62380* and *RIAC-HDBK-217 Plus*. Refined models are in *FIDES Guide 2009 A*. *MIL-HDBK-217* was up to revision *F* (Not. 2, 1995) the most common reference, it is possible that starting with revision *H* it will take back this position. For mixed components /parts, *ESA Q-30-08*, *NSWC-11*, and *NPRD-2011* can be useful [2.20, 2.26, 2.27]. An international agreement on failure rate models for *reliability predictions at equipment and systems level in practical applications* should be found, also to simplify comparative investigations (see e. g. [1.2 (1996)] and the remark on p.38).

Table 2.3 Indicative figures for *environmental conditions* and corresponding factors π_E

Environment	Vibrations	Stress				π_E factor			
		Sand	Dust	RH (%)	Mech. shocks	ICs	DS	R	C
G_B (+5 to +45°C) (Ground benign)	2–200 Hz $\leq 0.1 g_n$	l	l	40–70	$\leq 5 g_n / 22$ ms	1	1	1	1
G_F (-40 to +45°C) (Ground fixed)	2–200 Hz $1 g_n$	m	m	5–100	$\leq 20 g_n / 6$ ms	2	2	3	3
G_M (-40 to +45°C) (Ground mobile)	2–500 Hz $2 g_n$	m	m	5–100	$10 g_n / 11$ ms to $30 g_n / 6$ ms	5	5	7	7
N_S (-40 to +45°C) (Nav. sheltered)	2–200 Hz $2 g_n$	l	l	5–100	$10 g_n / 11$ ms to $30 g_n / 6$ ms	4	4	6	6
N_U (-40 to +70°C) (Nav. unsheltered)	2–200 Hz $5 g_n$	h	m	10–100	$10 g_n / 11$ ms to $50 g_n / 2.3$ ms	6	6	10	10

C=capacitors, DS=discrete semicond., R=resistors, RH=rel. humidity, h=high, m=med., l=low, $g_n \approx 10 \text{ m/s}^2$ (G_B is *Ground stationary weather protected in* [2.24, 2.25, 2.30] and is taken as reference value in [2.22, 2.23])

Failure rates are taken from one of the above handbooks or from *one's own field data* for the calculation of the predicted reliability. Models in these handbooks have often a simple structure, of the form

$$\lambda = \lambda_0 \pi_T \pi_E \pi_Q \pi_A \quad (2.2)$$

or

$$\lambda = \pi_Q (C_1 \pi_T + C_2 \pi_E + C_3 \pi_L + \dots), \quad (2.3)$$

with $\pi_Q = \pi_{Q \text{ component}} \cdot \pi_{Q \text{ assembly}}$, often further simplified to

$$\lambda = \lambda_{ref} \pi_T \pi_U \pi_I, \quad (2.4)$$

by taking $\pi_E = \pi_Q = 1$ because of the assumed standard industrial environment ($\theta_A = 40^\circ\text{C}$, G_B as per Table 2.3, and steady-state conditions in field) and standard quality level. Indicative figures are in Tables 2.3, 2.4, A10.1, and in Example 2.4.

λ lies between 10^{-10} h^{-1} for passive components and 10^{-7} h^{-1} for VLSI ICs. The unit 10^{-9} h^{-1} is designated by *FIT* (failures in time or failures per 10^9 h).

For many electronic components, λ increases exponentially with temperature, doubling for an increase of 10 to 20°C . This is considered by the factor π_T , for which an *Arrhenius Model* is often used, yielding for the ratio of π_T factors at temperatures T_2, T_1 (for the case of *one dominant failure mechanism*, Eq. (7.56))

$$\frac{\pi_{T_2}}{\pi_{T_1}} = A \approx e^{\frac{E_a}{k} \left(\frac{1}{T_1} - \frac{1}{T_2} \right)}. \quad (2.5)$$

Thereby, A is the *acceleration factor*, k the Boltzmann constant ($8.6 \cdot 10^{-5} \text{ eV / K}$),

Table 2.4 Reference values for the *quality factors* π_Q component

	Qualification		
	Reinforced	CECC *	no special
Monolithic ICs	0.7	1.0	1.3
Hybrid ICs	0.2	1.0	1.5
Discrete Semiconductors	0.2	1.0	2.0
Resistors	0.1	1.0	2.0
Capacitors	0.1	1.0	2.0

* reference value in [2.22-224,2.28], class II in [2.30] (corresponds to *MIL-HDBK-217F* classes B, JANTX,M)

T the temperature in Kelvin degrees (junction for semiconductor devices), and E_a the *activation energy* in eV. As given in Figs. 2.4-2.6, experience shows that a *global value* for E_a often lie between 0.3eV and 0.6eV for Si devices. The design guideline $\theta_J \leq 100^\circ\text{C}$, if possible $\theta_J \leq 80^\circ\text{C}$, given in Section 5.1 for semiconductor devices is based on this consideration (see π_T in linear scale on Fig. 2.5). However, it must be pointed out that *each failure mechanism has its own activation energy* (see e.g. Table 3.5), and that the Arrhenius model does not hold for all electronic devices and for any temperature range (e.g. limited to about 0-150°C for ICs).

Models in *IEC 61709* assumes for π_T *two dominant failure mechanisms* with activation energies E_{a1} and E_{a2} (about 0.3eV for E_{a1} and 0.6eV for E_{a2}). The corresponding equation for π_T takes in this case the form

$$\pi_T = \frac{a e^{z E_{a1}} + (1-a) e^{z E_{a2}}}{a e^{z_{ref} E_{a1}} + (1-a) e^{z_{ref} E_{a2}}}, \quad (2.6)$$

with $0 \leq a \leq 1$, $z = (1/T_{ref} - 1/T_2) / k$, $z_{ref} = (1/T_{ref} - 1/T_1) / k$, and $T_{ref} = 313\text{K}$ (40°C). Multiple failure mechanisms are also considered in *FIDES Guide 2009A* [2.21, 3.32].

It can be noted that for $T_2 = T_1 + \Delta T$, Eq. (2.5) yields $A \approx e^{\Delta T E_a / k T_1^2}$ (straight line in Fig. 7.10). Assuming ΔT normally distributed (during operation), it follows from case (i) of Example A6.18 that the *acceleration factor* A is *lognormally distributed*; this can be used to refine failure rate calculations for missions with variable operating temperature, see also [3.57 (2005), 3.61] and remarks to Eqs. (7.55) & (7.56).

For components of good commercial quality, and using $\pi_E = \pi_Q = 1$, failure rate calculations lead to figures which for practical applications in *standard industrial environments* ($\theta_A = 40^\circ\text{C}$, G_B as per Table 2.3, and steady-state conditions in field) *often agree reasonably well with field data* (up to a factor of 2). This holds at *equipment & system level*, although deviations can occur at component level, depending on the failure rate catalog used (see e.g. Example 2.4). Greater differences can occur if field conditions are severe or not sufficiently well known. However, comparisons with obsolete data should be dropped and it would seem to be opportune to

unify models and data, taking from each model the "good part" and putting them together for "better" models (strategy applicable to many situations). Models for prediction in practical applications should remain *reasonably simple*, laws for *dominant failure mechanisms* should be given in *standards*, and the list of *reference failure rates* λ_{ref} should be yearly updated. Models based on *failure mechanisms* (physics of failure) have to be used as basis for simplified models, see e. g. [2.15, 3.55, 3.58, 3.66, 3.67] for concrete steps in this direction and pp. 102, 103, and 333 for some considerations. Also it can become necessary to consider temperature and stress dependent parameters. The assumption $\lambda < 10^{-9} \text{h}^{-1}$ should be confined to components with stable production process and a *reserve to technological limits*.

Calculation of the failure rate at system level often requires considerations on the *mission profile*. If the mission can be partitioned in time spans with almost homogeneous stresses, switching effects are negligible, and the failure rate is time independent (between successive state changes of the system), the contribution of each time span can be added linearly, as often assumed for *duty cycles*. With these assumptions, investigation of *phased-mission* systems is possible (Section 6.8.6.2).

Estimation and demonstration of component's and system's failure rates are considered in Section 7.2.3, accelerated tests in Section 7.4.

Example 2.4

For indicative purpose, following table gives failure rates calculated according to some different data bases [2.30 (2001), 2.24, 2.23] for *continuous operation* in non interface application; $\theta_A=40^\circ\text{C}$, $\theta_J=55^\circ\text{C}$, $S = 0.5$, G_B , and $\pi_Q=1$ as for CECC certified and class II Telcordia; PI is used for plastic package; λ in 10^{-9}h^{-1} (FIT), *quantified* at $1 \cdot 10^{-9} \text{h}^{-1}$ (see also Tab. A10.1).

	Telcordia 2001	IRPH 2003	IEC ** 62380 2004	λ_{ref} *
DRAM, CMOS, 1 M, PI	32	10	6	10
SRAM, CMOS, 1 M, PI	60	30	11	30
EPROM CMOS, 1 M, PI	53	30	20	20
16 Bit μ P($10^5 TR$), CMOS, PI	18	(60)	(10)	40
Gate array, CMOS, 30,000 gates , 40 Pins, PI	17	35	17	25
Lin, Bip, 70 Tr, PI	33	7	21	10
GP diode, Si, 100 mA, lin, PI	4	1	1	2
Bip. transistor, 300 mW, switching, PI	6	3	1	3
JFET, 300 mW, switching, PI	(28)	5	1	4
Ceramic capacitor, 100 nF, 125°C, class 1	1	1	1	1
Foil capacitor, 1 μ F	1	1	1	1
Ta solid (dry) capacitor, herm., 100 μ F, 0.3 Ω / V	1	1	1	2
MF resistor, 1/4 W, 100 k Ω	1	1	1	1
Cermet pot, 50 k Ω , < 10 annual shaft rot.	(20)	(30)	1	6

* suggested values for computations per IEC 61709 [2.22], $\theta_A=40^\circ\text{C}$; ** production year 2001 for ICs

2.2.5 Reliability of One-Item Structures

A *one-item nonrepairable structure* is characterized by the distribution function $F(t) = \Pr\{\tau \leq t\}$ of its *failure-free time* $\tau > 0$, hereafter used as a synonym for *failure-free operating time*. The *reliability function* $R(t)$, i. e. the probability of no failure in the interval $(0, t]$, follows as (Eq. (A6.24))

$$R(t) = \Pr\{\text{no failure in } (0, t]\} = \Pr\{\tau > t\} = 1 - F(t),^{+)} \quad F(0) = 0, R(0) = 1. \quad (2.7)$$

$R(0) = 1$ implies *item new at* $t=0$, and is a consequence of $F(0) = 0$. At system level,

to specify the state at $t=0$, $R_{S_i}(t)$ will be used starting from Section 2.2.6; thereby, S stands for system (the highest integration level of the item considered) and i for the state entered at $t=0$ ($R_{S_i}(0) = 1$, Table 6.2); $i=0$ holds for system new at $t=0$, yielding $R_{S_0}(t)$ with $R_{S_0}(0) = 1$.

In this section, as in Chapter 1 & Appendix A6.5, *item new at* $t=0$ is tacitly assumed.

The mean (expected value) of the failure-free time τ , designated as *MTTF* (*mean time to failure*), can be calculated from Eq. (A6.38) as

$$MTTF = E[\tau] = \int_0^{\infty} R(t) dt. \quad (2.8)$$

Should the item exhibit a *useful life* limited to T_L , Eq. (2.8) yields $MTTF_L = \int_0^{T_L} R(t) dt$. In the following, $T_L = \infty$ is tacitly assumed (except in Example 6.25 suppl. results). Equation (2.8) is an important relationship. It is valid not only for a one-item structure, often considered as an indivisible entity, but it also holds for a one-item structure of arbitrary complexity; $R_{S_i}(t)$ & $MTTF_{S_i}$ will be used to emphasize this

$$MTTF_{S_i} = \int_0^{\infty} R_{S_i}(t) dt. \quad (2.9)$$

Assuming $R(t)$ derivable, the *failure rate* $\lambda(t)$ of a *nonrepairable one-item structure new at* $t=0$ is given by (Eq. (A6.25))

$$\lambda(t) = \lim_{\delta t \downarrow 0} \frac{1}{\delta t} \Pr\{t < \tau \leq t + \delta t \mid \tau > t\} = - \frac{dR(t)/dt}{R(t)}, \quad (2.10)$$

with $R(t)$ as per Eq. (2.7). Considering $R(0) = 1$, Eq. (2.10) yields

$$R(t) = e^{-\int_0^t \lambda(x) dx}, \quad (2.11)$$

from which, for $\lambda(t) = \lambda$,

$$R(t) = e^{-\lambda t}. \quad (2.12)$$

⁺) If the mission duration is a random time $\tau_W > 0$, Eq. (2.76) applies, see also Eq. (6.244).

The mean time to failure is in this case equal to $1/\lambda$. In practical applications

$$1/\lambda = MTBF \quad (2.13)$$

($1/\lambda_S = MTBF_S$ for systems) is often used, where *MTBF* stands for *mean operating time between failures*, expressing a figure applicable to *repairable structures*. Because of the often used estimate $\hat{MTBF} = T/k$ (Eq.(7.28)) and also to avoid misuses,

MTBF should be confined to repairable items with constant (time independent) failure rate which are as-good-as-new after repair (pp. 6, 316, 380).

As shown by Eq. (2.11), the reliability function of a nonrepairable one-item structure *new at $t=0$* is *completely defined* by its failure rate $\lambda(t)$. In the case of electronic components, $\lambda(t) = \lambda$ can often be assumed. The failure-free time τ then exhibits an *exponential distribution* ($F(t) = \Pr\{\tau \leq t\} = 1 - e^{-\lambda t}$). For a time dependent failure rate (e.g. $\lambda(t)$ as in Fig. 1.2), the distribution function of the failure-free time can often be approximated by the weighted sum (Eq. (A6.34)) of a Gamma distribution (Eq. (A6.97)), $\beta < 1$) and a shifted Weibull distribution (Eq. (A6.96), $\beta > 1$).

Equations (2.7), (2.8), (2.10) - (2.12) implies that the nonrepairable one-item structure is *new at time $t=0$* . Also of interest in, some applications, is the probability of failure-free operation during an interval $(0, t]$ *under the condition that the item has already operated without failure for x_0 time units before $t=0$* . This quantity is a *conditional probability*, designated by $R(t | x_0)$ and given by (Eq. (A6.27))

$$R(t | x_0) = \Pr\{\tau > t + x_0 | \tau > x_0\} = \frac{R(t + x_0)}{R(x_0)} = e^{-\int_{x_0}^{t+x_0} \lambda(x) dx}, \quad R(0) = 1. \quad (2.14)$$

For $\lambda(x) = \lambda$, Eq. (2.14) reduces to Eq. (2.12). This *memoryless property* occurs only with *constant* (time independent) *failure rate*. Its use greatly simplifies calculations, in particular in Chapter 6 for repairable systems. $R(t | x_0)$ has to be distinguished from the *interval reliability* $IR(t, t+\theta) = \Pr\{up \text{ in } [t, t+\theta] | \text{new at } t=0\}$ per Eq. (6.26), which *applies to repairable items*. In particular,

for a nonrepairable item $IR(t, t+\theta) = R(t+\theta)$, and this is a good reason to avoid to use $IR(t_1, t_2)$ as reliability $R(t_1, t_2)$, see also pp. 179, 384, 426.

In some applications, it can appear that elements of a population of similar items exhibits different failure rate. Considering as an example the case of components delivered from two manufacturer with proportion p & $(1-p)$ and failure rates λ_1 & λ_2 , the reliability function of an arbitrarily selected component is (Eq. (A6.34))

$$R(t) = pR_1(t) + (1-p)R_2(t) = pe^{-\lambda_1 t} + (1-p)e^{-\lambda_2 t}.$$

According to Eq. (2.10), it follows for the failure rate that

$$\lambda(t) = (p\lambda_1 e^{-\lambda_1 t} + (1-p)\lambda_2 e^{-\lambda_2 t}) / (pe^{-\lambda_1 t} + (1-p)e^{-\lambda_2 t}). \quad (2.15)$$

$\lambda(t)$ decrease monotonically from $p\lambda_1 + (1-p)\lambda_2$ to the minimum of $\{\lambda_1, \lambda_2\}$.

As a final remark, let us point out that Eqs. (2.8) and (2.9) *can also be used for repairable items*. In fact, assuming that at failure the item is replaced by a statistically equivalent one, or repaired to *as-good-as-new*, a new independent failure-free time τ with the *same distribution function* as the former one is started after repair (replacement), yielding the same expected value. However, for these cases the variable x starting by $x=0$ after each repair has to be used instead of t (as for *interarrival times*). With this,

MTTF_{S_i} can be used for the mean time to failure of a system, independently of whether it is repairable or not; the only assumption is that the system is *as-good-as-new* after repair, with respect to the state Z_i entered at $t=0$.

This applies, in particular, to systems described by Markov and semi-Markov processes (Tables 6.1 & 6.2 on pp. 171-173), and implies that *at each repair all non repaired (renewed) elements in the system have constant failure rates* (if the failure rate of one non renewed element is not constant, difficulties can arise, also in the case of an *as-bad-as-old* hypothesis, see pp. 138, 427, 519 for greater details).

2.2.6 Reliability of Series - Parallel Structures

For nonrepairable items (up to item failure), reliability calculation at equipment and systems level can often be performed using models of Table 2.1 (p. 31). The one-item structure has been introduced in Section 2.2.5. Series, parallel, and series-parallel structures are considered in this Section. Section 2.3 deals with the last 3 models of Table 2.1. To unify notation, *system* will be used for the *item investigated*, and it is assumed that at $t=0$ the system is new (yielding $R_{S0}(t)$, with $R_{S0}(0)=1$).

2.2.6.1 Systems without Redundancy

From a reliability point of view, a system has *no redundancy* (series model) if all elements must work in order to fulfill the required function. The reliability block diagram consists in this case of the series connection of all elements (E_1 to E_n) of the system (row 2 in Table 2.1). For calculation purposes it is often assumed that each element operates and fails *independently* from every other element (p. 52). For series systems, this assumption must not (in general) be verified, because the first failure is a system failure for reliability purposes. Let e_i be the event

$$\{e_i\} \equiv \{\text{element } E_i \text{ works without failure in the interval } (0, t] \mid \text{new at } t=0\}.$$

The probability of this event is the reliability function $R_i(t)$ of element E_i , i. e.

$$\Pr\{e_i\} = \Pr\{\tau_i > t\} = R_i(t), \quad R_i(0) = 1. \quad (2.16)$$

The system does not fail in the interval $(0, t]$ if and only if all elements, E_1, \dots, E_n do not fail in that interval, thus

$$R_{S0}(t) = \Pr\{e_1 \cap \dots \cap e_n\}.$$

Here and in the following, S stands for system and 0 specifies that the system is new at $t=0$. Due to the assumed independence among the elements E_1, \dots, E_n and thus among e_1, \dots, e_n , it follows (Eq. (A6.9)) that for the *reliability function* $R_{S0}(t)$

$$R_{S0}(t) = \prod_{i=1}^n R_i(t), \quad R_i(0) = 1, \quad (2.17)$$

holds. The *failure rate* of the system can be calculated from Eq. (2.10)

$$\lambda_S(t) = \sum_{i=1}^n \lambda_i(t), \quad (2.18)$$

Equation (2.18) leads to the following important conclusion:

The failure rate of a series system (system without redundancy), consisting of independent elements (p.52), is equal to the sum of the failure rates of its elements.

The system's *mean time to failure* follows from Eq. (2.9). The special case in which all elements have a *constant failure rate* $\lambda_i(t) = \lambda_i$ leads to

$$R_{S0}(t) = e^{-\lambda_S t}, \quad \lambda_S(t) = \lambda_S = \sum_{i=1}^n \lambda_i(t), \quad MTTF_{S0} = \frac{1}{\lambda_S}. \quad (2.19)$$

2.2.6.2 Concept of Redundancy

High reliability, availability, and/or safety at equipment and systems level can often only be reached with the help of redundancy. *Redundancy* is the existence of more than one means (in an item) for performing the required function. Redundancy does not just imply a *duplication of hardware*, since it can be implemented at the software level or as a *time redundancy*. However, to avoid *common cause* and *single-point failures*, redundant elements should be realized (designed and manufactured) *independently* from each other. Irrespective of the *failure mode* (e. g. shorts or opens), redundancy still appears in *parallel on the reliability block diagram*, not necessarily in the hardware (Example 2.6). In setting up the reliability block diagram, particular attention must be paid to the *series* element to a redundancy. An FMEA (Section 2.6) is generally *mandatory* for such a decision. Should a redundant element fulfill only a part of the required function a *pseudo redundancy* exist. From the operating point of view, one distinguishes between active, warm, and standby redundancy:

^{+) In Eq. (2.18) and in the following, $\lambda_S(t)$ is used instead of $\lambda_{S0}(t)$ also to point out that for considerations on the failure rate, the item (system) is generally assumed new at $t=0$ (Eq. (2.10)).}

1. *Active Redundancy* (parallel, hot): Redundant elements are subjected from the beginning to the *same load* as operating elements; *load sharing* is possible, but is not considered in the case of *independent elements* (Section 2.2.6.3).
2. *Warm Redundancy* (lightly loaded): Redundant elements are subjected to a *lower load* until one of the operating elements fails; *load sharing* is present; however, the failure rate is lower in reserve than in operation (Section 2.3.5).
3. *Standby Redundancy* (cold, unloaded): Redundant elements are subjected to *no load* until one of the operating elements fails; *no load sharing* is possible, and the failure rate in reserve state is *assumed* to be zero (Section 2.3.5).

Important redundant structures with *independent elements in active redundancy* are considered in Sections 2.2.6.3 to 2.3.4. Warm and standby redundancies are investigated in Section 2.3.5 and Chapter 6 (repair rate $\mu=0$).

2.2.6.3 Parallel Models

A parallel model consists of n (often statistically identical) elements in *active redundancy*, of which k ($1 \leq k < n$) are necessary to perform the required function and the remaining $n - k$ are in reserve. Such a structure is designated as a *k-out-of-n* (or *k-out-of-n: G*) *redundancy*. Investigation assumes, in general, independent elements (see Sections 2.3.5, 6.4, 6.5 for load sharing and Section 6.8 for further refinements like imperfect switching, common cause failures etc.).

Let us consider at first the case of an active *1-out-of-2 redundancy* as given in Table 2.1 (row 3). The required function is fulfilled if at least one of the elements E_1 or E_2 works without failure in the interval $(0, t]$. With the same notation as for Eq. (2.16) it follows that (Eq. (A6.13))

$$R_{S0}(t) = \Pr\{e_1 \cup e_2\} = \Pr\{e_1\} + \Pr\{e_2\} - \Pr\{e_1 \cap e_2\}; \quad (2.20)$$

from which, due to the assumed independence among the elements E_1 & E_2 and thus among the events e_1 & e_2 (Eqs. (A6.8), (2.16))

$$R_{S0}(t) = R_1(t) + R_2(t) - R_1(t)R_2(t), \quad R_1(0) = R_2(0) = 1. \quad (2.21)$$

The *mean time to failure* $MTTF_{S0}$ can be calculated from Eq.(2.9). For two identical elements with constant failure rate λ ($R_1(t) = R_2(t) = e^{-\lambda t}$) it follows that

$$R_{S0}(t) = 2e^{-\lambda t} - e^{-2\lambda t}, \quad \lambda_S(t) = 2\lambda \frac{1 - e^{-\lambda t}}{2 - e^{-\lambda t}}, \quad MTTF_{S0} = \frac{2}{\lambda} - \frac{1}{2\lambda} = \frac{3}{2\lambda}. \quad (2.22)$$

Equation (2.22) shows that in the presence of redundancy, the system failure rate $\lambda_S(t)$ is a function of time (strictly increasing from 0 to λ), even if the element's failure rate λ is constant. However, the stochastic behavior of the system is still described by a Markov process (Section 2.3.5). This time dependence becomes negligible in the case of *repairable systems* (see Eq. (6.94) for const. failure & repair rates).

Generalization to an active *k-out-of-n redundancy* (*k-out-of-n:G*) with *n* identical ($R_1(t) = \dots = R_n(t) = R(t)$) and independent elements follows from the *binomial distribution* (Eq. (A6.120)) by setting $p = R(t)$

$$R_{S0}(t) = \sum_{i=k}^n \binom{n}{i} R^i(t) (1-R(t))^{n-i}, \quad R(0) = 1. \quad (2.23)$$

$R_{S0}(t)$ is the sum of the probabilities for $0, 1, \dots, n-k$ failures ($i = n, n-1, \dots, k$) and can be interpreted as the probability of observing at least *k* successes in *n* Bernoulli trials with $p = R(t)$. The case $k = 1$ yields (with $R = R(t)$ and $R(0) = 1$)

$$R_{S0}(t) = \sum_{i=1}^n \binom{n}{i} R^i (1-R)^{n-i} = \sum_{i=0}^n \binom{n}{i} R^i (1-R)^{n-i} - (1-R)^n = 1 - (1-R)^n. \quad (2.24)$$

The mean time to failure $MTTF_{S0}$ can be calculated from Eq. (2.9), yielding

$$R_{S0}(t) = 1 - (1 - e^{-\lambda t})^n \quad \text{and} \quad MTTF_{S0} = \frac{1}{\lambda} \left(1 + \frac{1}{2} + \dots + \frac{1}{n} \right) \quad (2.25)$$

for $k=1$ and $R(t) = e^{-\lambda t}$. The improvement in $MTTF_{S0}$ shown by Eq. (2.25) becomes much greater when *repair* without interruption of operation at system level is possible ($\mu/2\lambda$ instead of $3/2$ for an active 1-out-of-2 redundancy, where $\mu = 1/MTTR$ is the constant repair rate, see Tables 6.6 & 6.8). However,

as shown in Fig. 2.7, the increase of the reliability function $R_{S0}(t)$ caused by redundancy is important for short missions ($t \ll 1/\lambda$), even in the nonrepairable case.

If the elements of a *k-out-of-n* active redundancy are independent but different, computation must consider all $\binom{n}{i}$ subsets with exactly *i* elements up and $n-i$ elements down, and sum from $i=k$ to *n* (for $k=1$, Eq.(2.24) applies as $R_{S0} = 1 - \prod(1-R_i)$).

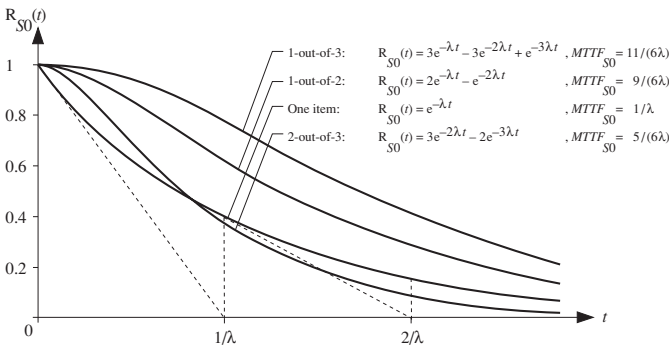


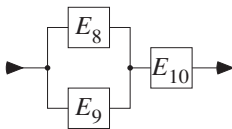
Figure 2.7 Reliability functions for the one-item structure (as reference) and for some active redundancies (nonrepairable up to system failure, constant failure rates, *identical and independent elements*, ideal failure detection & switch, no load sharing (see Section 2.3.5 for load sharing))

In addition to the k -out-of- n redundancy described by Eq. (2.23), of interest in some applications are cases in which the fulfillment of the required function asks that *not more than* $n - k$ consecutive elements fail (in linear or circular arrangement). Such a structure can allow more than $n - k$ failures and is thus at least as reliable as the corresponding k -out-of- n redundancy. For a 3-out-of-5 redundancy it holds e.g. $R_{S0} = R^5 + 5R^4(1-R) + 10R^3(1-R)^2 + 7R^2(1-R)^3 + R(1-R)^4$ for linear and $R_{S0} = R^5 + 5R^4(1-R) + 10R^3(1-R)^2 + 5R^2(1-R)^3$ for circular arrangement ($R_{S0} = R^5 + 5R^4(1-R) + 10R^3(1-R)^2$ according to Eq. (2.23)). The model considered here differs from the so called *consecutive k-out-of-n: F system*, in which the system is failed if k or more consecutive elements are failed [2.31, 2.38, 2.42]. Examples for consecutive k -out-of- n structures are conveying systems and relay stations. However, for this kind of application it is important to verify that all elements are *independent*, in particular with respect to common cause failures, load sharing, etc. (of course, for $k = 1$ the *consecutive k-out-of-n: F system* reduces to a series model).

2.2.6.4 Series - Parallel Structures

Series - parallel structures can be investigated through successive use of the results for series and parallel models. This holds in particular for *nonrepairable* systems with *active redundancy* and *independent* elements (p. 52). To demonstrate the procedure, let us consider row 5 in Table 2.1:

1st step: The series elements $E_1 - E_3$ are replaced by E_8 , $E_4 - E_5$ by E_9 , and $E_6 - E_7$ by E_{10} , yielding



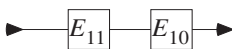
with

$$R_8(t) = R_1(t)R_2(t)R_3(t)$$

$$R_9(t) = R_4(t)R_5(t)$$

$$R_{10}(t) = R_6(t)R_7(t)$$

2nd step: The 1-out-of-2 redundancy $E_8 - E_9$ is replaced by E_{11} , giving



with $R_{11}(t) = R_8(t) + R_9(t) - R_8(t)R_9(t)$

3rd step: From steps 1 and 2, the *reliability function* of the system follows as (with $R_S = R_{S0}(t)$, $R_i = R_i(t)$, $R_i(0) = 1$, $i = 1, \dots, 7$)

$$R_S = R_{11} R_{10} = (R_1 R_2 R_3 + R_4 R_5 - R_1 R_2 R_3 R_4 R_5) R_6 R_7. \tag{2.26}$$

The mean time to failure can be calculated from Eq. (2.9). Should all elements have a constant failure rate (λ_1 to λ_7), then

$$R_{S0}(t) = e^{-(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_6 + \lambda_7)t} + e^{-(\lambda_4 + \lambda_5 + \lambda_6 + \lambda_7)t} - e^{-(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7)t}$$

and

$$MTTF_{S0} = \frac{1}{\lambda_1 + \lambda_2 + \lambda_3 + \lambda_6 + \lambda_7} + \frac{1}{\lambda_4 + \lambda_5 + \lambda_6 + \lambda_7} - \frac{1}{\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7}. \quad (2.27)$$

Under the assumptions of active redundancy, nonrepairable (up to system failure), independent elements (p. 52), and constant failure rates, the *reliability function* $R_{S0}(t)$ of a series - parallel structure is given by a *sum of exponential functions*. The *mean time to failure* $MTTF_{S0}$ follows then directly from the exponent terms of $R_{S0}(t)$, see Eq. (2.27) for an example.

The use of *redundancy* implies the introduction of a *series element* in the reliability block diagram which takes into account the parts which are common to the redundant elements, creates the redundancy (Example 2.5), or assumes a control and/or *switching function*. For a design engineer it is important to *evaluate the influence of the series element* in a redundant structure. Figures 2.8 and 2.9 allow such an evaluation to be made for the case of *constant failure rates, independent elements, and active redundancy*. In Fig. 2.8, a one-item structure (E_1 with failure rate λ_1) is compared with a 1-out-of-2 redundancy with a series element (E_2 with failure rate λ_2). In Fig. 2.9, the 1-out-of-2 redundancy with a series element E_2 is compared with the structure which would be obtained if a 1-out-of-2 redundancy for E_2 with a series element E_3 would become necessary. Obviously $\lambda_3 < \lambda_2 < \lambda_1$ ($\lambda_1 = \lambda_2$ for Fig. 2.8 and $\lambda_1 = \lambda_2 = \lambda_3$ for Fig. 2.9 have an indicative purpose only). The three cases are labeled a, b, and c. The upper parts of Figs. 2.8 and 2.9 depict the reliability functions and the lower parts the ratios $MTTF_{S0b}/MTTF_{S0a}$ and $MTTF_{S0c}/MTTF_{S0a}$, respectively. Comparison between case a of Fig. 2.8 and case c of Fig. 2.9, given as $MTTF_{S0c}/MTTF_{S0a}$ on Fig. 2.8, shows the lower dependency on λ_2/λ_1 . From Figs. 2.8 and 2.9 following *design guideline* can be formulated:

To approach the 1.5 MTTF gain given by the redundancy (Eq. (2.25) with $n=2$), the failure rate λ_2 of the series element in a nonrepairable (up to system failure) 1-out-of-2 active redundancy should not be larger than 10% of the failure rate λ_1 of the redundant elements (similar is for λ_3 in Fig. 2.9); thus,

$$10 \lambda_3 < \lambda_2 < 0.1 \lambda_1. \quad (2.28)$$

The investigation of the structures given in Figs. 2.8 & 2.9 for the *repairable case* ($\mu = 1/MTTR$ as constant repair rate) leads in Section 6.6 to more severe conditions ($\lambda_2 < 0.01\lambda_1$ in general, and $\lambda_2 < 0.002\lambda_1$ for $\mu/\lambda_1 > 500$), see Figs. 6.17 & 6.18.

Influence of imperfect switching, as well as incomplete coverage, common cause failures, and other more, are investigated for the repairable case in Section 6.8.

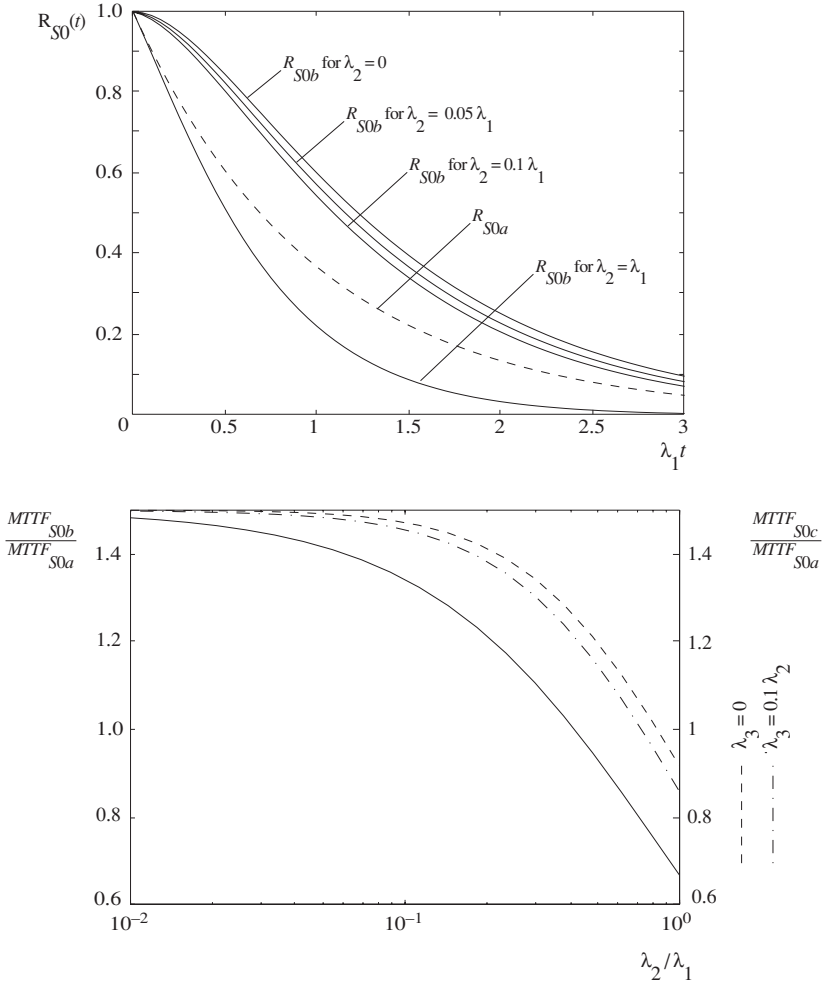
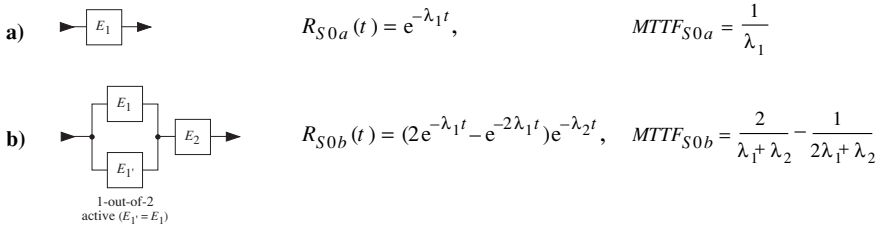


Figure 2.8 Comparison between the *one-item structure* and a *1-out-of-2 active redundancy with series element*: *nonrepairable* (up to system failure), *independent elements*, *constant failure rates* λ_1 & λ_2 (λ_1 remains the same in both structures, equations from Table 2.1, given on the right-hand side is $MTTF_{S0c}/MTTF_{S0a}$ with $MTTF_{S0c}$ from Fig. 2.9; see Fig. 6.17 for the repairable case)

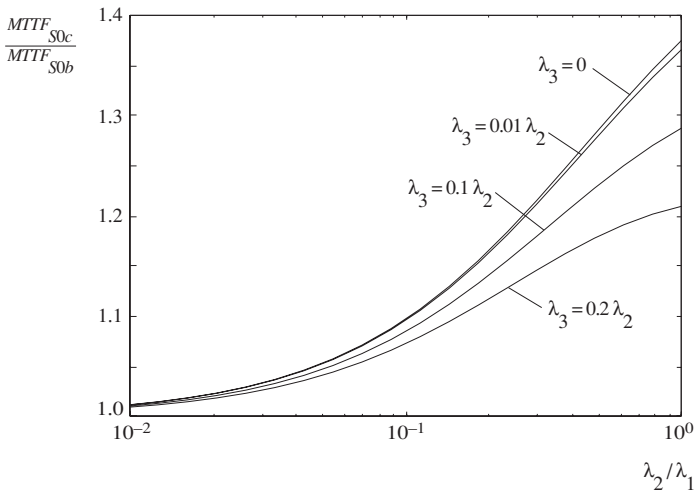
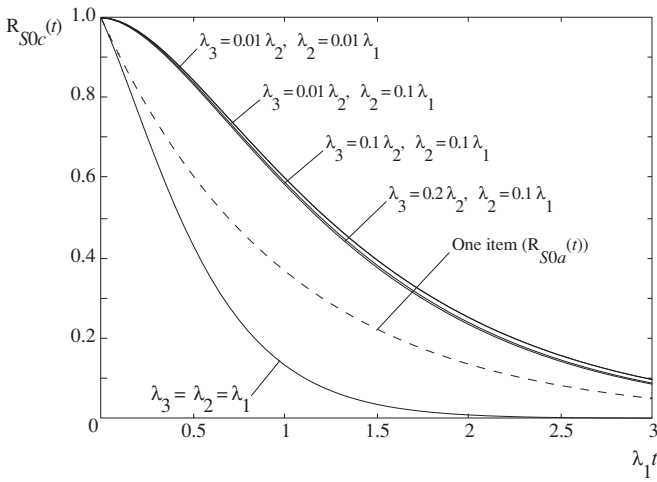
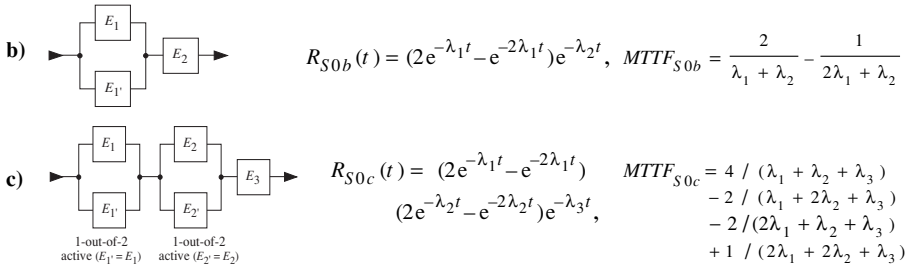


Figure 2.9 Comparison between *basic series-parallel structures: nonrepairable* (up to system failure), *active redundancy, independent elements, constant failure rates* λ_1 to λ_3 (λ_1 and λ_2 remain the same in both structures, equations from Table 2.1; see Fig. 6.18 for the repairable case)

2.2.6.5 Majority Redundancy

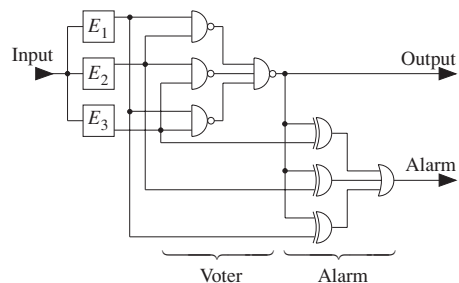
Majority redundancy is a special case of a k -out-of- n redundancy, frequently used in, but not limited to, redundant digital circuits. $2n + 1$ outputs are fed to a *voter* whose output represents the majority of its $2n + 1$ input signals (N -modular redundancy). The investigation is based on the previously described procedure for series - parallel structures, see for example the case of $n = 1$ (active redundancy 2-out-of-3 in series with the voter E_v) given in row 6 of Table 2.1. The majority redundancy realizes in a simple way a *fault-tolerant structure without the need for control or switching elements*. The required function is performed with no operational interruption up to the time point of the second failure, while the first failure is automatically masked by the majority redundancy. In digital circuits, the *voter* for a majority redundancy with $n = 1$ consists of three two-input NAND and one three-input NAND gate, for a bit solution. An *alarm circuitry* is also simple to realize, and can be implemented with three two-input EXOR and one three-input OR gates (Example 2.5). A similar structure as for the alarm circuitry can be used to realize a second alarm circuitry giving a pulse at the second failure, expanding thus the 2-out-of-3 active redundancy to a 1-out-of-3 active redundancy (Problem 2.6 in Appendix A11). A majority redundancy can also be realized with software (N -version programming). Without loss of generality, majority redundancy applies to serial or parallel n bit words (bytes). See e.g. [6.65 (Chapter 4)] for a deeper discussion.

Example 2.5

Realize a majority redundancy for $n = 1$ with voter and alarm signal at the first failure of a redundant element (a bit solution with "1" for operating and "0" for failure).

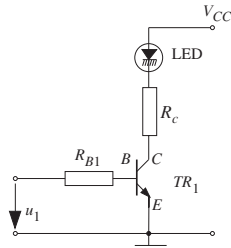
Solution

Using the same notation as for Eq. (2.16), the 2-out-of-3 active redundancy can be implemented by $(e_1 \cap e_2) \cup (e_1 \cap e_3) \cup (e_2 \cap e_3)$. With this, the functional block diagram of the voter for a majority redundancy with $n = 1$ is obtained as realization of the logic equation related to the above expression. The alarm circuitry giving a logic 1 at the occurrence of the first failure is also easy to implement. Also it is possible to realize a second alarm circuitry to detect the second failure, expanding the 2-out-of-3 to a 1-out-of-3 redundancy (Problem 2.6 in Appendix A11; see also Fig. 2.7 for a comparison).



Example 2.6

Compute the predicted reliability for the following circuitry, for which the required function asks that the LED must light when the control voltage u_1 is high. The environmental conditions correspond to G_B in Table 2.3, with ambient temperature $\theta_A = 50^\circ\text{C}$ inside the equipment and 30°C at the location of the LED; quality factor $\pi_Q = 1$ as per Table 2.4.



u_1 : 0.1 V and 4 V
 V_{CC} : 5 V
 LED : 1 V at 20 mA, $I_{\max} = 100$ mA
 R_C : 150 Ω , 1/2 W, MF
 TR_1 : Si, 0.3 W, 30 V, $\beta > 100$, plastic
 R_{B1} : 10 k Ω , 1/2 W, MF

Solution

The solution is based on the procedure given in Fig 2.1.

1. The required function can be fulfilled since the transistor works as an electronic switch with $I_C \approx 20$ mA and $I_B \approx 0.33$ mA in the on state (saturated) and the off state is assured by $u_1 = 0.1$ V.
2. Since all elements are involved in the required function, the reliability block diagram consists of the series connection of the five items E_1 to E_5 , where E_5 represents the printed circuit with soldering joints.



3. The stress factor of each element can be easily determined from the circuitry and the given rated values. A stress factor 0.1 is assumed for all elements when the transistor is off. When the transistor is on, the stress factor is 0.2 for the diode and about 0.1 for all other elements. The ambient temperature is 30°C for the LED and 50°C for the remaining elements.
4. The failure rates of the individual elements is determined (approximately) with data from Section 2.2.4 (Example 2.4, Figs. 2.4 - 2.6, Tables 2.3 and 2.4 with $\pi_E = \pi_Q = 1$). Thus,

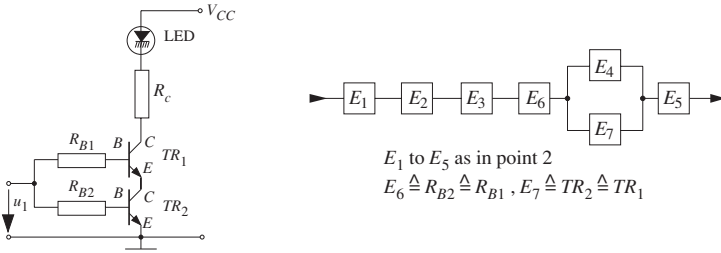
$$\begin{aligned}
 \text{LED} & : \lambda_1 \approx 1.3 \cdot 10^{-9} \text{ h}^{-1} \\
 \text{Transistor} & : \lambda_4 \approx 3 \cdot 10^{-9} \text{ h}^{-1} \\
 \text{Resistor} & : \lambda_2 = \lambda_3 \approx 0.3 \cdot 10^{-9} \text{ h}^{-1},
 \end{aligned}$$

when the transistor is on. For the printed circuit board and soldering joints, $\lambda_5 = 2 \cdot 10^{-9} \text{ h}^{-1}$ is assumed. The above values for λ remain practically unchanged when the transistor is off due to the low stress factors (the stress factor in the off state was set at 0.1).

5. Based on the results of Step 4, the reliability function of each element can be determined as $R_i(t) = e^{-\lambda_i t}$
6. The reliability function $R_{S_0}(t)$ for the whole circuitry can now be calculated. Equation (2.19)

yields $R_S(t) = e^{-6.9 \cdot 10^{-9}t}$. For 10 years of continuous operation, for example, the predicted reliability of the circuitry is > 0.999 .

7. **Supplementary result:** To discuss this example further, let us assume that the failure rate of the transistor is too high (e.g. for safety reasons) and that no transistor of better quality can be obtained. Redundancy should be implemented for this element. Assuming as *failure modes short* between emitter and collector for transistors and *open* for resistors, the resulting circuitry and the corresponding reliability block diagram are



Due to the very small stress factor, calculation of the individual element failure rates yields the same values as without redundancy. Thus, for the reliability function of the circuitry one obtains, assuming independent elements (up to failure),

$$R_{S0}(t) = e^{-4.2 \cdot 10^{-9}t} (2e^{-3 \cdot 10^{-9}t} - e^{-6 \cdot 10^{-9}t}),$$

from which it follows that

$$R_{S0}(t) \approx e^{-4.2 \cdot 10^{-9}t} \quad \text{for } t \leq 10^6 \text{ h.}$$

Circuitry reliability is then practically no longer influenced by the transistor. This agrees with the discussion made with Fig. 2.7 for $\lambda t \ll 1$. If the *failure mode* of the transistors were an open between collector and emitter, both elements E_4 and E_7 would appear in series in the reliability block diagram; redundancy would be a *disadvantage* in this case. The intention to put R_{B1} and R_{B2} in parallel (redundancy) or to use just one basis resistor is wrong, the functionality of the circuitry would be compromised because of the saturation voltage of TR_2 .

2.2.7 Part Count Method

In an early development phase, for logistic purposes, or in some particular applications, a *rough estimate* of the predicted reliability can be required. For such an analysis, it is generally assumed that the system under consideration is *without redundancy* (series structure as in Section 2.2.6.1) and the calculation of the failure rate at component level is made either using *field data* or by considering technology, environmental, and quality factors only. This procedure is known as *part count method* [2.25] and differs basically from the *part stress method* introduced in Section 2.2.4. Advantage of a part count prediction is the great simplicity, but its usefulness is often limited to specific applications.

2.3 Reliability of Systems with Complex Structure

Complex structures arise in many applications, e. g. in power, telecommunications, defense, and aerospace systems. In the context of this book, a structure is *complex*

when the reliability block diagram either cannot be reduced to a series-parallel structure with independent elements or does not exist.

For instance, a reliability block diagram does not exist if more than two states (good / failed) or one failure mode (e. g. short or open) must be considered for an element. Moreover, the reduction of a reliability block diagram to a series - parallel structure with independent elements is in general not possible with distributed (meshed) structures or when elements appear in the diagram more than once (cases 7-9 in Tab. 2.1). The term *independent elements* refers to *independence up to the system failure*, in particular *without load sharing* between redundant elements (see Section 2.3.5 and Chapter 6 for load sharing). For comparative investigations in Chapter 6, the term *totally independent elements* will be used to indicate *independence with respect to operation and repair* (each element in the reliability block diagram operates and fails *independently* from every other element and has its own repair crew).

Analysis of complex structures can become time-consuming. However, methods are well developed, should the reliability block diagram exist and the system satisfy:

1. Only active (parallel) redundancy is considered.
2. Elements can appear more than once in the reliability block diagram, but different elements are independent (totally independent for Eq. (2.48)).
3. On / off operations are either 100% reliable, or their effect has been considered in the reliability block diagram according to the above restrictions.

Under these assumptions, analysis can be performed using Boolean models. However, for practical applications, simple heuristically oriented methods apply well. *Heuristic methods* are given in Sections 2.3.1-2.3.3, *Boolean models* in Section 2.3.4.

Section 2.3.5 deals then with *warm redundancy*, allowing for *load sharing*. Section 2.3.6 considers elements with *two failure modes*. Stress / strength analysis are discussed in Section 2.5. Further aspects, as well as situations in which the reliability block diagram does not exist, are considered in Section 6.8 (see also Section 6.9 for an introduction to BDD, dynamic FT, Petri nets & computer-aided analysis).

As in Section 2.2.6 and Chapter 6, reliability figures have the indices S_i , where S stands for *system* and i for the *state entered at $t=0$* ($i=0$ for *system new*).

2.3.1 Key Item Method

The *key item method* is based on the theorem of *total probability* (Eq. (A6.17)). Assuming the item (system) new at $t=0$, the event {item operates failure free in $(0, t]$ | system new at $t=0$ }, or {system up in $(0, t]$ | system new at $t=0$ }, can be split

into the following two complementary events (p. 414)

$$\{ (\text{Element } E_i \text{ up in } (0, t] \cap \text{system up in } (0, t]) \mid \text{system new at } t=0 \}$$

and

$$\{ (\text{Element } E_i \text{ fails in } (0, t] \cap \text{system up in } (0, t]) \mid \text{system new at } t=0 \}.$$

From this it follows (Example A7.2, p. 481) that, for the *reliability function* $R_{S_0}(t)$,

$$R_{S_0}(t) = R_i(t) \Pr\{\text{system up in } (0, t] \mid (E_i \text{ up in } (0, t] \cap \text{system new at } t=0)\} + (1 - R_i(t)) \Pr\{\text{system up in } (0, t] \mid (E_i \text{ failed in } (0, t] \cap \text{system new at } t=0)\}, \tag{2.29}$$

where $R_i(t) = \Pr\{E_i \text{ up in } (0, t] \mid \text{system new at } t=0\} = \Pr\{E_i \text{ up in } (0, t] \mid E_i \text{ new at } t=0\}$ as in Eq. (2.16). Element E_i must be chosen in such a way that a series-parallel structure is obtained for the reliability block diagrams conditioned by the events $\{E_i \text{ up in } (0, t]\}$ and $\{E_i \text{ failed in } (0, t]\}$. Successive application of Eq. (2.29) is also possible (Examples 2.9 and 2.14). Sections 2.3.1.1 and 2.3.1.2 present two typical situations. In the context of Boolean functions, the above decomposition is known as a *Shannon decomposition* (Eq. (2.38)) and leads in particular to *binary decision diagrams* (Section 6.9.3).

2.3.1.1 Bridge Structure

The reliability block diagram of a *bridge structure* with a bi-directional connection is shown in Fig. 2.10 (row 7 in Table 2.1). Element E_5 can work with respect to the required function in *both directions*, from E_1 via E_5 to E_4 and from E_2 via E_5 to E_3 . It is therefore in a *key position* (key element). This property is used to calculate the reliability function by means of Eq. (2.29) with $E_i = E_5$. For the conditional probabilities in Eq. (2.29), the corresponding reliability block diagrams are



From Eq. (2.29), it follows that (with $R_S = R_{S_0}(t)$, $R_i = R_i(t)$, and $R_i(0) = 1, i = 1, \dots, 5$)

$$R_S = R_5(R_1 + R_2 - R_1 R_2)(R_3 + R_4 - R_3 R_4) + (1 - R_5)(R_1 R_3 + R_2 R_4 - R_1 R_2 R_3 R_4). \tag{2.30}$$

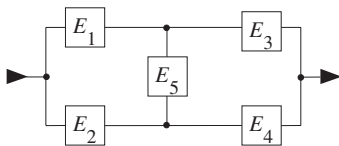


Figure 2.10 Reliability block diagram for a *bridge circuit* with a *bi-directional connection* on E_5

Same considerations apply to the bridge structure with a directed connection (row 8 in Table 2.1). Here, E_i must be $E_1, E_2, E_3,$ or E_4 (preferably E_1 or E_4), yielding

$$R_S = R_4 [R_2 + R_1(R_3 + R_5 - R_3R_5) - R_2R_1(R_3 + R_5 - R_3R_5)] + (1 - R_4)R_1R_3, \quad (2.31)$$

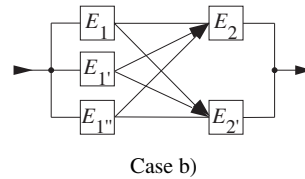
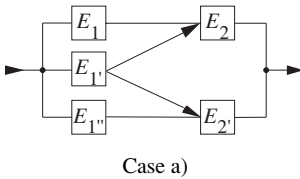
when choosing $E_i = E_4$, and to the same result

$$R_S = R_1 [R_3 + R_4(R_2 + R_5 - R_2R_5) - R_3R_4(R_2 + R_5 - R_2R_5)] + (1 - R_1)R_2R_4,$$

when choosing E_1 . Example 2.7 shows a further application of the key item method.

Example 2.7

Give the reliability of the item according to case a) below. How much would the reliability be improved if the structure were modified according to case b)? (Assumptions: nonrepairable up to system failure, active redundancy, independent elements, $R_{E_1}(t) = R_{E_1'}(t) = R_{E_1''}(t) = R_1(t)$ and $R_{E_2}(t) = R_{E_2'}(t) = R_2(t)$).



Solution

Element E_1 is in a key position in case a). Thus, similarly to Eq. (2.30), one obtains $R_a = R_1(2R_2 - R_2^2) + (1 - R_1)(2R_1R_2 - R_1^2R_2^2)$ with $R_a = R_{0a}(t)$, $R_i = R_i(t)$, $R_i(0) = 1$, $i = 1, 2$. Case b) represents a series connection of a 1-out-of-3 redundancy with a 1-out-of-2 redundancy. From Sections 2.2.6.3 and 2.2.6.4 it follows that $R_b = R_1R_2(3 - 3R_1 + R_1^2)(2 - R_2)$, with $R_b = R_{0b}(t)$, $R_i = R_i(t)$, $R_i(0) = 1$, $i = 1, 2$. From this,

$$R_b - R_a = 2R_1R_2(1 - R_2)(1 - R_1)^2. \quad (2.32)$$

The difference $R_b - R_a$ reaches as maximum the value $2/27$ for $R_1 = 1/3$ and $R_2 = 1/2$, i.e. $R_b = 57/108$ and $R_a = 49/108$ ($R_b - R_a = 0$ for $R_1 = 0, R_1 = 1, R_2 = 0, R_2 = 1$); the advantage of case b) is small, as far as reliability is concerned.

2.3.1.2 Reliability Block Diagram in Which at Least One Element Appears More than Once

In practice, situations often occur in which an element appears more than once in the reliability block diagram, although, physically, there is only one such element in the system considered. These situations can be investigated with the *key item method* introduced in Section 2.3.1.1, see Examples 2.8, 2.9, and 2.14.

Example 2.8

Give the reliability for the equipment introduced in Example 2.2 (p. 30).

Solution

In the reliability block diagram of Example 2.2, element E_2 is in a key position. Similarly to Eq. (2.30) it follows that

$$R_S = R_2 R_1 (R_4 + R_5 - R_4 R_5) + (1 - R_2) R_1 R_3 R_5, \quad (2.33)$$

with $R_S = R_{S0}(t)$ and $R_i = R_i(t)$, $R_i(0) = 1$, $i = 1, \dots, 5$.

Example 2.9

Give the reliability for the redundant circuit of Example 2.3 (p. 32).

Solution

In the reliability block diagram of Example 2.3, U_1 and U_2 are in a key position. Using the method introduced in Section 2.3.1 successively on U_1 and U_2 , i. e. on E_5 and E_6 , yields.

$$R_S = R_9 [R_5 [R_6 (R_1 R_7 + R_4 R_8 - R_1 R_4 R_7 R_8) (R_2 + R_3 - R_2 R_3) + (1 - R_6) R_1 R_2 R_7] \\ + (1 - R_5) R_3 R_4 R_6 R_8].$$

With $R_1 = R_2 = R_3 = R_4 = R_D$, $R_5 = R_6 = R_U$, $R_7 = R_8 = R_I$, $R_9 = R_{II}$ it follows that

$$R_S = R_U R_{II} [R_U (2 R_D R_1 - R_D^2 R_1^2) (2 R_D - R_D^2) + 2(1 - R_U) R_D^2 R_1], \quad (2.34)$$

with $R_S = R_{S0}(t)$, $R_U = R_U(t)$, $R_D = R_D(t)$, $R_I = R_I(t)$, $R_{II} = R_{II}(t)$, $R_i(0) = 1$ ($i = 1, \dots, 9$).

2.3.2 Successful Path Method

In this and in the next section, two general (closely related) methods are introduced. For simplicity, considerations will be based on the reliability block diagram given in Fig. 2.11. As in Section 2.2.6.1, e_i stands for the *event*

$$\{ \text{element } E_i \text{ up in the interval } (0, t] \mid \text{new at } t=0 \},$$

hence $\Pr\{e_i\} = R_i(t)$ with $R_i(0) = 1$, as in Eq. (2.16), and $\Pr\{\bar{e}_i\} = 1 - R_i(t)$. The *successful path method* is based on the following concept:

The system fulfills its required function if there is at least one path between the input and the output upon which all elements perform their required function.

Paths must lead from left to right and may not contain any loops. Only the given direction is possible along a directed connection. The following successful paths exist in the reliability block diagram of Fig. 2.11

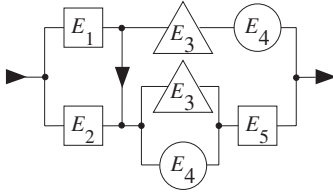


Figure 2.11 Reliability block diagram of a *complex structure* (elements E_3 and E_4 appear each twice in the RBD, the directed connection has reliability 1)

$$e_1 \cap e_3 \cap e_4, \quad e_1 \cap e_3 \cap e_5, \quad e_1 \cap e_4 \cap e_5, \quad e_2 \cap e_3 \cap e_5, \quad e_2 \cap e_4 \cap e_5.$$

Consequently it follows that

$$R_{S_0}(t) = \Pr\{(e_1 \cap e_3 \cap e_4) \cup (e_1 \cap e_3 \cap e_5) \cup (e_1 \cap e_4 \cap e_5) \cup (e_2 \cap e_3 \cap e_5) \cup (e_2 \cap e_4 \cap e_5)\};$$

from which, using the addition theorem of probability theory (Eqs. (A6.14), (A6.15)),

$$R_S = R_1 R_3 R_4 + R_1 R_3 R_5 + R_1 R_4 R_5 + R_2 R_3 R_5 + R_2 R_4 R_5 - 2 R_1 R_3 R_4 R_5 - R_1 R_2 R_3 R_5 - R_1 R_2 R_4 R_5 - R_2 R_3 R_4 R_5 + R_1 R_2 R_3 R_4 R_5, \quad (2.35)$$

with $R_S = R_{S_0}(t)$, $R_i = R_i(t)$, and $R_i(0) = 1$, $i = 1, \dots, 5$. Equation (2.35) follows also (directly) using the key item method (Section 2.3.1) successively on E_3 and E_5 ($R_S = R_3[R_5(R_1 + R_2 - R_1 R_2) + (1 - R_5) R_1 R_4] + (1 - R_3) R_4 R_5(R_1 + R_2 - R_1 R_2)$).

2.3.3 State Space Method

This method is based on the following concept:

To each element E_i is assigned an indicator (binary process) $\zeta_i(t)$ with the following property: $\zeta_i(t) = 1$ as long as E_i does not fail, and $\zeta_i(t) = 0$ if E_i has failed ($\zeta_i(0) = 1$). For any given (fixed) $t \geq 0$, the vector with components $\zeta_i(t)$ determines the system state. Since each element in the interval $(0, t]$ functions or fails independently of the others, 2^n states are possible for an item with n elements. After listing the 2^n possible states at time t , all those states are determined in which the system performs the required function. The probability that the system is in one of these states is the reliability function $R_{S_0}(t)$ of the system considered (with $R_{S_0}(0) = 1$).

The 2^n possible conditions at time t for the reliability block diagram of Fig. 2.11 are

E_1	1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
E_2	1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0
E_3	1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0
E_4	1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
E_5	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
S	1 1 1 0 1 1 1 0 1 1 1 0 0 0 0 0 1 0 1 0

A "1" in this table means that the element or item considered has not failed in $(0, t]$ (see footnote on p. 58 for fault tree analysis). For Fig. 2.11, the event

{ system *up* in the interval $(0, t]$ | new at $t=0$ }

is equivalent to the event

$$\begin{aligned} & \{ (e_1 \cap e_2 \cap e_3 \cap e_4 \cap e_5) \cup (\bar{e}_1 \cap e_2 \cap e_3 \cap e_4 \cap e_5) \cup (e_1 \cap \bar{e}_2 \cap e_3 \cap e_4 \cap e_5) \\ & \cup (e_1 \cap e_2 \cap \bar{e}_3 \cap e_4 \cap e_5) \cup (\bar{e}_1 \cap e_2 \cap \bar{e}_3 \cap e_4 \cap e_5) \cup (e_1 \cap \bar{e}_2 \cap \bar{e}_3 \cap e_4 \cap e_5) \\ & \cup (e_1 \cap e_2 \cap e_3 \cap \bar{e}_4 \cap e_5) \cup (\bar{e}_1 \cap e_2 \cap e_3 \cap \bar{e}_4 \cap e_5) \cup (e_1 \cap \bar{e}_2 \cap e_3 \cap \bar{e}_4 \cap e_5) \\ & \cup (e_1 \cap e_2 \cap e_3 \cap e_4 \cap \bar{e}_5) \cup (e_1 \cap \bar{e}_2 \cap e_3 \cap e_4 \cap \bar{e}_5) \}. \end{aligned}$$

After appropriate simplification, this reduces to

$$\begin{aligned} & \{ (e_2 \cap e_3 \cap e_5) \cup (e_1 \cap e_3 \cap e_4 \cap \bar{e}_5) \cup (e_1 \cap \bar{e}_2 \cap e_3 \cap \bar{e}_4 \cap e_5) \\ & \cup (e_1 \cap \bar{e}_2 \cap e_4 \cap e_5) \cup (e_2 \cap \bar{e}_3 \cap e_4 \cap e_5) \}, \end{aligned}$$

from which

$$R_{S0}(t) = \Pr\{ (e_2 \cap e_3 \cap e_5) \cup (e_1 \cap e_3 \cap e_4 \cap \bar{e}_5) \cup (e_1 \cap \bar{e}_2 \cap e_3 \cap \bar{e}_4 \cap e_5) \cup (e_1 \cap \bar{e}_2 \cap e_4 \cap e_5) \cup (e_2 \cap \bar{e}_3 \cap e_4 \cap e_5) \}. \quad (2.36)$$

Evaluation of Eq. (2.36) leads to Eq. (2.35). Note that all events in the state space method (columns in state space table & terms in Eq. (2.36)) are *mutually exclusive*.

2.3.4 Boolean Function Method

The *Boolean function method* generalizes & formalizes the methods based on the reliability block diagram (Section 2.2) and those introduced in Sections 2.3.1 - 2.3.3. For this analysis, besides the 3 assumptions given on p. 52, it is supposed that the system considered is *coherent* (see Eq. (2.37) for a definition); i. e., basically, that the state of the system depends on the states of all of its elements and the structure function (Eq. (2.37)) is monotone (implying in particular, that for a system down no additional failure of any element can bring it in an up state and, for a repairable system, if the system is up it remains up if any element is repaired). Almost all systems in practical applications are coherent. In the following, *up* is used for *system in operating state* and *down* for *system in a failed state* (in repair if repairable).

A system is *coherent* if its state can be described by a *structure function* ϕ

$$\phi = \phi(\zeta_1, \dots, \zeta_n) = \begin{cases} 1 & \text{for system up} \\ 0 & \text{for system down}^{\ast}) \end{cases} \quad (2.37)$$

of the *indicators* (binary processes) $\zeta_i = \zeta_i(t)$, defined in Section 2.3.3⁺⁺⁾ ($\zeta_i = 1$ if element E_i is *up* and $\zeta_i = 0$ if element E_i is *down*), for which the following applies:

1. ϕ depends on all the variables ζ_i ($i = 1, \dots, n$).
2. ϕ is non decreasing in all variables (with $\phi = 0$ for all $\zeta_i = 0$, $\phi = 1$ for all $\zeta_i = 1$).

ϕ is a Boolean function and can thus be written as (Shannon decomposition)

$$\begin{aligned} \phi(\zeta_1, \dots, \zeta_n) &= \zeta_i \phi(\zeta_1, \dots, \zeta_{i-1}, 1, \zeta_{i+1}, \dots, \zeta_n) \\ &\quad + (1 - \zeta_i) \phi(\zeta_1, \dots, \zeta_{i-1}, 0, \zeta_{i+1}, \dots, \zeta_n), \quad i = 1, \dots, n. \end{aligned} \quad (2.38)$$

Equation (2.38) is similar to Eq. (2.29). Successive Shannon's decompositions leads to *Binary Decision Diagrams* (BDD), see Section 6.9.3.

Since the indicators ζ_i and the structure function ϕ take only values 0 and 1, it follows that $E[\zeta_i(t)] = 1 \cdot \Pr\{\zeta_i(t) = 1\} + 0 \cdot \Pr\{\zeta_i(t) = 0\} = \Pr\{\zeta_i(t) = 1\}$; thus,

$$R_i(t) = \Pr\{\zeta_i(t) = 1\} = E[\zeta_i(t)], \quad R_i(0) = 1, \quad i = 1, \dots, n, \quad (2.39)$$

applies for the *reliability function* $R_i(t)$ of element E_i ⁺⁺⁾, and

$$R_{S_0}(t) = \Pr\{\phi(\zeta_1(t), \dots, \zeta_n(t)) = 1\} = E[\phi(\zeta_1(t), \dots, \zeta_n(t))], \quad R_{S_0}(0) = 1, \quad (2.40)$$

applies for the *reliability function* $R_{S_0}(t)$ of the system (calculation of $E[\phi]$ is often easier than calculation of $\Pr\{\phi = 1\}$).

The Boolean function method transfers thus the problem of calculating $R_{S_0}(t)$ to that of the determination of the structure function $\phi(\zeta_1, \dots, \zeta_n)$. Two methods with a great intuitive appeal are available for this purpose (for coherent systems):

1. *Minimal Path Sets* approach: A set \mathcal{P}_i of elements is a *minimal path set* if the system is up when $\zeta_j = 1$ for all $E_j \in \mathcal{P}_i$ and $\zeta_k = 0$ for all $E_k \notin \mathcal{P}_i$, but this does not apply for any subset of \mathcal{P}_i (for the bridge in Fig. 2.10, $\{1,3\}$, $\{2,4\}$, $\{1,5,4\}$, and $\{2,5,3\}$ are the minimal path sets). The elements E_j within \mathcal{P}_i form a *series model* with structure function

$$\phi_{\mathcal{P}_i} = \prod_{E_j \in \mathcal{P}_i} \zeta_j. \quad (2.41)$$

If for a given system there are r minimal path sets, these form an *active 1-out-of- r redundancy*, yielding (see also Eq. (2.24))

^{*)} In fault tree analysis (FTA), "0" for up and "1" for down is often used [A2.6 (IEC 61025)].

⁺⁺⁾ No distinction is made here between *Boolean random variable* ζ_i and *Boolean variable* (realization of ζ_i); equations with $\zeta_i(t)$, $R_i(t)$, $R_{S_0}(t)$ are intended to apply for every given (fixed) $t \geq 0$; considering that each ζ_i takes values 0 & 1 and appears only in linear form, addition, subtraction & multiplication can be used (in particular $\zeta_i \zeta_j \equiv \zeta_i \wedge \zeta_j$, $1 - (1 - \zeta_i)(1 - \zeta_j) \equiv \zeta_i \vee \zeta_j$, $1 - \zeta_i \equiv \bar{\zeta}_i$).

$$\phi = \phi(\zeta_1, \dots, \zeta_n) = 1 - \prod_{i=1}^r (1 - \phi_{\mathcal{P}_i}) = 1 - \prod_{i=1}^r (1 - \prod_{E_j \in \mathcal{P}_i} \zeta_j). \quad (2.42)$$

2. *Minimal Cut Sets* approach: A set C_i is a *minimal cut set* if the system is down when $\zeta_j = 0$ for all $E_j \in C_i$ and $\zeta_k = 1$ for all $E_k \notin C_i$, but this does not apply for any subset of C_i (for the bridge in Fig. 2.10, $\{1,2\}$, $\{3,4\}$, $\{1,5,4\}$, and $\{3,5,2\}$ are the minimal cut sets). The elements E_j within C_i form a *parallel model* (*active redundancy with $k=1$*) with structure function (Eq. (2.24))

$$\phi_{C_i} = 1 - \prod_{E_j \in C_i} (1 - \zeta_j). \quad (2.43)$$

If for a given system there are m minimal cut sets, these form a *series model*, yielding (see also Eq. (2.17))

$$\phi = \phi(\zeta_1, \dots, \zeta_n) = \prod_{i=1}^m \phi_{C_i} = \prod_{i=1}^m (1 - \prod_{E_j \in C_i} (1 - \zeta_j)). \quad (2.44)$$

A series model with elements E_1, \dots, E_n has one path set and n cut sets, a parallel model (1-out-of- n) has one cut set and n path sets. Algorithms for finding all minimal path sets and all minimal cut sets are known, see e.g. [2.33, 2.34 (1975)].

For coherent *nonrepairable systems* (up to system failure) with structure function $\phi(\zeta_1, \dots, \zeta_n)$ per Eq. (2.42) or (2.44), the reliability function $R_{S_0}(t)$ follows (for any given (fixed) $t > 0$, $R_{S_0}(0)=1$) from Eq. (2.40) or directly from

$$R_{S_0}(t) = \Pr\{\phi_{\mathcal{P}_1} = 1 \cup \dots \cup \phi_{\mathcal{P}_r} = 1\} = 1 - \Pr\{\phi_{C_1} = 0 \cup \dots \cup \phi_{C_m} = 0\}. \quad (2.45)$$

Equation (2.45) has a great intuitive appeal. For practical applications, the following bounds on the reliability function $R_{S_0}(t)$ can often be used [2.34 (1975)]

$$\prod_{i=1}^m \Pr\{\phi_{C_i} = 1\} \leq R_{S_0}(t) \leq 1 - \prod_{i=1}^r \Pr\{\phi_{\mathcal{P}_i} = 0\}. \quad (2.46)$$

If the minimal path sets have no common elements, the right-hand inequality of Eq. (2.46) becomes an equality, similar is for the minimal cut sets (left-hand inequality).

For coherent *nonrepairable systems* (up to system failure) with *independent elements*, the reliability function $R_{S_0}(t)$ can also be obtained, considering $\zeta_i \zeta_i = \zeta_i$,

directly from the structure function $\phi(\zeta_1, \dots, \zeta_n)$ given by Eqs. (2.42) or (2.44), by substituting $R_i(t)$ for ζ_i (Eqs. (2.39), (2.40), (A6.68), (A6.69)).

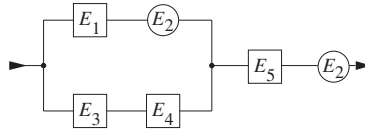
Also it is possible to use the *disjunctive normal form* $\phi_D(\zeta_1, \dots, \zeta_n)$ or *conjunctive normal form* $\phi_L(\zeta_1, \dots, \zeta_n)$ of the structure function $\phi(\zeta_1, \dots, \zeta_n)$, yielding

$$R_{S_0}(t) = \phi_D(R_1, \dots, R_n) = \phi_L(R_1, \dots, R_n), \quad R_i = R_i(t), R_i(0)=1, i=1, \dots, n. \quad (2.47)$$

The path sets given on p. 56 are the minimal path sets for the reliability block diagram of Fig. 2.11. Equation (2.35) follows then from Eq. (2.40), using Eq. (2.42) for $\phi(\zeta_1, \dots, \zeta_5) = 1 - (1 - \zeta_1 \zeta_3 \zeta_4)(1 - \zeta_1 \zeta_3 \zeta_5)(1 - \zeta_1 \zeta_4 \zeta_5)(1 - \zeta_2 \zeta_3 \zeta_5)(1 - \zeta_2 \zeta_4 \zeta_5)$, simplified by considering $\zeta_i \zeta_i = \zeta_i$, and substituting $R_i(t)$ for ζ_i in the final $\phi(\zeta_1, \dots, \zeta_5)$, see also the footnote on p. 58. Investigation of the block diagram of Fig. 2.11 by the method of minimal cut sets is more laborious. Obviously, minimal path sets and minimal cut sets deliver the same structure function, with different effort depending on the structure of the reliability block diagram considered (structures with many series elements can be treated easily with minimal path sets).

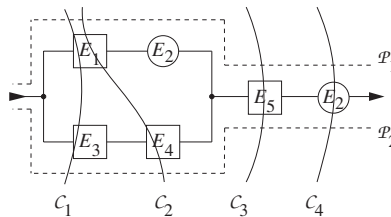
Example 2.10

Give the structure function according to the minimal path sets and the minimal cut sets approach for the following reliability block diagram, and calculate the reliability function assuming independent elements and active redundancies.



Solution

For the above reliability block diagram, there exist 2 minimal path sets $\mathcal{P}_1, \mathcal{P}_2$ and 4 minimal cut sets C_1, \dots, C_4 , as given below.



The structure function follows then from Eq. (2.42) for the minimal path sets

$$\phi(\zeta_1, \dots, \zeta_5) = 1 - (1 - \zeta_1 \zeta_2 \zeta_5)(1 - \zeta_2 \zeta_3 \zeta_4 \zeta_5) = \zeta_1 \zeta_2 \zeta_5 + \zeta_2 \zeta_3 \zeta_4 \zeta_5 - \zeta_1 \zeta_2 \zeta_3 \zeta_4 \zeta_5$$

or from Eq. (2.44) for the minimal cut sets (in both cases by considering $\zeta_i \zeta_i = \zeta_i, \zeta_i \zeta_j = \zeta_j \zeta_i$)

$$\begin{aligned} \phi(\zeta_1, \dots, \zeta_5) &= [1 - (1 - \zeta_1)(1 - \zeta_3)][1 - (1 - \zeta_1)(1 - \zeta_4)][1 - (1 - \zeta_5)][1 - (1 - \zeta_2)] \\ &= (\zeta_1 + \zeta_3 - \zeta_1 \zeta_3)(\zeta_1 + \zeta_4 - \zeta_1 \zeta_4)\zeta_2 \zeta_5 \\ &= \zeta_1 \zeta_2 \zeta_5 + \zeta_2 \zeta_3 \zeta_4 \zeta_5 - \zeta_1 \zeta_2 \zeta_3 \zeta_4 \zeta_5. \end{aligned}$$

Assuming independence for the (different) elements, it follows for the reliability function (for both cases and with $R_S = R_{S_0}(t), R_i = R_i(t)$, and $R_i(0) = 1, i = 1, \dots, 5$)

$$R_S = R_1 R_2 R_5 + R_2 R_3 R_4 R_5 - R_1 R_2 R_3 R_4 R_5.$$

Supplementary results: Calculation with the key item method leads directly to

$$R_S = R_2 (R_1 + R_3 R_4 - R_1 R_3 R_4) R_5 + (1 - R_2) \cdot 0.$$

For *coherent repairable systems* with elements which are *as-good-as-new* after repair and *totally independent* (every element operates and is repaired independently from each other element, i. e., has its own repair crew and continues operation during the repair of a failed element), expressions for $R_{S0}(t)$ can be used to calculate the *point availability* $PA_{S0}(t)$, substituting $R_i(t)$ with $PA_{i0}(t)$. For Eq. (2.47) this leads to

$$PA_{S0}(t) = \Phi_D(PA_1, \dots, PA_n) = \Phi_L(PA_1, \dots, PA_n), \tag{2.48}$$

with $PA_i = PA_{i0}(t)$ for the general case (Eq. (6.17)) or $PA_i = MTTF_i / (MTTF_i + MTTR_i)$ for steady-state or $t \rightarrow \infty$ (Eq. (6.48)). However, in practical applications, a repair crew for each element in the reliability block diagram of a system is not available and, except for redundant elements, not failed elements often stop to operate during the repair of a failed element. Nevertheless, Eq.(2.48) can be used as an *approximation* (upper bound) for $PA_{S0}(t)$. For *repairable* elements, the indicator (binary process) $\zeta_i(t)$ given in Section 2.3.3 alternates between $\zeta_i(t)=1$ for element E_i *operating* (up) and $\zeta_i(t)=0$ for E_i *in repair* (down), yielding $E[\zeta_i(t)] = PA_{i0}(t)$. In practical applications, it is often preferable to compute $1 - PA_{S0}(t)$.

2.3.5 Parallel Models with Const. Failure Rates & Load Sharing

In the redundancy structures investigated in the previous sections, all elements were operating under the same conditions. For this type of redundancy, called *active* (parallel) *redundancy*, the assumed statistical independence of the elements implies, in particular, that there is *no load sharing*. This assumption does not arise in many practical applications, for example, at component level or in the presence of power elements. The investigation of the reliability function in the case of load sharing or of other kinds of dependency involves the use of *stochastic processes*. The situation is simple if one can assume that *the failure rate of each element can change only when a failure occurs*. In this case, the general model for a *k-out-of-n redundancy* is a *death process* as given in Fig. 2.12 (birth and death process as in Fig. 6.13 for the repairable case with constant failure & repair rates). Z_0, \dots, Z_{n-k+1} are the states of the process. In state Z_i , i elements are down. At state Z_{n-k+1} the system is down.

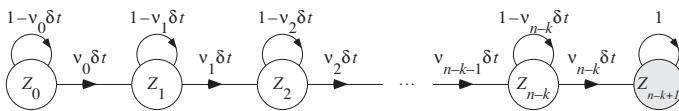


Figure 2.12 Diagram of the transition probabilities in $(t, t + \delta t]$ for a *k-out-of-n redundancy*, *nonrepairable*, *constant failure rates during the sojourn time in every state* (not necessarily at a state change), *ideal failure detection & switch*; t arbitrary, $\delta t \rightarrow 0$, Markov process, Z_{n-k+1} down state)

Assuming

$$\lambda = \text{failure rate of an element in the } \textit{operating state} \quad (2.49)$$

and

$$\lambda_r = \text{failure rate of an element in the } \textit{reserve state} \quad (\lambda_r \leq \lambda), \quad (2.50)$$

the model of Fig. 2.12 considers in particular the following cases:

1. Active redundancy without load sharing (independent elements)

$$v_i = (n - i) \lambda, \quad i = 0, \dots, n - k, \quad (2.51)$$

λ is the same for all states.

2. Active redundancy with *load sharing* ($\lambda = \lambda(i)$)

$$v_i = (n - i) \lambda(i), \quad i = 0, \dots, n - k, \quad (2.52)$$

$\lambda(i)$ increases at each state change.

3. Warm (lightly loaded) redundancy ($\lambda_r < \lambda$)

$$v_i = k \lambda + (n - k - i) \lambda_r, \quad i = 0, \dots, n - k, \quad (2.53)$$

λ and λ_r are the same for all states.

4. Standby (cold) redundancy ($\lambda_r \equiv 0$)

$$v_i = k \lambda, \quad i = 0, \dots, n - k, \quad (2.54)$$

λ is the same for all states.

For a *standby redundancy*, it is assumed that the failure rate in the reserve state is $\equiv 0$ (the reserve elements are switched on when needed). *Warm redundancy* is somewhere between active and standby ($0 < \lambda_r < \lambda$). It should be noted that the *k-out-of-n* active, warm, or standby redundancy is only the *simplest* representatives of the general concept of redundancy. Series - parallel structures, voting techniques, bridges, and more complex structures are frequently used (see Sections 2.2.6, 2.3.1-2.3.4, and 6.6-6.8 with repair rate $\mu = 0$, for some examples). Furthermore, redundancy can also appear in other forms, e.g. at software level, and the benefit of redundancy can be limited by the involved *failure modes* as well as by *control and switching elements* (see Section 6.8 for some examples).

For the analysis of the model shown in Fig. 2.12, let

$$P_i(t) = \Pr\{\text{the process is in state } Z_i \text{ at time } t\} \quad (2.55)$$

be the *state probabilities* ($i = 0, \dots, n - k + 1$). $P_i(t)$ is obtained by considering the process at two adjacent time points t and $t + \delta t$ and by making use of the *memoryless property* resulting from the *constant failure rate assumed between consecutive state changes* (Appendix A7.5). The function $P_i(t)$ thus satisfies the following *difference equation*

$$P_i(t + \delta t) = P_i(t)(1 - v_i \delta t) + P_{i-1}(t)v_{i-1} \delta t + o(\delta t), \quad i = 1, \dots, n-k, \quad (2.56)$$

where $o(\delta t)$ denotes a quantity having an order higher than that of δt (Eq.(A7.89)). For $\delta t \rightarrow 0$, there follows a system of differential equations describing a *death process*

$$\begin{aligned} \dot{P}_0(t) &= -v_0 P_0(t) \\ \dot{P}_i(t) &= -v_i P_i(t) + v_{i-1} P_{i-1}(t), \quad i = 1, \dots, n-k, \\ \dot{P}_{n-k+1}(t) &= v_{n-k} P_{n-k}(t). \end{aligned} \quad (2.57)$$

Assuming the initial conditions $P_i(0) = 1$ and $P_j(0) = 0$ for $j \neq i$ at $t = 0$, the solution (generally obtained using the Laplace transform) leads to $P_i(t)$, $i = 0, \dots, n-k+1$. Knowing $P_i(t)$, one can evaluate the *reliability function* $R_S(t)$

$$R_S(t) = \sum_{i=0}^{n-k} P_i(t) = 1 - P_{n-k+1}(t) \quad (2.58)$$

and the *mean time to failure* from Eq. (2.9). Assuming, for instance. $P_0(0) = 1$ as initial condition, the Laplace transform of $R_{S0}(t)$,

$$\tilde{R}_{S0}(s) = \int_0^{\infty} R_{S0}(t) e^{-st} dt, \quad (2.59)$$

is given by (with $\tilde{P}_{n-k+1}(s)$ obtained recursively from Eq. (2.57))

$$\tilde{R}_{S0}(s) = \frac{(s + v_0) \dots (s + v_{n-k}) - v_0 \dots v_{n-k}}{s(s + v_0) \dots (s + v_{n-k})}. \quad (2.60)$$

The *mean time to failure* follows then from

$$MTTF_{S0} = \tilde{R}_{S0}(0), \quad (2.61)$$

yielding (using $dy/ds = y \cdot d(\ln y)/ds$ with $y = (s+v_0)\dots(s+v_{n-k})$ in the numerator)

$$MTTF_{S0} = \sum_{i=0}^{n-k} \frac{1}{v_i}. \quad (2.62)$$

Thereby, S stands for system and 0 specify the initial condition $P_0(0) = 1$ (Table 6.2).

A *k-out-of-n standby redundancy* (Eq. (2.54)) leads to (Tab. A9.7b, Eq. (A7.102))

$$R_{S0}(t) = \sum_{i=0}^{n-k} \frac{(k\lambda t)^i}{i!} e^{-k\lambda t} \quad (2.63)$$

and

$$MTTF_{S0} = \frac{n-k+1}{k\lambda}. \quad (2.64)$$

Equation (2.63) gives the probability for up to $n-k$ failures $(0, 1, \dots, n-k)$ in $(0, t]$ by constant failure rate $k\lambda$, and shows the relation existing between the *Poisson distribution* and the occurrence of *exponentially distributed events* (Appendix A7.2.5).

For the case of a k -out-of- n active redundancy without load sharing, it follows from Eqs. (2.62) and (2.51) that

$$MTTF_{S0} = \frac{1}{\lambda} \left(\frac{1}{k} + \dots + \frac{1}{n} \right), \quad (2.65)$$

see also Table 6.8 with $\mu = 0$, and $\lambda_r = \lambda$. Some examples for $R_{S0}(t)$ with different values for n and k are given in Fig. 2.7.

2.3.6 Elements with more than one Failure Mechanism or one Failure Mode

In the previous sections, it was assumed that each element exhibits only one dominant *failure mechanism*, causing one dominant *failure mode*; for example intermetallic compound causing a short, or corrosion causing an open, for integrated circuits. However, in practical applications, components can have some failure mechanisms and fail in different manner (see e.g. Table 3.4). A simple way to consider more than one failure mechanism is to *assume* that each failure mechanism is *independent* of each other and causes a failure at item level. In this case, a *series model* can be used by assigning a failure rate to each failure mechanism, and Eq. 2.18 or Eq. 7.57 delivers the total failure rate of the item considered. More sophisticated models are possible. A mixture of failure rates and /or mechanisms has been discussed in Section 2.2.5 (Eq. (2.15)). This section will consider as an example the case of a diode exhibiting two failure modes. Let

$$R(t) = \Pr\{\text{no failure in } (0, t] \mid \text{diode new at } t=0\}$$

$$\bar{R}(t) = 1 - R(t) = \Pr\{\text{failure in } (0, t] \mid \text{diode new at } t=0\}$$

$$\bar{R}_U(t) = \Pr\{\text{open in } (0, t] \mid \text{diode new at } t=0\}$$

$$\bar{R}_K(t) = \Pr\{\text{short in } (0, t] \mid \text{diode new at } t=0\}.$$

Obviously (Example 2.11)

$$1 - R(t) = \bar{R}(t) = \bar{R}_U(t) + \bar{R}_K(t). \quad \text{---} \blacktriangleright \text{---} \quad (2.66)$$

The series connection of two diodes exhibits a circuit failure if either one open or two shorts occur. From this,

$$\bar{R}_S = 1 - (1 - \bar{R}_U)^2 + \bar{R}_K^2 = 2\bar{R}_U - \bar{R}_U^2 + \bar{R}_K^2, \quad \text{---} \blacktriangleright \blacktriangleright \text{---} \quad (2.67)$$

with $R_S = R_{S0}(t)$, $\bar{R}_K = \bar{R}_K(t)$, $\bar{R}_U = \bar{R}_U(t)$.

Similarly, for two diodes in parallel (Example 2.12),

$$\bar{R}_S = 1 - (1 - \bar{R}_K)^2 + \bar{R}_U^2 = 2\bar{R}_K - \bar{R}_K^2 + \bar{R}_U^2. \quad \text{---} \circ \text{---} \begin{array}{c} \rightarrow \\ \rightarrow \end{array} \text{---} \circ \text{---} \quad (2.68)$$

To be *simultaneously* protected against at *least one* failure of *arbitrary mode* (short or open), a *quad redundancy* is necessary. Depending upon whether opens or shorts are more frequent, a quad redundancy with or without a bridge connection is used. For both these cases it follows that

$$\bar{R}_S = 2\bar{R}_U^2 - \bar{R}_U^4 + (2\bar{R}_K - \bar{R}_K^2)^2, \quad \text{---} \circ \text{---} \begin{array}{c} \rightarrow \bullet \rightarrow \\ \rightarrow \bullet \rightarrow \end{array} \text{---} \circ \text{---} \quad (2.69)$$

and

$$\bar{R}_S = 2\bar{R}_K^2 - \bar{R}_K^4 + (2\bar{R}_U - \bar{R}_U^2)^2. \quad \text{---} \circ \text{---} \begin{array}{c} \rightarrow \bullet \rightarrow \\ \rightarrow \bullet \rightarrow \end{array} \text{---} \circ \text{---} \quad (2.70)$$

Equations (2.67) to (2.70) can be obtained using the *state space method* introduced in Section 2.3.3, however with *three states* for every element (good, open (U), and short (K)) leading to a *state space* with 3^n elements in each line, see Example 2.12).

Equations (2.67) and (2.68) yield for n diodes, $\bar{R}_S = 1 - (1 - \bar{R}_U)^n + \bar{R}_K^n$ and $\bar{R}_S = 1 - (1 - \bar{R}_K)^n + \bar{R}_U^n$, respectively.

Example 2.11

In an accelerated test of 1000 diodes, 100 failures occur, of which 30 are opens and 70 shorts. Give an estimate for \bar{R} , \bar{R}_U , and \bar{R}_K .

Solution

The maximum likelihood estimate of an unknown probability p is, according to Eq. (A8.29), $\hat{p} = k/n$. Hence, $\hat{\bar{R}} = 0.1$, $\hat{\bar{R}}_U = 0.03$, and $\hat{\bar{R}}_K = 0.07$.

Example 2.12

Using the state space method, give the reliability of two parallel connected diodes, assuming that opens and shorts are possible.

Solution

Considering the three possible states (good (1), open (U), and short (K)), the state space for two parallel connected diodes is

D_1	1	1	1	U	U	U	K	K	K
D_2	1	U	K	1	U	K	1	U	K
S	1	1	0	1	0	0	0	0	0

From the above table, it follows that

$$\begin{aligned} \bar{R}_S &= \Pr\{S = 0\} = 2R\bar{R}_K + \bar{R}_U^2 + 2\bar{R}_U\bar{R}_K + \bar{R}_K^2 \\ &= 2(1 - \bar{R}_U - \bar{R}_K)\bar{R}_K + \bar{R}_U^2 + 2\bar{R}_U\bar{R}_K + \bar{R}_K^2 = 2\bar{R}_K - \bar{R}_K^2 + \bar{R}_U^2. \end{aligned}$$

The linear superposition of the two failure modes, appearing in the final result for \bar{R}_S , do not apply necessarily to arbitrary structures.

2.3.7 Basic Considerations on Fault Tolerant Structures

In applications with *high reliability, availability or safety requirements*, items must be *designed* to be *fault tolerant* at components level (see e.g. pp. 51, 64-65), and/or *fault tolerant reconfigurable* at equipment and systems level. This means that at system level, the item considered should be able to *recognize a fault* (failure or defect) and quickly *reconfigure* itself in such a way as to remain *safe* and possibly continue to operate with minimal performance loss (*fail-safe, graceful degradation*).

Methods to investigate *fault tolerant* items have been introduced in Sections 2.2.6.2 through 2.3.6, in particular Sections 2.2.6.5 (*majority redundancy*) and 2.3.6 (*quad redundancy*). The latter is one of the few structures which can support *at least one failure of any mode*, the price paid is four devices instead of one. Other possibilities are known to implement fault tolerance at components level, e.g. [2.41].

Repairable fault tolerant reconfigurable systems are considered carefully in Chapter 6, in particular Section 6.8 for *non ideal reconfiguration* (imperfect switching, incomplete coverage, a.o.). It is shown, that the stochastic processes introduced in Appendix A7 can be used to investigate reliability and availability of *fault tolerant systems* for cases in which a reliability block diagram does not exist as well.

To avoid *common cause* or *single-point failures*, redundant elements should be designed and produced *independently* from each other, in critical cases with different technology, tools, and personnel. Investigation of all possible *failure (fault) modes* during the design of fault tolerant equipment and systems is mandatory. This is generally done using *failure modes and effects analysis* (FMEA /FMECA), *fault tree analysis* (FTA), *causes-to-effects diagrams* or similar tools (Sections 2.6 & 6.9), supported by appropriate investigation models (see e.g. Examples 6.15 & 6.17). Failure modes analysis is essential where *redundancy* appears, among other to identify the parts which are in series to the ideal redundancy (in the reliability block diagram), to discover *interactions* between elements of the given item, and to find appropriate measures to avoid *failure propagation* (secondary failures).

Protection against *secondary failures* can be realized, at component level, with *decoupling elements* such as diodes, resistors, capacitors (diodes $E_1 - E_4$ in Example 2.3). Other possibilities are the introduction of *standby elements* which are activated at failure of working elements, the use of basically different technologies for redundant elements, etc. As a general rule, all parts which are essential for basic functions (e.g. interfaces and monitoring circuitries) have to be designed with care. Adherence to appropriate *design guidelines* is important (Chapter 5). Detection and localization of *hidden failures* as well as avoidance of *false alarms* (caused e.g. by *synchronization problems*) is mandatory. These and similar considerations applies in particular for equipment and systems with high reliability and/or safety requirements, as used e.g. in aerospace, automotive, and nuclear applications.

In digital systems, fault tolerance can often be obtained using error correction techniques (see e.g.[4.22] for an application). Basic possibilities for redundancy in software are *N-version programming* and *N self configuring programming*.

2.4 Reliability Allocation and Optimization

With complex equipment and systems, it is important to allocate reliability goals at subsystem and assembly levels early in the design phase. Such an allocation motivates the design engineer to consider reliability aspects at all system levels.

Allocation is simple if the item (system) has no redundancy and its components have constant failure rates. The system's failure rate λ_S is then constant and equal to the sum of the failure rates of its elements (Eq. (2.19)). In such a case, the allocation of λ_S can be done as follows:

1. Break down the system into elements E_1, \dots, E_n .
2. Define a complexity factor k_i for each element ($0 \leq k_i \leq 1$, $k_1 + \dots + k_n = 1$).
3. Determine the *duty cycle* d_i for each element ($d_i = \text{operating time of element } E_i / \text{operating time of the system}$).
4. Allocate the system's failure rate λ_S among elements E_1, \dots, E_n according to

$$\lambda_i = \lambda_S k_i / d_i, \quad \lambda_S = \sum_i \lambda_i d_i. \quad (2.71)$$

Should all elements have the same complexity ($k_1 = \dots = k_n = 1/n$) and the same duty cycle ($d_1 = \dots = d_n = 1$), then $\lambda_i = \lambda_S / n$.

Often it is necessary to consider *cost aspects*. Assuming that for element E_i the cost relation to the failure rate is of the form $c_i = f_i(\lambda_i)$, e. g. $c_i = b_i / \lambda_i$, *cost optimization* ask for the minimization of $C = \sum_i c_i = \sum_i f_i(\lambda_i)$. For the case of a series system with elements E_1 and E_2 , this leads to take λ_1 as solution of

$$d(f_1(\lambda_1) + f_2(\lambda_S - \lambda_1)) / d\lambda_1 = 0$$

and λ_2 as $\lambda_2 = \lambda_S - \lambda_1$. For a series system with elements E_1, \dots, E_n , the method of the *Lagrange multiplier*, yielding $\lambda_1, \dots, \lambda_n$ as solution of the system of $n+1$ algebraic equations

$$\begin{cases} \lambda_S - \lambda_1 - \dots - \lambda_n = 0 \\ \frac{\partial \phi}{\partial \lambda_i} = 0, \quad i=1, \dots, n, \end{cases} \quad (2.72)$$

with $\phi(\lambda_1, \dots, \lambda_n, \alpha) = f_1(\lambda_1) + \dots + f_n(\lambda_n) + \alpha \cdot (\lambda_S - \lambda_1 - \dots - \lambda_n)$, or methods based on linear or nonlinear programming can be used, as necessary. For instance, Eq. (2.72) with $c_i = f_i(\lambda_i) = b_i / \lambda_i$ yields $\lambda_i = \lambda_S / (1 + \sum_{j \neq i} \sqrt{b_j / b_i})$, $i, j=1, \dots, n$.

Complexity and duty cycle can be integrated in $c_i = f_i(\lambda_i)$, considering also empirical data as well as aspects of technology risk and failure effect (consequence).

Should individual element failure rates not be constant and/or the system contain redundancy, allocation of reliability goals is more laborious, see e. g. [2.34(1965)]. In the case of *repairable series-parallel structures*, one can often assume that the failure rate at equipment and systems level is basically fixed by the series elements (Section 6.6, Example 4.2), and thus concentrate the allocation to these elements.

2.5 Mechanical Reliability, Drift Failures

As long as the reliability is considered to be the probability R for a mission success (without relation to the distribution of the failure-free time), the reliability *analysis procedure* for mechanical equipment and systems is similar to that used for electronic equipment and systems and is based on the following steps:

1. Definition of the system and of its associated mission profile.
2. Derivation of the corresponding reliability block diagram.
3. Determination of the reliability for each element of the reliability block diagram.
4. Calculation of the system reliability R_S (R_{S0} to point out system new at $t = 0$).
5. Elimination of reliability weaknesses and return to step 1 or 2, as necessary.

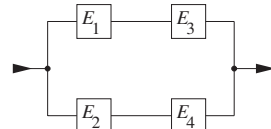
Such a procedure is currently used in practical applications and is illustrated by Examples 2.13 and 2.14.

Example 2.13

The fastening of two mechanical parts should be easy and reliable. It is done by means of two flanges which are pressed together with 4 clamps E_1 to E_4 placed 90° to each other. Experience has shown that the fastening holds when at least 2 opposing clamps work. Set up the reliability block diagram for this fixation and compute its reliability (each clamp is news at $t = 0$ and has reliability $R_1 = R_2 = R_3 = R_4 = R$).

Solution

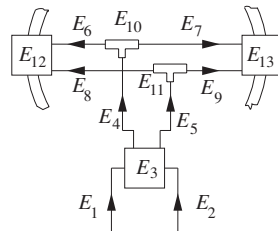
Since at least two opposing clamps (E_1 and E_3 or E_2 and E_4) have to function without failure, the reliability block diagram is obtained as the series connection of E_1 and E_3 in parallel with the series connection of E_2 and E_4 , see graph on the right. Under the assumption that clamp is independent from every other one, the item reliability follows from $R_{S0} = 2R^2 - R^4$.



Supplementary result: If two arbitrary clamps were sufficient for the required function, a 2-out-of-4 active redundancy would apply yielding (Tab. 2.1) $R_{S0} = 6R^2 - 8R^3 + 3R^4$.

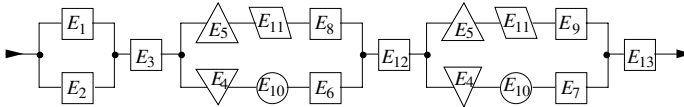
Example 2.14

To separate a satellite's protective shielding, a special electrical-pyrotechnic system described in the functional block diagram on the right is used. An electrical signal comes through the cables E_1 and E_2 (redundancy) to the electrical-pyrotechnic converter E_3 which lights the fuses. These carry the pyrotechnic signal to explosive charges for guillotining bolts E_{12} and E_{13} of the tensioning belt. The charges can be ignited from two sides, although one ignition will suffice (redundancy). For fulfillment of the required function, both bolts must be exploded simultaneously. Give the reliability of this separation system as a function of the reliability R_1, \dots, R_{13} of its elements (news at $t = 0$).



Solution

The reliability block diagram is easily obtained by considering first the ignition of bolts E_{12} & E_{13} separately and then connecting these two parts of the reliability block diagram in series.



Elements E_4 , E_5 , E_{10} , and E_{11} each appear twice in the reliability block diagram. Repeated application of the *key item method* (successively on E_5 , E_{11} , E_4 , and E_{10} , see Section 2.3.1 and Example 2.9), by assuming that the elements E_1, \dots, E_{13} are independent, leads to

$$\begin{aligned}
 R_{S0} &= R_3 R_{12} R_{13} (R_1 + R_2 - R_1 R_2) \{ R_5 \langle R_{11} [R_4 \{ R_{10} (R_6 + R_8 - R_6 R_8) (R_7 + R_9 - R_7 R_9) \\
 &\quad + (1 - R_{10}) R_8 R_9 \} + (1 - R_4) R_8 R_9 \rangle + (1 - R_{11}) R_4 R_6 R_7 R_{10} \rangle + (1 - R_5) R_4 R_6 R_7 R_{10} \} \\
 &= R_3 R_{12} R_{13} (R_1 + R_2 - R_1 R_2) \{ R_4 R_5 R_{10} R_{11} (R_6 + R_8 - R_6 R_8) (R_7 + R_9 - R_7 R_9) \\
 &\quad + (1 - R_4 R_{10}) R_5 R_8 R_9 R_{11} + (1 - R_5 R_{11}) R_4 R_6 R_7 R_{10} \}. \tag{2.73}
 \end{aligned}$$

More complicated is the situation when the reliability function $R(t)$ is required. For electronic components it is possible to operate with the failure rate, since models and data are often available. This is generally not the case for mechanical parts, although failure rate models for some parts and units (bearings, springs, couplings, etc.) have been developed [2.26, 2.27]. If no information about failure rates is available, a general approach based on the *stress-strength method*, often supported by *finite element analysis*, can be used. Let $\xi_L(t)$ be the *stress* (load) and $\xi_S(t)$ the *strength*, a failure occurs at the time t for which $|\xi_L(t)| > |\xi_S(t)|$ holds for the first time. Often, $\xi_L(t)$ and $\xi_S(t)$ can be considered as deterministic values and the ratio $\xi_S(t)/\xi_L(t)$ is the *safety factor*. In many practical applications, $\xi_L(t)$ and $\xi_S(t)$ are random variables, often stochastic processes. A practical oriented *procedure* for the reliability analysis of mechanical systems in these cases is:

1. Definition of the system and of its associated mission profile.
2. Formulation of *failure hypotheses* (buckling, bending, etc.) and validation of them using an FMEA/ FMECA (Section 2.6); failure hypotheses are often correlated, this dependence must be identified and considered.
3. Evaluation of the stresses applied with respect to the critical failure hypotheses.
4. Evaluation of the strength limits by considering also dynamic stresses, notches, surface condition, etc.
5. Calculation of the system reliability (Eqs. (2.74) – (2.80)).
6. Elimination of reliability weaknesses and return to step 1 or 2, as necessary.

Reliability calculation often leads to one of the following situations:

1. One failure hypothesis, stress & strength > 0 ; the *reliability function* is given by

$$R_{S0}(t) = \Pr\{\xi_S(x) > \xi_L(x), \quad 0 < x \leq t\}, \quad R_{S0}(0) = 1. \tag{2.74}$$

2. More than one ($n > 1$) failure hypothesis that can be correlated, stresses and strength > 0 ; the *reliability function* is given by

$$R_{S0}(t) = \Pr\{(\xi_{S1}(x) > \xi_{L1}(x)) \cap (\xi_{S2}(x) > \xi_{L2}(x)) \cap \dots \cap (\xi_{Sn}(x) > \xi_{Ln}(x)), \quad 0 < x \leq t\}, \quad R_{S0}(0) = 1. \quad (2.75)$$

Equation (2.75) can take a complicated form, according to the degree of dependence encountered.

The situation is easier when stress and strength can be assumed to be *independent and positive random variables*. In this case, $\Pr\{\xi_S > \xi_L \mid \xi_L = x\} = \Pr\{\xi_S > x\} = 1 - F_S(x)$ and the theorem of total probability leads to

$$R_{S0}(t) = R_{S0} = \Pr\{\xi_S > \xi_L\} = \int_0^{\infty} f_L(x)(1 - F_S(x)) dx. \quad (2.76)$$

Examples 2.15 and 2.16 illustrate the use of Eq. (2.76).

Example 2.15

Let the stress ξ_L of a mechanical joint be normally distributed with mean $m_L = 100 \text{ N/mm}^2$ and standard deviation $\sigma_L = 40 \text{ N/mm}^2$. The strength ξ_S is also normally distributed with mean $m_S = 150 \text{ N/mm}^2$ and standard deviation $\sigma_S = 10 \text{ N/mm}^2$. Compute the reliability of the joint.

Solution

Since ξ_L and ξ_S are normally distributed, their difference is also normally distributed (Example A.6.17). Their mean and standard deviation are $m_S - m_L = 50 \text{ N/mm}^2$ and $\sqrt{\sigma_S^2 + \sigma_L^2} \approx 41 \text{ N/mm}^2$, respectively. The reliability of the joint is then given by (Table A9.1)

$$R_{S0} = \Pr\{\xi_S > \xi_L\} = \Pr\{\xi_S - \xi_L > 0\} = \frac{1}{41\sqrt{2\pi}} \int_0^{\infty} e^{-\frac{(x-50)^2}{2 \cdot 41^2}} dx = \frac{1}{\sqrt{2\pi}} \int_{-50/41}^{\infty} e^{-y^2/2} dy \approx 0.89.$$

Example 2.16

Let the strength ξ_S of a rod be normally distributed with mean $m_S = 450 \text{ N/mm}^2 - 0.01 t \text{ N/mm}^2 \text{ h}^{-1}$ and standard deviation $\sigma_S = 25 \text{ N/mm}^2 + 0.001 t \text{ N/mm}^2 \text{ h}^{-1}$. The stress ξ_L is constant and equal 350 N/mm^2 . Calculate the reliability of the rod at $t = 0$ and $t = 10^4 \text{ h}$.

Solution

At $t = 0$, $m_S = 450 \text{ N/mm}^2$ and $\sigma_S = 25 \text{ N/mm}^2$. Thus (as for Example 2.15),

$$R_{S0} = \Pr\{\xi_S > \xi_L\} = \frac{1}{\sqrt{2\pi}} \int_{\frac{350-450}{25}}^{\infty} e^{-y^2/2} dy \approx 0.99997.$$

After 10,000 operating hours, $m_S = 350 \text{ N/mm}^2$ and $\sigma_S = 35 \text{ N/mm}^2$. The reliability is then

$$R_{S0} = \Pr\{\xi_S > \xi_L\} = \frac{1}{\sqrt{2\pi}} \int_{\frac{350-350}{35}}^{\infty} e^{-y^2/2} dy = \frac{1}{\sqrt{2\pi}} \int_0^{\infty} e^{-y^2/2} dy = 0.5.$$

Equation (2.76) holds for a one-item structure. For a series model, i.e., in particular for the *series connection of two independent elements* one obtains:

1. Same stress ξ_L ($\xi_L, \xi_{S_i} > 0$)

$$R_{S0} = \Pr\{\xi_{S_1} > \xi_L \cap \xi_{S_2} > \xi_L\} = \int_0^{\infty} f_L(x)(1 - F_{S_1}(x))(1 - F_{S_2}(x))dx. \quad (2.77)$$

2. Independent stresses ξ_{L_1} and ξ_{L_2} ($\xi_{L_i}, \xi_{S_i} > 0$)

$$\begin{aligned} R_{S0} &= \Pr\{\xi_{S_1} > \xi_{L_1} \cap \xi_{S_2} > \xi_{L_2}\} = \Pr\{\xi_{S_1} > \xi_{L_1}\} \Pr\{\xi_{S_2} > \xi_{L_2}\} \\ &= \left(\int_0^{\infty} f_{L_1}(x)(1 - F_{S_1}(x))dx\right) \left(\int_0^{\infty} f_{L_2}(x)(1 - F_{S_2}(x))dx\right) \hat{=} R_1 R_2. \end{aligned} \quad (2.78)$$

For a parallel model, i. e., in particular for the *parallel connection of two non repairable independent elements* it follows that:

1. Same stress ξ_L ($\xi_L, \xi_{S_i} > 0$)

$$R_{S0} = 1 - \Pr\{\xi_{S_1} \leq \xi_L \cap \xi_{S_2} \leq \xi_L\} = 1 - \int_0^{\infty} f_L(x)F_{S_1}(x)F_{S_2}(x)dx. \quad (2.79)$$

2. Independent stresses ξ_{L_1} and ξ_{L_2} ($\xi_{L_i}, \xi_{S_i} > 0$)

$$R_{S0} = 1 - \Pr\{\xi_{S_1} \leq \xi_{L_1}\} \Pr\{\xi_{S_2} \leq \xi_{L_2}\} \hat{=} 1 - (1 - R_1)(1 - R_2) = R_1 + R_2 - R_1 R_2. \quad (2.80)$$

As with Eqs. (2.78) and (2.80), the results of Table 2.1 (p. 31) can be applied in the case of *independent* stresses and elements. However, this *ideal situation* is seldom true for mechanical systems, for which Eqs. (2.77) and (2.79) are often more realistic. Moreover, the *uncertainty* about the *exact form* of the distributions for stress and strength far from the mean value, *severely reduce the accuracy* of the results obtained from the above equations in practical applications. For mechanical items, *tests* are thus often the only way to evaluate their reliability. Investigations into new methods are in progress, paying particular attention to the *dependence between stresses* and to a *realistic truncation* of the stress and strength distribution functions or densities (Eq. (A6.33)). Other approaches are possible for mechanical systems, see e. g. [2.61-2.77].

For electronic items, Eqs. (2.76) and (2.77) - (2.80) can often be used to investigate *drift failures*. Quite generally, all considerations of Section 2.5 could be applied to electronic items. However, the method based on the failure rate, introduced in Section 2.2, is easier to be used and works reasonably well in many practical applications dealing with electronic and electromechanical equipment and systems.

2.6 Failure Modes Analyses

Failure rate analyses (Sections 2.1 - 2.5) basically do not account for the *mode* and *effect* (consequence) of a failure. To understand the mechanism of system failures and in order to identify *potential weaknesses of a fail-safe concept* it is necessary to perform a *failure modes analysis*, at least where redundancy appears and for critical parts of the item considered. Such an analysis is termed FMEA (Failure Modes and Effects Analysis) or alternatively FMECA (Failure Modes, Effects, and Criticality Analysis) if also the *failure severity* is of interest. If *failures and defects* have to be considered, *fault modes* is to use, allowing *errors/flaws* as possible causes as well. An FMEA/FMECA consists of the systematic analysis of failure (fault) *modes*, their *causes*, *effects*, and *criticality* [2.81, 2.83, 2.84, 2.87-2.93, 2.96-2.98], including *common mode & common cause* failures as well. All possible failure (fault) modes for the item considered, their causes and consequences are systematically investigated, in one run or in several steps (design FMEA/FMECA, process FMEA/FMECA). For critical cases, possibilities to avoid the failure (fault) or to minimize (mitigate) its consequence must be analyzed and corresponding corrective (or preventive) actions *have to be realized*. The criticality describes the severity of the consequence of the failure (fault) and is designated by categories or levels which are function of the risk for damage or loss of performance. Considerations on failure modes for electronic components are in Tables 3.4 & A10.1 and Section 3.3.

The FMEA/FMECA is a *bottom-up* (inductive) procedure, performed as a team work with designer & reliability engineers. The procedure is established in *international standards* [2.89]. It is easy to understand but can become time-consuming for complex equipment and systems. For this reason *it is recommended to concentrate efforts to critical parts*, in particular where *redundancy appears*. Table 2.5 shows a procedure for an FMEA/FMECA. Basic are steps 3 to 8. Table 2.6 gives an example of a detailed FMECA for the switch in Example 2.6, Point 7. Each row of Tab. 2.5 is a column in Tab. 2.6. Other sheets are possible [2.83, 2.84, 2.89]. Quite generally,

an FMEA/FMECA is mandatory in the presence of redundancy, and/ or for items with fail-safe behavior, to verify effectiveness and to define elements in series on the reliability block diagram; it is useful to support safety and maintainability analyses, and should be performed prior to a final reliability prediction.

To visualize the item's criticality, the FMECA is often completed by a *criticality grid* (*criticality matrix*), see e.g. [2.89]. In such a matrix, each failure (fault) mode give an entry (dot) with criticality category as ordinate and probability of occurrence as abscissa (Fig. 2.13). Generally accepted classifications are *minor* (I), *major* (II), *critical* (III), *catastrophic* (IV) for the criticality level, and *very low*, *low*, *medium*, *high* for the probability of occurrence. In a criticality grid, the further an entry is far from the origin, the greater is the necessity for a corrective or preventive action.

Table 2.5 Basic procedure for performing an FMECA** (according also to IEC 60812 [2.89])

1. Sequential numbering of the step.
2. Designation of the element or part under consideration, short description of its function, and reference to the reliability block diagram, part list, etc. (3 steps in IEC 60812)
3. Assumption of a <i>possible failure* mode</i> (all possible failure* modes have to be considered).
4. Identification of <i>possible causes</i> for the failure* mode assumed in step 3 (a cause for a failure* can also be a flaw in the design phase, production phase, transportation, installation or use).
5. Description of the <i>symptoms</i> which will characterize the failure* mode assumed in step 3 and of its local effect (output/input relationships, possibilities for secondary failures, etc.).
6. Identification of the <i>consequences</i> of the failure* mode assumed in step 3 on the next higher integration levels (up to the system level) and on the mission to be performed.
7. Identification of <i>failure* detection provisions and of corrective actions</i> which can mitigate the severity of the failure* mode assumed in step 3, reduce the probability of occurrence, or initiate an alternate operational mode which allows continued operation when the failure* occurs.
8. Identification of <i>possibilities to avoid</i> the failure* mode assumed in step 3, and <i>realization</i> of corresponding corrective (or preventive) actions.
9. Evaluation of the <i>severity</i> of the failure* mode assumed in step 3 (FMECA only); e.g. I for minor, II for major, III for critical, IV for catastrophic (or alternatively, 1 for failure* to complete a task, 2 for large economic loss, 3 for large material damage, 4 for loss of human life).
10. Estimation of the <i>probability of occurrence</i> (or failure rate) of the failure* mode assumed in step 3 (FMECA only), with consideration of the cause of failure* identified in step 4, e.g. <i>very low, low, medium, high</i> .
11. Formulation of <i>pertinent remarks</i> which complete the information in the previous columns and also of <i>recommendations for corrective actions</i> , which will reduce the consequences of the failure* mode assumed in step 3 (e.g. introduction of failure* sensing devices).

* *fault* is to use if *failures and defects* have to be considered, allowing *errors / flaws* as possible causes as well;
 ** steps 1 to 11 are columns in Tab. 2.6, FMEA by omitting steps 9 & 10

The procedure for an FMEA/FMECA has been developed for *hardware*, but can also be used for *software* as well [2.87, 2.88, 5.75, 5.79]. For mechanical items, the FMEA/FMECA is an *essential tool in reliability analyses* (Section 2.5).

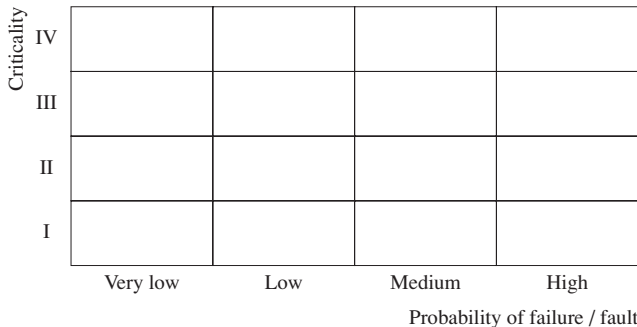


Figure 2.13 Example of *criticality grid* for an FMECA (according to IEC 60812 [2.89])

Table 2.6 Example of a detailed FMECA for elements $E_1 - E_7$ in Point 7 of Example 2.6 (p. 51)

FAILURE MODES AND EFFECTS ANALYSIS / FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS											
(fault modes is to use if failures and defects have to be considered, allowing errors/flaws as possible causes as well)											
FMEA/FMECA											
Mission / required function: fault signaling State: operating phase											
Page: 1&2											
(1) No.	(2) Element, Function, Position	(3) Assumed failure mode	(4) Possible causes	(5) Symptoms, local effects	(6) Effect on mission	(7) Failure detection possibilities	(8) Possibilities to avoid the failure mode in (3)	(9) Se- verity	(10) Probability of occurrence	(11) Remarks and suggestions	
1.	TR ₁ , NPN Si transistor in plastic - package (E ₄)	Short BCE, CE	Bad solder joint	Redundancy failed; U _{CE} = 0; no consequence to other elements	practically no consequence	U _{CE} =0, U _{RC} >0	—	1	p = 10 ⁻⁵ λ = 1.8 · 10 ⁻⁹ h ⁻¹	a) λ for θ _A = 50°C and G _B	
			Inherent failure	LED lights dimly; disappears by bridging CE; no conse- quence to other elements	Partial failure	U _{BC} =0, U _{RC} >0	Use a transistor of better quality; impr. handling, assembly, and soldering proc.	2	p = 10 ⁻⁵ λ = 0.3 · 10 ⁻⁹ h ⁻¹	b) it is possible to notify the failure of TR ₁ (Level detector)	
		Short BC	Bad solder joint	Circuit faulty; disappears by bridging CE; no consequence to other elements	Complete (possibly partial) failure	U _{BE} =0, U _{RB1} >0	Improve handling, as- sembly & soldering procedures	3 to 2	p = 10 ⁻⁵ λ = 0.3 · 10 ⁻⁹ h ⁻¹	p = 10 ⁻⁵ λ = 0.3 · 10 ⁻⁹ h ⁻¹	
			Inherent failure	Circuit works intermittently; no consequence to other elements	Partial to complete failure	U _C =V _{CC} , U _{BC} =U _I					
		Short BE	Wrong connection, cold solder joint	The circuit works correctly even with large parameter deviations; no consequence to other elements	Practically no consequence	—	Improve handling	1 to 2	p = 10 ⁻⁴ λ = 0.6 · 10 ⁻⁹ h ⁻¹	p = 10 ⁻⁴ λ = 0.1 · 10 ⁻⁹ h ⁻¹	
			Inherent failure	LED does not light; no con- sequence to other elements	Complete failure	U _{RB1} > 0, U _{LED} =V _{CC}					
		Open	Intermit- tent solder joint failure	Damage	LED does not light; no con- sequence to other elements	Complete failure	Improve soldering procedures	3	p = 10 ⁻³ λ = 0.8 · 10 ⁻⁹ h ⁻¹	p = 10 ⁻³ λ = 0.8 · 10 ⁻⁹ h ⁻¹	a) λ for θ _A = 30°C and G _B b) be careful when forming the leads c) Observe the max. soldering time; distance between package and board > 2 mm
				Wear out	LED lights dimly; no con- sequence to other elements	Partial to complete failure					
		Drift	Intermit- tent failure	Damage, cold solder joint	LED does not light; no con- sequence to other elements	Complete failure	Improve handling, assembly & soldering procedures	2 to 3	p = 10 ⁻⁴ λ = 0.3 · 10 ⁻⁹ h ⁻¹	p = 10 ⁻⁴ λ = 0.3 · 10 ⁻⁹ h ⁻¹	d) pay attention to the cleaning medium
				Damage	LED lights dimly; no con- sequence to other elements	Partial failure					
Drift	Intermit- tent failure	Wear out	LED does not light; no con- sequence to other elements	Partial failure	Prot. against humid.	2	p = 10 ⁻⁴ λ = 0.2 · 10 ⁻⁹ h ⁻¹	p = 10 ⁻⁴ λ = 0.2 · 10 ⁻⁹ h ⁻¹	e) hermet. package		
		Corrosion	LED lights dimly; no con- sequence to other elements	Partial failure							
2.	LED (E ₁)	Open	Wrong connection, damage, cold solder joint	LED does not light; no con- sequence to other elements	Complete failure	U _{RB1} > 0, U _{LED} =V _{CC}	Improve handling, assembly & soldering procedures	3	p = 10 ⁻³ λ = 0.8 · 10 ⁻⁹ h ⁻¹	a) λ for θ _A = 30°C and G _B b) be careful when forming the leads c) Observe the max. soldering time; distance between package and board > 2 mm	
		Short	Bad solder joint	LED does not light; no con- sequence to other elements	Complete failure	U _{LED} =0, U _{RC} >0	Improve soldering procedures	3	p = 10 ⁻⁵ λ = 0.3 · 10 ⁻⁹ h ⁻¹	d) pay attention to the cleaning medium	
		Intermit- tent failure	Damage, cold solder joint	LED lights intermittently; no consequence to other elements	Partial to complete failure	—	Improve handling, assembly & soldering procedures	2 to 3	p = 10 ⁻⁴ λ = 0.3 · 10 ⁻⁹ h ⁻¹	e) hermet. package	
		Drift	Damage Wear out	LED lights dimly; no con- sequence to other elements	Partial failure	—	Improve handling Reduce θ _A	2	p = 10 ⁻⁴ λ = 0.2 · 10 ⁻⁹ h ⁻¹		

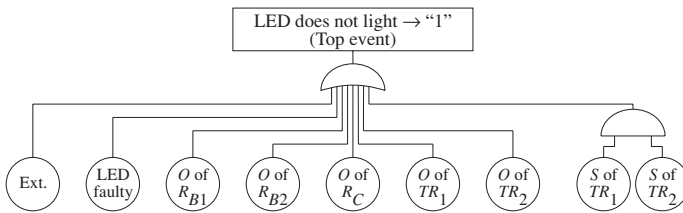


Figure 2.14 Example of *fault tree* (FT) for the electronic switch given in Example 2.6, Point 7, p.51 (O = open, S = short, Ext. are possible external causes, such as power out, manufacturing error, etc.); as in use for FTA, "0" holds for operating and "1" for failure (Section 6.9.2)

A further possibility to investigate failure and defect causes-to-effects relationships is the *Fault Tree Analysis* (FTA) [2.89 (IEC 61025)]. The FTA is a *top-down* (deductive) procedure in which the undesired event, for example a critical failure at system level, is represented (for coherent \rightarrow systems) by AND and OR combinations of causes at lower levels. It is a current rule in FTA [2.89 (IEC 61025)] to use "0" for operating and "1" for failure (the top event "1" being in general a failure). Some examples for *fault trees* (FT) are in Figs. 2.14, 6.40 - 6.42. In a fault tree, a *cut set* is a set of basic events whose occurrence (of all) causes the *top event* to occur. *Minimal cut sets*, defined as per Eq. (2.43) can be identified. Algorithms have been developed to obtain all *minimal cut sets* (and *minimal path sets*) belonging to a given system, see e.g. [2.33, 2.34 (1975)]. From a complete and correct fault tree it is possible to compute the reliability for the nonrepairable case and the point availability for the repairable case, when *active redundancy & totally independent elements* (p. 52) can be assumed (Eqs. (2.45) & (2.48), Section 6.9.1). To consider some dependencies, *dynamic gates* have been introduced (Section 6.9.2). For computation purposes, *binary decision diagrams* (BDD) have been developed (Sections 6.9.3).

Compared to FMEA/FMECA, FTA can take *external influences or causes* (human and/or environmental) better into account, and handle situations where *more than one primary fault* (multiple faults) has to occur in order to cause the undesired event at system level. However, it does not necessarily go through all possible fault modes. *Combination* of FMEA/FMECA and FTA can provide better assurance for completeness of analysis. However, for consistency checks, FMEA / FMECA and FTA should be performed separately and independently. FMEA / FMECA and FTA can also be combined with *Event Tree Analysis* (Section 6.9.4), leading to *causes-to-effects charts* and showing relationship between causes and their single or *multiple consequences* as well as efficacy of mitigating factors.

Further methods/tools which can support *causes-to-effects analyses* are *sneak analysis* (circuit, path, timing), *worst-case analysis*, *drift analysis*, *stress-strength analysis*, *Ishikawa diagrams*, *Kepner-Tregoe method*, *Shewhart cycles* (Plan-Analyze-Check-Do), and *Pareto diagrams*, see e.g. [1.22, 2.14, A2.6 (IEC 60300-3-1)].

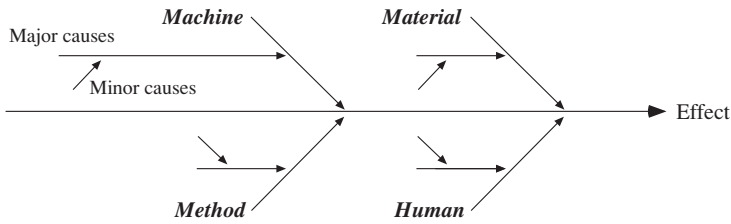


Figure 2.15 Typical structure of a *causes-to-effects* diagram (Ishikawa or fishbone diagram); causes can often be grouped into *Machine*, *Material*, *Method*, and *Human (Man)*, into *failure mechanisms*, or into a combination of all them, as appropriate

Table 2.7 gives a comparison of important tools used for *causes-to-effects* analyses. Figure 2.15 shows the basic structure of an Ishikawa (fishbone) diagram. The Ishikawa diagram is a graphical visualization of the relationships between *causes and effects*, grouping the causes into *machine*, *material*, *method*, and *human (man)*, into *failure mechanisms*, or into a combination of all them, as appropriate.

Performing an FMEA /FMECA, FTA, or any other similar investigation presupposes a *detailed* technical knowledge and *thorough understanding* of the item and the technologies considered. This is necessary to *identify all relevant* failure modes and potential errors/flaws (during design, development, manufacture, operation), their causes, and the more appropriate *corrective or preventive actions*.

2.7 Reliability Aspects in Design Reviews

Design reviews are important to point out, discuss, and eliminate *design weaknesses*. Their objective is also to *decide about continuation or stopping* of the project on the basis of objective considerations (*feasibility checks* in Fig. 1.6 and in Tables 5.3 and A3.3). The most important design reviews are described in Table A3.3 for hardware and in Table 5.5 for software. To be effective, design reviews must be supported by *project specific checklists*. Table 2.8 gives a catalog of questions which can be used to generate project specific checklists for reliability aspects in design reviews (see Table 4.3 for maintainability and Appendix A4 for other aspects). As shown in Table 2.8, checking the reliability aspects during a design review is more than just verifying the value of the predicted reliability or the source used for failure rate calculation. The purpose of a design review is, in particular, to discuss selection and use of components and materials, adherence to given *design guidelines*, presence of *potential reliability weaknesses*, and results of *analyses and tests*. Tables 2.8 and 2.9 can be used to support this aim.

Table 2.7 Important tools for *causes-to-effects-analysis* (see also [A2.6 (IEC 60300-3-1)] and Sections 6.9.2 – 6.9.4)

Tool	Description	Application	Effort**
FMEA/FMECA (Failure Modes & Effects Analysis / Failure Modes, Effects & Criticality Analysis)*	Systematic <i>bottom-up</i> investigation of the effects (consequences) at system (item) level of the <i>failure* modes</i> of all parts of the system considered, and analysis of the possibilities to reduce (mitigate) these effects and/or their occurrence probabilities	Development phase (design FMEA/FMECA) and production phase (process FMEA/FMECA); mandatory for all interfaces, in particular where <i>redundancy</i> appears and for <i>safety</i> relevant parts	Very large if performed for all elements (≥ 0.1 MM for a PCB)
FTA (Fault Tree Analysis, see Section 6.9.2 for dynamic FT)	Quasi-systematic <i>top-down</i> investigation of the effects (consequences) of faults (failures and defects) as well as of external influences on the reliability and/or safety of the system (item) considered; the top event (e. g. a specific catastrophic failure*) is the result of AND & OR combinations of elementary events	Similar to FMEA/FMECA; however, combination of more than one fault (or elementary event) can be better considered as by an FMEA/FMECA; also is the influence of <i>external events</i> (natural catastrophe, sabotage etc.) easier to be considered	Large to very large, if many top events are considered
Ishikawa Diagram (Fishbone Diagram)	Graphical representation of the causes-to-effects relationships; the causes are often grouped in four classes: machine, material, method / process, and human (man) dependent	Ideal for team-work discussions, in particular for the investigation of design, development, or production weaknesses	Small to large
Kepner-Tregoe Method	Structured problem detection, analysis, and solution by complex situations; the main steps of the method deal with a careful problem analysis, decision making, and solution weighting	Generally applicable, especially by complex situations and in interdisciplinary work-groups	Largely dependent on the specific situation
Pareto Diagram	Graphical presentation of the frequency (histogram) and (cumulative) distribution of the problem causes, grouped in application specific classes	Supports the objective decision making in selecting the causes of a fault and defining the appropriate corrective action (<i>Pareto rule</i> : 80% of the problems are generated by 20% of the possible causes)	Small
Correlation Diagram	Graphical representation of (two) quantities with possible functional (deterministic or stochastic) relation on an appropriate x/y-Cartesian coordinate system	Assessment of a relationship between two quantities	Small

* *fault* is to use if *failures and defects* have to be considered, allowing *errors / flaws* as possible causes as well

** MM stays for man month

Table 2.8 Catalog of questions which can be used to generate *project specific checklists* for the evaluation of *reliability aspects in preliminary design reviews* (Appendices A3 and A4) of complex equipment and systems with high reliability requirements (see p. 120 for *maintainability*, including human and ergonomic aspects)

<ol style="list-style-type: none"> 1. Is it a new development, redesign, or change /modification? 2. Is there test or field data available from similar items? What were the problems? 3. Has a list of preferred components been prepared and consequently used? 4. Is the selection/qualification of nonstandard components and material specified? How? 5. Have the interactions among elements been minimized? Can interface problems be expected? 6. Have all the specification requirements of the item been fulfilled? Can individual requirements be reduced? 7. Has the mission profile been defined? How has it been considered in the analysis? 8. Has a reliability block diagram been prepared? Are series elements to redundant parts been carefully evaluated? How? 9. Have the environmental conditions for the item been clearly defined? How are the operating conditions for each element? 10. Have derating rules been appropriately applied? 11. Has the junction temperature of all semiconductor devices been kept lower than 100°C? 12. Have drift, worst-case, and sneak path analyses been performed? What are the results? 13. Has the influence of on-off switching and of external interference (EMC) been considered? 14. Is it necessary to improve the reliability by introducing redundancy? Have common cause failures (faults) been avoided? 15. Has an FMEA/FMECA been performed, at least for the parts where redundancy appears? How? Are single-point failures present? Can nothing be done against them? Are there safety problems? Can liability problems be expected? 16. Does the predicted reliability of each element correspond to its allocated value? With which π-factors it has been calculated? 17. Has the predicted reliability of the whole item been calculated? Does this value correspond to the target given in the item's specifications? 18. Are there elements with a limited useful life? 19. Are there components which require screening? Assemblies which require environmental stress screening (ESS)? 20. Can design or construction be further simplified? 21. Is failure detection, localization, and removal easy? 22. Are hidden failures possible? Is their effect (consequence) minimized? How? 23. Have reliability tests been planned? What does this test program include? 24. Have the aspects of manufacturability, testability, and reproducibility been considered? 25. Have the supply problems (second source, long-term deliveries, obsolescence) been solved?

Table 2.9 Example of form sheets for detecting and investigating potential *reliability weaknesses* at assemblies and equipment level

a) Assembly design

Position	Component	Failure rate λ (FITs)	Deviation from reliability design guidelines	Component selection and qualification	Problems during design, develop., manufact., test, use	El. test and screening

b) Assembly manufacturing

Item	Layout	Placing	Soldering	Cleaning	El. tests	Screening	Fault (defect, failure) analysis	Corrective actions	Transportation and storage

c) Prototype qualification tests

Item	Electrical tests	Environmental tests	Reliability tests	Fault (defect, failure) analysis	Corrective actions

d) Equipment and systems level

Assembling	Test	Screening (ESS)	Fault (defect, failure) analysis	Corrective actions	Transportation and storage	Operation (field data)

3 Qualification Tests for Components and Assemblies

Components, materials, and assemblies have a great impact on the quality and reliability of the equipment and systems in which they are used. Their *selection and qualification* has to be considered with care by new technologies or important redesigns, on a *case-by-case basis*. Besides cost and availability on the market, important selection criteria are *intended application, technology, quality, long-term behavior* of relevant parameters, and *reliability*. A *qualification test* includes *characterization* at different stresses (for instance, electrical and thermal for electronic components), *environmental tests, reliability tests, and failure analysis*. After some considerations on *selection criteria* for electronic components (Section 3.1), this chapter deals with *qualification tests* for complex integrated circuits (Section 3.2) and electronic assemblies (Section 3.4), and discusses *basic aspects of failure modes, mechanisms, and analysis* of electronic components (Section 3.3). Procedures given in this chapter can be extended to nonelectronic components and materials as well. Reliability related basic technological properties of electronic components are summarized in Appendix A10. Statistical tests are in Chapter 7, test and screening strategies in Chapter 8, *design guidelines* in Chapter 5.

3.1 Basic Selection Criteria for Electronic Components

As given in Section 2.2 (Eq. (2.18)), the failure rate of equipment and systems without redundancy is the *sum* of the failure rates of their elements. Thus, for large equipment and systems *without redundancy*, high reliability can only be achieved by selecting components and materials with sufficiently *low failure rates*. Useful *information for such a selection* are:

1. Intended application, in particular required function, *environmental conditions*, as well as reliability and safety targets.
2. Specific properties of the component or material considered, in particular *technological limits*, useful life, long term behavior of relevant parameters.
3. Possibility for accelerated tests.

4. Results of qualification tests on similar components or materials.
5. Experience from *field operation*.
6. Influence of derating, influence of screening
7. Potential design problems, in particular sensitivity of performance parameters, interface problems, EMC.
8. Limitations due to standardization or logistic aspects.
9. Potential production problems (assembling, testing, handling, storage, etc.).
10. Purchasing considerations (cost, delivery time, second sources, long-term availability, quality level).

As many of the above requirements are conflicting, component selection often results in a *compromise*. The following is a brief discussion of the most important aspects in selecting electronic components (see e.g. [3.1,3.10,3.15] for greater details).

3.1.1 Environment

Environmental conditions have a major impact on the functionality and reliability of electronic components, equipment, and systems. They are defined in *international standards* [3.8]. Such *standards* specify stress limits and test conditions, among others for

heat (steady-state, rate of temperature change), cold, humidity, precipitation (rain, snow, hail), radiation (solar, heat, ionizing), salt, sand, dust, noise, vibration (sinusoidal, random), shock, fall, acceleration.

Several combinations of stresses have also been defined, for instance,

temperature and humidity, temperature and vibration, humidity and vibration.

Not all stress combinations are relevant and by combining stresses, or in defining sequences of stresses, care must be taken to avoid the activation of failure mechanisms which would *not appear in the field*.

Environmental conditions at equipment and systems level are given by the *application*. They can range from severe, as in aerospace and defense fields (with extreme low and high ambient temperatures, 100% relative humidity, rapid thermal changes, vibration, shock, and high electromagnetic interference), to favorable, as in computer rooms (with forced cooling at constant temperature and no mechanical stress). *International standards* can be used to fix representative environmental conditions for many applications, e.g. *IEC 60721* [3.8]. Table 3.1 gives *examples* for environmental test conditions for electronic/ electromechanical equipment and systems. The stress conditions given in Table 3.1 have indicative purpose and have to be refined according to the specific application, to be cost and time effective.

Table 3.1 Examples for *environmental test conditions* for electronic / electromechanical equipment and systems (according to IEC 60068 [3.8])

Environmental condition	Stress profile, procedure	Induced failures
Dry heat	48 or 72 h at 55, 70 or 85°C: El. test, warm up (2°C/min), hold (80% of test time), power-on (20% of test time), el. test, cool down (1°C/min), el. test between 2 and 16 h	<i>Physical:</i> Oxidation, structural changes, softening, drying out, viscosity reduction, expansion <i>Electrical:</i> Drift parameters, noise, insulating resistance, opens, shorts
Damp heat (cycles)	2, 6, 12 or 24 x 24 h cycles 25 ÷ 55°C with rel. humidity over 90% at 55°C and 95% at 25°C: El. test, warm up (3 h), hold (9 h), cool down (3 h), hold (9 h), at the end dry with air and el. test between 6 and 16 h	<i>Physical:</i> Corrosion, electrolysis, absorption, diffusion <i>Electrical:</i> Drift parameters, insulating resistance, leakage currents, shorts
Low temperature	48 or 72 h at -25, -40 or -55°C: El. test, cool down (2°C/min), hold (80% test time), power-on (20% test time), el. test, warm up (1°C/min), el. test between 6 and 16 h	<i>Physical:</i> Ice formation, structural changes, hardening, brittleness, increase in viscosity, contraction <i>Electrical:</i> Drift parameters, opens
Vibrations (random)	30 min random acceleration with rectangular spectrum 20 to 2000 Hz and an acceleration spectral density of 0.03, 0.1, or 0.3 g_n^2 /Hz: El. test, stress, visual inspection, el. test	<i>Physical:</i> Structural changes, fracture of fixings and housings, loosening of connections, fatigue <i>Electrical:</i> Opens, shorts, contact problems, noise
Vibrations (sinusoidal)	30 min at 2 g_n (0.15 mm), 5 g_n (0.35 mm), or 10 g_n (0.75 mm) at the resonant freq. and the same test duration for swept freq. (3 axes): El. test, resonance determination, stress at the resonant frequencies, stresses at swept freq. (10 to 500 Hz), visual inspection, el. test	
Mechanical shocks (impact)	1000, 2000 or 4000 impacts (half sine curve 30 or 50 g_n peak value and 6 ms duration in the main loading direction or distributed in the various impact directions: El. test, stress (1 to 3 impacts/s), inspection (shock absorber), visual inspection, el. test	<i>Physical:</i> Structural changes, fracture of fixings and housings, loosening of connections, fatigue
Free fall	26 free falls from 50 or 100 cm drop height distributed over all surfaces, corners and edges, with or without transport packaging: El. test, fall onto a 5 cm thick wooden block (fir) on a 10 cm thick concrete base, visual insp., el. test	<i>Electrical:</i> Opens, shorts, contact problems, noise

$g_n = 10 \text{ m/s}^2$; el. = electrical

At *component level*, to the stresses caused by the equipment or system environmental conditions *add* those stresses produced by the component itself, due to its internal electrical or mechanical load. The *sum* of these stresses gives the *operating conditions*, necessary to determine the *stress at component level* and the corresponding *failure rate*. For instance, the ambient temperature *inside* an electronic assembly can be just some few °C higher than the temperature of the cooling medium, if forced cooling is used, but can become more than 30°C higher than the ambient temperature if cooling is poor.

3.1.2 Performance Parameters

The required *performance parameters* at component level are defined by the intended application. Once these requirements are established, the necessary *derating* is determined taking into account the quantitative relationship between failure rate and stress factors (Sections 2.2.3, 2.2.4, 5.1.1). It must be noted that the use of "*better*" components does not necessarily imply better performance and / or reliability. For instance, a faster IC family can cause EMC problems, besides higher power consumption and chip temperature. In critical cases, component selection should not be based only on short data sheet information. Knowledge of parameter sensitivity can be mandatory for the application considered.

3.1.3 Technology

Technology is rapidly evolving for many electronic components, see Fig. 3.1 and Table A10.1 for some basic information. As each technology has its advantages and weaknesses with respect to performance parameters and / or reliability, it is necessary to have a set of rules which can help to select a technology. Such rules (*design guidelines* in Section 5.1) are evolving and have to be periodically refined.

Of particular importance for *integrated circuits* (ICs) is the selection of the packaging form and type.

For the *packaging form*, distinction is made between inserted and surface mount devices. *Inserted devices* offer the advantage of easy handling during the manufacture of PCBs and also of lower sensitivity to *manufacturing defects or deviations*. However, number of pins and frequency are limited (up to 68 I/O and 20 Mhz). *Surface mount devices* (SMD) are cost and space saving and have better electrical performance because of the shortened and symmetrical bond wires, in particular flatpack (up to 450 I/O and 250 Mhz) and ball grid array (up to 450 I/O and 1 Ghz). However, compared to inserted devices, they have greater junction to ambient *thermal resistance* (Table 5.2), are more stressed during soldering, and solder joints have a much lower mechanical strength (Section 3.4). Difficulties can be expected

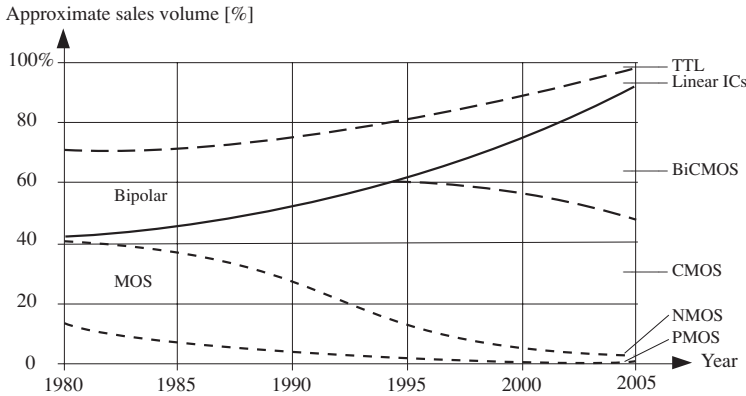


Figure 3.1 Basic IC technology evolution

with pitch lower than 0.3 mm, especially if thermal and/or mechanical stresses occur in field (Sections 3.4 and 8.3), in particular for JLead (PLCC).

Packaging types are subdivided into *hermetic* (ceramic, cerdip, metal can) and *nonhermetic* (plastic) packages. *Hermetic packages* should be preferred in applications with high humidity or in corrosive ambience, in any case if moisture condensation occurs on the package surface. Compared to plastic packages they offer lower *thermal resistance* between chip and case (Table 5.2), but are more expensive and sensitive to damage (microcracks) caused by inappropriate handling (mechanical shocks during testing or PCB production). *Plastic packages* are inexpensive, less sensitive to thermal or mechanical damage, but are permeable to *moisture* (other problems related to epoxy, such as ionic contamination and low *glass-transition temperature*, have been solved). However, better epoxy quality as well as new *passivation* (glassivation) based on silicon nitride leads to a much better protection against corrosion than formerly (Section 3.2.3, point 8).

If the results of qualification tests are good, the *use of ICs in plastic packages* can be allowed if one of the following conditions is satisfied:

1. Continuous operation, relative humidity < 70%, noncorrosive or marginally corrosive environment, junction temperature $\leq 100\text{ }^{\circ}\text{C}$, and equipment useful life less than 10 years.
2. Intermittent operation, relative humidity < 60%, noncorrosive environment, no moisture condensation on the package, junction temperature $\leq 100\text{ }^{\circ}\text{C}$, and equipment useful life less than 10 years.

For ICs with silicon nitride *passivation* (glassivation), the conditions stated in Point 1 above should also apply for the case of intermittent operation.

3.1.4 Manufacturing Quality

The *quality of manufacture* has a great influence on electronic component reliability. However, information about *global* defective probabilities (fraction of defective items) or agreed AQL values (even *zero defects*) are often *not sufficient* to monitor the *reliability level* (AQL is nothing more than an agreed upper limit of the defective probability, generally at a *producer risk* $\alpha \approx 10\%$, see Section 7.1.3). Information about changes in the *defective probability* and the results of the corresponding *failure analysis* are important. For this, a direct *feedback* to the component manufacturer is generally more useful than an agreement on an AQL value.

3.1.5 Long-Term Behavior of Performance Parameters

The *long-term stability* of performance parameters is an important selection criterion for electronic components, allowing differentiation between good and poor manufacturers (Fig. 3.2). Verification of this behavior is generally undertaken with *accelerated reliability tests* (trends are often enough for many practical applications).

3.1.6 Reliability

The reliability of an electronic component can often be specified by its *failure rate* λ . Failure rate figures obtained from field data are valid if *intrinsic* failures can be separated from *extrinsic* ones and reliable data/information are available. Those figures given by component manufacturers are useful if calculated with appropriate values for the (global) *activation energy* (for instance, 0.4 to 0.6eV for ICs) and *confidence level* ($> 60\%$ two sided or $> 80\%$ *one sided*, see Section 7.2.3.1). Moreover, besides the numerical value of λ , the influence of the *stress factor* (derating) S is important as a selection criteria (Eq. (2.1), Table 5.1).

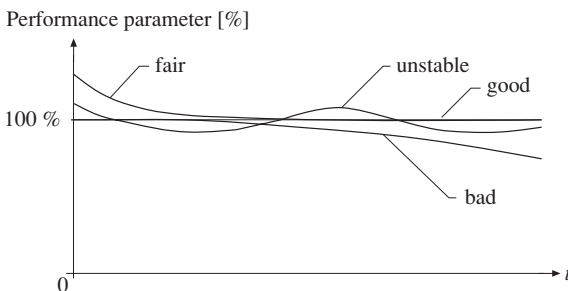


Figure 3.2 Long-term behavior of performance parameters

3.2 Qualification Tests for Complex Electronic Components

The purpose of a *qualification test* is to verify the *suitability* of a given item (material, component, assembly, equipment, system) for a stated application. Qualification tests are often a part of a *release procedure*. For instance, prototype release for a manufacturer and release for acceptance in a *preferred list (qualified part list)* for a user. Such a test is generally necessary for new technologies or after important redesigns or production processes changes. Additionally, periodic *requalification* of critical parameters is often necessary to monitor quality and reliability.

Electronic component qualification tests cover *characterization, environmental and special tests*, as well as *reliability tests*. They must be supported by intensive *failures (faults) analyses* to investigate *relevant failure mechanisms (and causes)*. For a *user*, such a qualification test must consider:

1. Range of validity, narrow enough to be representative, but sufficiently large to cover company's needs and to repay test cost.
2. Characterization, to investigate the electrical performance parameters.
3. Environmental and special tests, to check technology limits.
4. Reliability tests, to gain information on the failure rate.
5. Failure analysis, to identify failure causes and investigate failure mechanisms.
6. Supply conditions, to define cost, delivery schedules, second sources, etc.
7. Final report and feedback to the manufacturer.

The extent of the above steps depends on the *importance* of the component being considered, the *effect* (consequence) of its failure in an equipment or system, and the *experience* previously gained with similar components and with the same manufacturer. National and international activities are moving toward agreements which should make a qualification test by the user unnecessary for many components [3.8, 3.19]. Procedures for environmental tests are often defined in *standards* [3.8, 3.12].

A comprehensive qualification test procedure for ICs in *plastic packages* is given in Fig. 3.3. One recognizes the major steps (characterization, environmental and special tests, reliability tests, and failure analysis) of the above list. Environmental tests cover the thermal, climatic, and mechanical stresses expected in the application under consideration. The number of devices required for the reliability tests should be determined in order to *expect 3 to 6 failures during burn-in*. The procedure of Fig. 3.3 has been applied extensively (with device-specific aspects like data retention and programming cycles for nonvolatile memories, or modifications because of ceramic packages) to 12 memories each with 2 to 4 manufacturers for comparative investigations [3.6, 3.2 (1993), 3.16]. The cost for a qualification test based on Fig. 3.3 for 2 manufacturers (comparative studies) can exceed US\$ 50,000.

3.2.1 Electrical Test of Complex ICs

Electrical test of VLSI ICs is performed according to the following three steps:

1. Continuity test.
2. Test of DC parameters.
3. Functional and dynamic test (AC).

The *continuity test* checks whether every pin is connected to the chip. It consists in forcing a prescribed current (100 μ A) into one pin after another (with all other pins grounded) and measuring the resulting voltage. For inputs with protection diodes and for normal outputs this voltage should lie between -0.1 and -1.5 V.

Verification of *DC parameters* is simple. It is performed according to the manufacturer's specifications without restrictions (disregarding very low input currents). For this purpose a *precision measurement unit* (PMU) is used to force a current and measure a voltage (V_{OH} , V_{OL} , etc.) or to force a voltage and measure a current (I_{IH} , I_{IL} , etc.). Before each step, the IC inputs and outputs are brought to the logical state necessary for the measurement.

The *functional test* is performed together with the verification of the dynamic parameters, as shown in Figure 3.4. The generator in Fig. 3.4 delivers one row after another of the *truth table* which has to be verified, with a frequency f_o . For a 40-pin IC, these are 40-bit words. Of these binary words, called *test vectors*, the inputs are applied to the *device under test* (DUT) and the expected outputs to a logical comparator. The actual outputs from the DUT and the expected outputs are compared at a time point selected with high accuracy by a strobe. Modern VLSI *automatic test equipment* (ATE) for digital ICs have test frequencies $f_o > 600$ MHz and an overall precision better than 200 ps (resolution < 30 ps). In a VLSI ATE not only the strobe but other pulses can be varied over a wide range. The *dynamic parameters* can be verified in this way. However, the direct measurement of a time delay or of a rise time is in general time-consuming. The main problem with a functional test is that it is not possible to verify all the states and state sequences of a VLSI IC. To see this, consider for instance, that for an $n \times 1$ cell memory there are 2^n states and $n!$ possible address sequences, the corresponding *truth table* would contain $2^n \cdot n!$ rows, giving more than 10^{100} for $n = 64$. The procedure used in

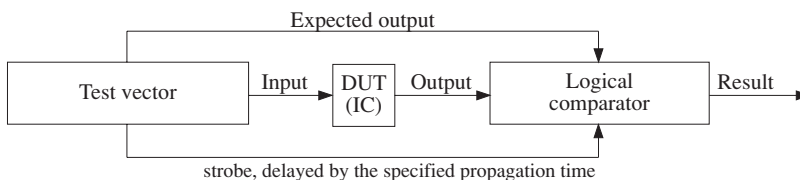


Figure 3.4 Principle of *functional and AC testing* for LSI and VLSI ICs (DUT=device under test)

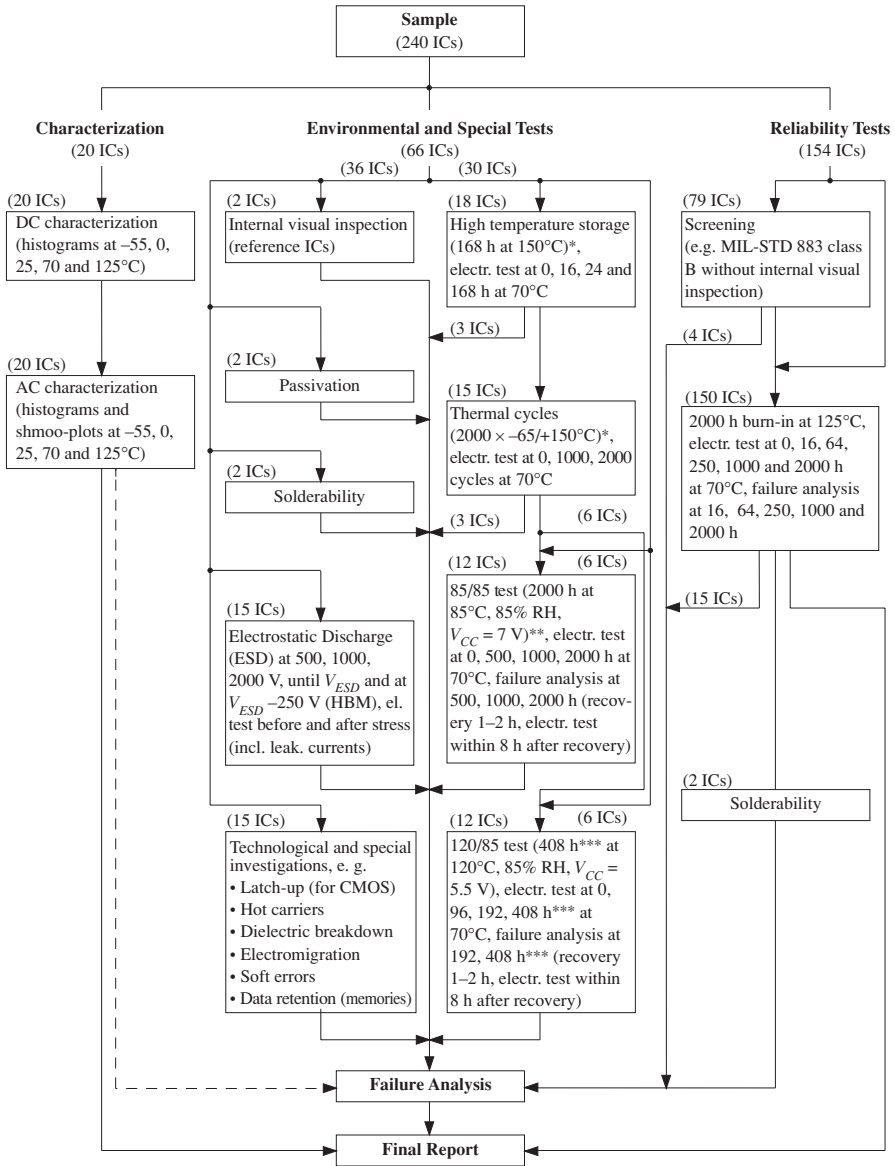


Figure 3.3 Example for a comprehensive qualification test procedure for complex ICs in plastic (PI) packages, see Sections 3.2 and 3.3 for details (industrial applications with normal environmental conditions (G_B in Table 2.3), 3 to 6 expected failures during reliability test ($A\lambda \approx 2 \cdot 10^{-5} h^{-1}$ in this example), RH=relative humidity, passivation=glasivation)

* 150°C by Epoxy resin, 175°C by Silicon resin; ** new is 40/93 tests for 168 to 500 h;

*** 1000 h by Si_3N_4 passivation

practical applications takes into account one or more of the following

- *partitioning* the device into modules and testing each of them separately,
- finding out *regularities* in the truth table or given by technological properties,
- limiting the test to the part of the truth table which is important for the application under consideration.

The above limitations rises the question of *test coverage*, i.e., the percentage of faults which are detected by the test. A precise answer to this question can only be given in *some particular cases*, because information about the faults which *actually* appear in a given IC is often lacking. *Fault models*, such as stuck-at-zero, stuck-at-one, or bridging are useful for PCB's testing, but generally of limited utility for a test engineer at the component level.

For packaged VLSI ICs, the electrical test should be performed at 70°C or at the highest specified operating temperature.

3.2.2 Characterization of Complex ICs

Characterization (electrical characterization) is a parametric, experimental analysis of the electrical properties of a given IC. Its purpose is to investigate the influence of different operating conditions such as supply voltage, temperature, frequency, and logic levels on the IC's behavior and to deliver a cost-effective test program for incoming inspection. For this reason a characterization is performed at 3 to 5 different temperatures and with a large number of different patterns.

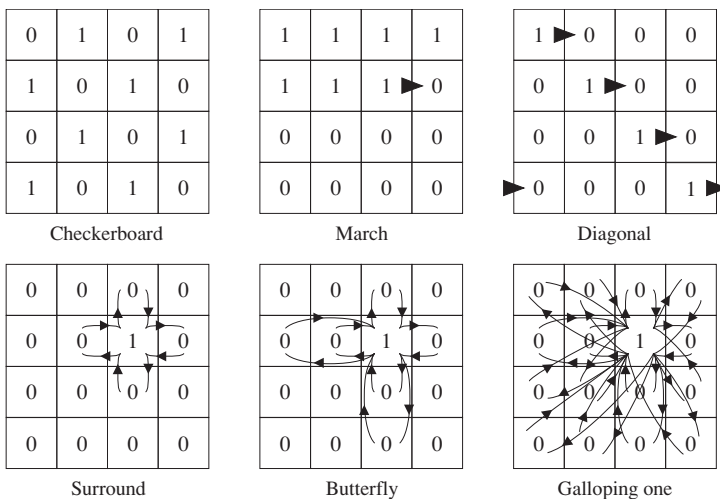


Figure 3.5 Examples for *memories test patterns* (see Table 3.2 for pattern sensitivity)

Table 3.2 Kindness of various test patterns for SRAMs, and approximate test times for a 100 ns 128K×8 SRAM [3.6] (Rel. Lab. at the ETH Zurich, tests Sentry S50, scrambling IDS5000 EBT)

Test pattern	Functional		Dyn. parameters		Number of test steps	Approx. test time[s]	
	D, H, S, O	C*	A, RA	C**		bit addr.	word addr.
Checkerboard	fair	poor	—	—	$4n$	—	0.05
March	good	poor	poor	—	$5n$	—	0.06
Diagonal	good	fair	poor	poor	$10n$	1	0.13
Surround	good	good	fair	fair	$26n - 16\sqrt{n}$	27	0.34
Butterfly	good	good	good	fair	$8n^{3/2} + 2n$	$8 \cdot 10^3$	38
Galloping one	good	good	good	good	$4n^2 + 6n$	$4 \cdot 10^5$	$7 \cdot 10^3$

A=addressing, C=cap.coupling, D=decoder, H=stuck at 0 or at 1, O=open, S=short, RA=read amplifier recovery time; * pattern dependent; ** pattern and level dependent

Referring to the functional and AC measurements, Figure 3.5 shows some *basic patterns* for memories. These patterns are generally performed twice, direct and inverse. For the patterns of Fig. 3.5, Table 3.2 gives a qualitative indication of the corresponding pattern sensitivity for static random access memories (SRAMs), and the approximate test time for a 128K×8 SRAM (see e.g. [3.6, 3.2(1989,1993)] for greater details and new patterns). *Quantitative* evaluation of *pattern sensitivity* or of *test coverage* is seldom possible; in general, because of the limited validity of *fault models* available (Sections 4.2.1 and 5.2.2). As shown in Table 3.2, test time strongly depends on the pattern selected. As test times greater than 10s per pattern are long also in the context of a characterization (the same pattern is repeated several thousands times, see e.g. Fig. 3.6), development of efficient test patterns is mandatory [3.6, 3.2(1989), 3.16, 3.20]. For such investigations, relationship between address and physical location (scrambling table) of the corresponding cell on the chip is important (in particular considering the increased presence of spare rows/columns in large memories [3.11]). If design information is not available, *electron beam tester* (EBT) can be helpful to establish the *scrambling table* [3.6].

An important evaluation tool during a characterization of complex ICs is the *shmoo plot*. A shmoo plot is the representation in an x/y -diagram of the operating region of an IC as a function of two parameters. As an example, Fig. 3.6 gives the shmoo plots for t_A versus V_{CC} of a 128K×8 SRAM for two patterns and two ambient temperatures [3.6]. For Fig. 3.6, test pattern has been performed about 4000 times ($2 \times 29 \times 61$), each with a different combination of V_{CC} and t_A . If no fault is detected, an x, otherwise a •, is plotted (defective cells are generally retested once, to confirm the fault). As shown in Fig. 3.6, a small (probably capacitive) coupling between nearby cells exists for this device, as a butterfly pattern is more sensitive than the diagonal pattern to this kind of fault. Statistical evaluation of shmoo plots is often done with *composite shmoo-plots* in which each record is labeled in 10% steps.

Table 3.3 DC parameters for a 40 pin CMOS ASIC specially developed for high noise immunity and with Schmitt-trigger inputs (20 ICs)

		25°C			70°C		
V_{DD}		12 V	15 V	18 V	12 V	15 V	18 V
I_{DD} (μA)	min	310	410	560	260	340	470
	mean	331	435	588	270	358	504
	max	340	450	630	290	390	540
V_{0H} (V) ($I_{0H} = 2.4 \text{ mA}$)	min	11.04	14.16	17.24	10.96	14.12	17.16
	mean	11.14	14.25	17.32	11.03	14.15	17.24
	max	11.20	14.33	17.40	11.12	14.20	17.32
V_{0L} (V) ($I_{0L} = 2.4 \text{ mA}$)	min	0.40	0.36	0.32	0.44	0.24	0.32
	mean	0.47	0.42	0.38	0.52	0.45	0.41
	max	0.52	0.44	0.44	0.60	0.52	0.48
V_{Hyst} (V)	min	2.65	3.19	3.89	2.70	3.19	3.79
	mean	2.76	3.33	3.97	2.75	3.32	3.93
	max	2.85	3.44	4.09	2.85	3.44	4.04

From the above considerations one recognizes that in general only a *small part* of the possible states and state sequences can be tested. The definition of appropriate test patterns must thus pay attention to the specific device, its technology and regularities in the truth table, as well as to information about its application and experience with similar devices [3.6, 3.2 (1989)]. A close *cooperation* between test engineer and user, and also if possible with the device designer and manufacturer, can help to reduce the amount of testing.

As stated in Section 3.2.1, measurement of DC parameters presents no difficulties. As an example, Table 3.3 gives some results for an application specific CMOS-IC (ASIC) specially developed for high noise immunity.

3.2.3 Environmental and Special Tests of Complex ICs

The aim of *environmental and special tests* is to submit a given IC to stresses which can be more severe than those encountered in field operation, in order to investigate *technological limits* and *failure mechanisms*. Such tests are often destructive. A failure analysis after each stress is important to evaluate *failure mechanisms* and to detect *degradation* (Section 3.3). Kind and extent of environmental and special tests depend on the intended application (G_F for Fig. 3.3) and specific characteristics of the component considered. The following is a description of the environmental and special tests given in Fig. 3.3 (considerations on production related potential reliability problems are in Sections 3.3 & 3.4, see also Figs. 3.7, 3.9, 3.10):

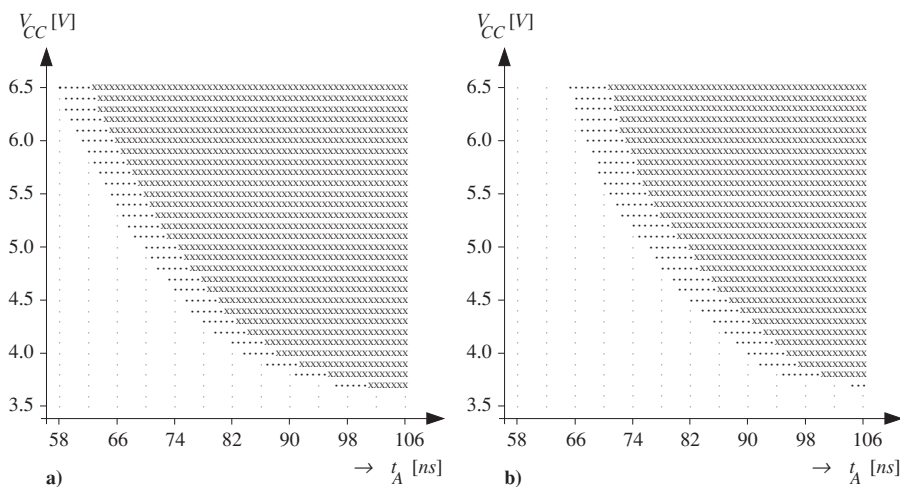


Figure 3.6 Shmoo plots of a 100 ns 128K \times 8 SRAM for test patterns **a)** Diagonal and **b)** Butterfly at two ambient temperatures 0°C (•) and 70°C (x) (Rel. Laboratory at the ETH Zurich)

1. **Internal Visual Inspection:** Two ICs are inspected and then kept as a reference for comparative investigation (check for damage after stresses). Before opening (using wet chemical or plasma etching), the ICs are x-rayed to locate the chip and to detect irregularities (package, bonding, die attach, etc.) or impurities. After opening, inspection is made with optical microscopes (conventional or stereo) and SEM if necessary. Improper placement of bonds, excessive height and looping of the bonding wires, contamination, etching, or metallization defects can be seen. Many of these deficiencies often have only a marginal effect on reliability. Figure 3.7a shows a limiting case (mask misalignment). Figure 3.7b shows voids in the metallization of a 1M DRAM.
2. **Passivation Test:** Passivation (glassivation) is the protective coating, usually *silicon dioxide* (PSG) and/or *silicon nitride*, placed on the entire (die) surface. For ICs in plastic packages it should ideally be free from *cracks* and *pinholes*. To check this, the chip is immersed for about 5 min in a 50°C warm mixture of nitric and phosphoric acid and then inspected with an optical microscope (e.g. as in *MIL-STD-883 method 2021* [3.12]). *Cracks* occur in a silicon dioxide passivation if the content of phosphorus is $< 2\%$. However, more than 4% phosphorus activates the formation of phosphoric acid. As a solution, *silicon nitride* passivation (often together with silicon dioxide in separate layers) has been introduced. Such a passivation shows much more resistance to the penetration of moisture (see humidity tests in Point 8 below) and of ionic contamination.

3. *Solderability*: Solderability of tinned pins should no longer constitute a problem today, except after a very long storage time in a non-protected ambient or after a long burn-in or high-temperature storage. However, problems can arise with gold or silver plated pins, see Section 5.1.5.4. The solderability test is performed according to established *standards* (e.g. *IEC 60068-2* or *MIL-STD-883* [3.8, 3.12]) after conditioning, generally using the solder bath or the meniscograph method.

4. *Electrostatic Discharge (ESD)*: Electrostatic discharges during *handling*, *assembling*, and *testing* of electronic components and populated printed circuit boards (PCBs) can destroy or damage sensitive components, particularly *semiconductor devices*. All ICs families and many discrete electronic components are sensitive to ESD. Integrated circuits have in general *protection circuitries*, passive and more recently active (factor ≥ 2). To determine *ESD immunity*, i.e., the voltage value at which damage occurs, different pulse shapes (models) and procedures to perform the test have been proposed. For semiconductor devices, the *human body model* (HBM), the *charged device model* (CDM), and the *machine model* (MM) are the most widely used. Both, CDM and MM can produce very short (some few 100ps) and high (10A peak) pulses, whereas pulses of HBM have rise time of 10ns, peak of 1.3A and decay time of 150ns. The CDM seems to apply better than the HBM in reproducing some of the damage observed in field applications. Based on the experiences gained in qualifying 12 memory types according to Fig. 3.3 [3.6, 3.2 (1993)], following procedure can be suggested for the HBM:

1. 9 ICs divided into 3 equal groups are tested at 500, 1000, and 2000 V, respectively. Taking note of the results obtained during these preliminary tests, 3 new ICs are stressed with steps of 250 V up to the voltage at which damage occurs (V_{ESD}). 3 further ICs are then tested at $V_{ESD} - 250$ V to confirm that no damage occurs.
2. The test consists of 3 positive and 3 negative pulses applied to each pin within 30 s. Pulses are generated by discharging a 100 pF capacitor through a 1.5 k Ω resistor placed in series to the capacitor (HBM), wiring inductance $< 10 \mu\text{H}$. Pulses are between pin and ground, unused pins open.
3. Before and after each test, leakage currents (when possible with the limits $\pm 1 \text{pA}$ for open and $\pm 200 \text{nA}$ for short) and electrical characteristics are measured (electrical test as after any other environmental test).

Experience shows that an electrostatic discharge often occurs between 1000 and 4000 V. The model parameters of 100 pF and 1.5 k Ω for the HBM are average values measured with humans (80 to 500 pF, 50 to 5000 Ω , 2 kV on synthetic floor and 0.8 kV on an antistatic floor with a relative humidity of about 50%). A new model for latent damages caused by ESD has been developed in [3.60 (1995)]. Protection against ESD is discussed in Sections 5.1.4 and 5.1.5.4, see also Section 3.3.4.

- a) Alignment error at a contact window (SEM, $\times 10,000$)
- b) Opens in the metallization of a 1 M DRAM bit line, due to particles present during the photolithographic process (SEM, $\times 2,500$)
- c) Cross section through two trench-capacitor cells of a 4 M DRAM (SEM, $\times 5,000$)
- d) Silver dendrites near an Au bond ball (SEM, $\times 800$)
- e) Electromigration in a 16K Schottky TTL PROM after 7 years field operation (SEM, $\times 500$)
- f) Bond wire damage (delamination) in a plastic-packaged device after $500 \times -50/+150^\circ\text{C}$ thermal cycles (SEM, $\times 500$)

Figure 3.7 Examples of SEM investigations/analyses on ICs (Rel. Laboratory at the ETH Zurich); see also Figs. 3.9 & 3.10

5. *Technological Characterization*: Technological investigations are performed to check technological and process parameters with respect to *adequacy* and *maturity*. The extent of these investigations can range from a simple check (Fig. 3.7c) to a comprehensive analysis, because of detected weaknesses. Refinement of techniques and evaluation methods for *technological characterization* is still in progress, see e.g. [3.30 - 3.67, 3.70 - 3.93]. The following is a simplified, short description of some important *technological characterization methods for VLSI ICs*:

- *Latch-up* is a condition in which an IC latches into a nonoperative state drawing an excessive current (often a short between power supply and ground), and can only be returned to an operating condition through removal and reapplication of the power supply. It is typical for CMOS structures, but can also occur in other technologies where a PNP structure appears. Latch-up is primarily induced by voltage overstresses (on signals or power supply lines) or by radiation. Modern devices often have a relatively high latch-up immunity (up to 200 mA injection current). A verification of latch-up sensitivity can become necessary for some special devices (ASICs for instance). Latch-up tests stimulate voltage overstresses on signal and power supply lines as well as power-on/power-off sequences.
- *Hot Carriers* arise in micron and submicron MOSFETs as a consequence of *high electric fields* (10^4 to 10^5 V/cm) in transistor channels. Carriers may gain sufficient kinetic energy (some eV, compared to 0.02 eV in thermal equilibrium) to surmount the potential barrier at the oxide interface. The injection of carriers into the gate oxide is generally followed by electron-hole pairs creation and causes an increasing degradation of the transistor parameters, in particular an increase with time of the threshold voltage V_{TH} which can be measured in NMOS transistors. Effects on VLSI and ULSI ICs are an increase of switching times (access times in RAMs for instance), possible data retention problems (soft writing in EPROMs) and in general an increase of noise. Degradation through hot carriers is accelerated with increasing drain voltage and lowering temperature (negative activation energy of about -0.1 to -0.2 eV). The test is generally performed under dynamic conditions, at high power supply voltages (7 to 9V) and at low temperatures (-50°C).
- *Time-Dependent Dielectric Breakdown* (TDDB) occurs in very thin gate oxide layers (< 20 nm) as a consequence of *extremely high electric fields* (10^7 - 10^8 V/cm). The mechanism is described by the thermochemical (E) model up to about 10^7 V/cm and by the carrier injection (1/E) model up to about $2 \cdot 10^7$ V/cm. An approach to unify both models has been proposed in [3.46 (1999)]. As soon as the critical threshold is reached, breakdown takes place, often suddenly. The effects of gate oxide breakdowns are increased

leakage currents or shorts between gate and substrate. The development in time of this failure mechanism depends on process parameters and oxide defects. Particularly sensitive are memories $>4\text{M}$. An *Arrhenius model* can be used for the temperature. Time-dependent dielectric breakdown tests are generally performed on special test structures (often capacitors).

- *Electromigration* is the migration of metal atoms, and also of Si at the Al/Si interface, as a result of *very high current densities*, see Fig. 3.7e for an example of a 16K TTL PROM after 7 years of field operation. Earlier limited to ECL, electromigration also occurs today with other technologies (because of scaling). The median t_{50} of the failure-free time as a function of the current density and temperature can be obtained from the empirical model given by Black [3.33], $t_{50} = B j^{-n} e^{E_a/kT}$, where $E_a = 0.55\text{ eV}$ for pure Al (0.75 eV for Al-Cu alloy), $n=2$, and B is a process-dependent constant. Electromigration tests are generally performed at wafer level on test structures. Measures to avoid electromigration are optimization of grain structure (bamboo structures), use of Al-Si-Cu alloys for the metallization and of compressive passivation, as well as introduction of multilayer metallizations.
- *Soft errors* can be caused by the process or chip design as well as by process deviations. Key parameters are MOSFET threshold voltages, oxide thickness, doping concentrations, and line resistance. If for instance, the post-implant of a silicon layer has been improperly designed, its conductivity might become too low. In this case, the word lines of a DRAM could suffer from signal reductions and at the end of the word line soft errors could be observed on some cells. As a further example, if logical circuits with different signal levels are unshielded and arranged close to the border of a cell array, stray coupling may destroy the information of cells located close to the circuit (chip design problem). Finally, process deviations can cause soft errors. For instance, signal levels can be degraded when metal lines are locally reduced to less than half of their width by the influence of dirt particles. The characterization of soft errors is difficult in general. At the chip level, an electron beam tester allows the measurement of signals within the chip circuitry. At the wafer level, single test structures located in the space between the chips (kerf) can be used to measure and characterize important parameters independently of the chip circuitry. These structures can usually be contacted by needles, so that a well equipped bench setup with high-resolution I-V and C-V measurement instrumentation would be a suitable characterization tool.
- *Data Retention* and *Program/ Erase Cycles* are important for nonvolatile memories (EPROM, EEPROM, FLASH). A test for data retention generally consists of storage (bake) at high temperature (2000 h at 125°C for plastic packages and 500 h at 250°C for ceramic packages) with an electrical test at

70°C at 0, 250, 500, 1000, and 2000 h (often using a checkerboard pattern with measurement of t_{AA} and of the margin voltage). Experimental investigation of EPROM data retention at temperatures higher than 250°C shown a deviation from the charge loss predicted by the thermionic model [3.6]. Typical values for program/erase cycles during a qualification test are 100 for EPROMs and 10,000 for EEPROMs and Flash memories.

6. *High-Temperature Storage*: The purpose of high-temperature storage is the stabilization of the thermodynamic equilibrium, and consequently of the IC's electrical parameters. Failure mechanisms related to surface problems (contamination, oxidation, contacts, charge induced failures) are activated. To perform the test, the ICs are placed on a metal tray (pins on the tray to avoid thermal voltage stresses) in an oven at 150°C for 168 h. Should solder-ability be a problem, a protective atmosphere (N_2) can be used. Experience shows that for a mature technology (design and production processes), high temperature storage produces only a very few failures (see also Section 8.2.2).
7. *Thermal Cycles*: The purpose of thermal cycles is to test the IC's ability to support rapid temperature changes. This activates failure mechanisms related to mechanical stresses caused by mismatch in the expansion coefficients of the materials used, as well as wear-out because of fatigue, see Fig. 3.7f for an example. Thermal cycles are generally performed from air to air in a two-chamber oven (transfer from one chamber to the other with a lift). To perform the test, the ICs are placed on a metal tray (pin on the tray to avoid thermal voltage stresses) and subjected to 2,000 thermal cycles from -65°C (+0, -10) to $+150^\circ\text{C}$ (+15, -0), transfer time ≤ 1 min, time to reach the specified temperature ≤ 15 min, dwell time at the temperature extremes ≥ 10 min. Should solderability be a problem, a protective atmosphere (N_2) can be used. Experience shows that for a mature technology (design and production processes), failures should not appear before some thousand thermal cycles (lower figures for power devices).
8. *Humidity or Damp Heat Test, 85/85 and pressure cooker*: The aim of humidity tests is to investigate the influence of *moisture* on the chip surface, in particular corrosion. It applies to nonhermetic (plastic) packages, and following two procedures are often used:
 - (i) Atmospheric pressure, $85 \pm 2^\circ\text{C}$ and $85 \pm 5\%$ rel. humidity (*85/85 Test*) for 500 to 2,000 h (new trend 40/93 tests for 168 to 500 h).
 - (ii) Pressurized steam, $110 \pm 2^\circ\text{C}$ or $120 \pm 2^\circ\text{C}$ or $130 \pm 2^\circ\text{C}$ and $85 \pm 5\%$ rel. humidity (*pressure-cooker test* or *highly accelerated stress test* (HAST)) for 24 to 408 h (1,000 h for silicon nitride passivation).

In both cases, a *voltage bias* is applied during exposure in such a way that power consumption is as low as possible, while the voltage is kept as high as possible (*reverse bias* with adjacent metallization lines alternatively polarized

high and low, e. g. 1h *on* / 3h *off* intermittently if power consumption is greater than 0.01W). For a detailed procedure one may refer to IEC 60749 [3.8]. In the procedure of Fig. 3.3, both 85/85 and HAST tests are performed in order to correlate results and establish (empirically) a conversion factor. Of great importance for applications is the relation between the *failure rates* at elevated temperature and humidity (e. g. 85/85 or 120/85) and at field operating conditions (e. g. 40/60). A large number of models have been proposed in the literature to empirically fit the *acceleration factor* A associated with 85/85 test

$$A = \frac{\text{failure rate } \lambda \text{ at } 85/85 (\theta_2, RH_2)}{\text{failure rate } \lambda \text{ at lower stress } (\theta_1, RH_1)}. \quad (3.1)$$

The most important of these models are

$$A = \left(\frac{RH_2}{RH_1}\right)^3 e^{\frac{E_a}{k} \left(\frac{1}{T_1} - \frac{1}{T_2}\right)}, \quad (3.2)$$

$$A = e^{E_a [C_1 (\theta_2 - \theta_1) + C_2 (RH_2 - RH_1)]}, \quad (3.3)$$

$$A = e^{\left[\frac{E_a}{k} \left(\frac{1}{T_1} - \frac{1}{T_2}\right) + C_3 (RH_2^2 - RH_1^2)\right]}, \quad (3.4)$$

$$A = e^{\left[\frac{E_a}{k} \left(\frac{1}{T_1} - \frac{1}{T_2}\right) + C_4 \left(\frac{1}{RH_1} - \frac{1}{RH_2}\right)\right]}, \quad (3.5)$$

$$A = e^{\left[\frac{1}{k} \left(\frac{E_a(RH_1)}{T_1} - \frac{E_a(RH_2)}{T_2}\right) + (RH_2 - RH_1)\right]}. \quad (3.6)$$

In Eqs. (3.2) to (3.6), E_a is the *activation energy*, k the Boltzmann constant ($8.6 \cdot 10^{-5}$ eV/K), θ the temperature in °C, T the absolute temperature (K), RH the relative humidity, and C_1 to C_4 are constants. Equations (3.2) to (3.6) are based on the *Eyring model* (Eq. (7.59)), the influence of the temperature and the humidity is multiplicative in Eqs. (3.2) to (3.5). Eq. (3.2) has the same structure as in the case of electromigration (Eq. (7.60)). In all models, the technological parameters (type, thickness, and quality of the passivation, kind of epoxy, type of metallization, etc.) appear indirectly in the activation energy E_a or in the constants C_1 to C_4 . Relationships for HAST are more empirical. From the above considerations, 85/85 and HAST tests can be used as *accelerated tests* to assess the effect of damp heat combined with bias on ICs by accepting a numerical uncertainty in calculating the acceleration factor. As a *global value* for the acceleration factor referred to operating field conditions of 40°C and 60% RH, one can assume for PSG a value between 100 and 150 for the 85/85 test and between 1,000 and 1,500 for the 120/85 test. To assure 10 years field operation at 40°C and 60% RH, PSG-ICs should thus pass without evident corrosion damage about 1,000 h at 85/85 or 100 h at 120/85. Practical

results show that *silicon-nitride glassivation* offers a much greater resistance to moisture than PSG by a factor up to 10 [3.6].

Also related to the effects of humidity is metal migration in the presence of reactive chemicals and voltage bias, leading to the formation of conductive paths (*dendrites*) between electrodes [3.36], see an example in Fig. 3.7d on p. 95. A further problem related to *plastic packaged ICs* is that of bonding a *gold wire* to an *aluminum* contact surface. Because of the different interdiffusion constants of gold and aluminum, an inhomogeneous *intermetallic layer* (Kirkendall voids) appears at high temperature and/or in presence of contaminants, considerably reducing the electrical and mechanical properties of the bond [3.53]. Voids grow into the gold surface like a plague, from which the name *purple plague* derives. Purple plague was an important reliability problem in the sixties. It propagates exponentially at temperatures greater than about 180°C. Although almost generally solved (bond temperature, Al-alloy, metallization thickness, wire diameter, etc.), verification after high temperature storage and thermal cycles is a part of a qualification test, especially for ASICs and devices in small-scale production.

Table 3.4 Indicative values for *failure modes* of electronic components (%)

Component	Shorts	Opens	Drift	Functional
Digital bipolar ICs	50 ^{*Δ}	30 [*]	—	20
Digital MOS ICs	10 ^Δ	70 [*]	—	20
Linear ICs	—	25 ⁺	—	75 ⁺⁺
Bipolar transistors	80	20	—	—
Field effect transistors (FET)	80 ^Δ	10	10	—
Diodes (Si) general purpose	80	20	—	—
Zener	70	20	10	—
Thyristors	20	20	50	10 [◇]
Optoelectronic (optocoupler)	10	50	40	—
Resistors, fixed (film)	—	60	40	—
Resistors, variable (Cermet)	—	60	30	10 [#]
Capacitors foil	15	80	5	—
ceramic	70	10	20	—
Ta (solid)	80	15	5	—
Al (wet)	30	30	40	—
Coils	20	80	—	—
Relays (electromechanical)	20	—	—	80 [†]
Quartz crystals	—	80	20	—

* input and output half each; ^Δ short to V_{CC} or to GND half each; ⁺ no output; ⁺⁺ improper output; [◇] fail to off; [#] localized wear-out; [†] fail to trip/spurious trip $\approx 3/2$

3.2.4 Reliability Tests

The aim of a *reliability test* for electronic components is to obtain information about

- early failures
- failure rate
- long-term behavior of critical parameters,
- effectiveness of screening to be performed at the incoming inspection.

The test consists in general of a *dynamic burn-in* with electrical measurements and *failure analysis* at appropriate time points (Fig. 3.3), also for some components which have not failed (check for degradation). The number (n) of devices under test can be estimated from the *predicted failure rate* λ and the *acceleration factor* A (Eq. (7.56)) in order to expect 3 to 6 failures (k) during burn-in ($n \approx k / (\lambda A t)$). Half of the devices can be submitted to a *screening* (Section 8.2.2) to better isolate *early failures*. Statistical data analyses are given in Chapter 7 and Appendix A8.

3.3 Failure Modes, Failure Mechanisms, and Failure Analysis of Electronic Components

This section introduces some basic concepts and considerations on failure modes, mechanisms, and analysis of electronic components. It aims to bring the attention to this field, important for both equipment and systems level reliability engineering. For greater details see e.g. [3.30–3.67].

3.3.1 Failure Modes of Electronic Components

A *failure mode* is the *symptom* (local effect) through which a failure is observed. Typical failure modes are *opens*, *shorts*, *drift*, *functional faults* for electronic, and brittle fracture, creep, buckling, fatigue for mechanical components. *Average values* for the relative frequency of failure modes in electronic components are given in Table 3.4, see also e.g. [3.58 (2013)]. The values given in Table 3.4 have indicative purpose and have to be completed by application specific results, as far as necessary.

The different failure modes of *hardware*, often influenced by the specific application, cause difficulties in investigating the *effect* of a given failure, and thus in the concrete implementation of *redundancy* (series if short, parallel if open). For critical situations it can become necessary to use *quad redundancy* (Section 2.3.6). Quad redundancy is the simplest *fault tolerant structure* which can accept at least one failure (short or open) of any one of the 4 elements involved in the redundancy.

3.3.2 Failure Mechanisms of Electronic Components

A *failure mechanism* is the physical, chemical, or other process that leads to a failure. A large number of failure mechanisms have been investigated in the literature, see e. g. [3.30 - 3.67, 3.70 - 3.93], in particular [3.49, 3.66, 3.67] for recent publications. For some of them, appropriate physical explanations have been found. For others, models are *empirical* and often of limited validity. Evaluation of models for failure mechanisms should be developed in two steps:

(i) *verify the physical validity of the model and (ii) give its analytical formulation with the appropriate set of parameters to fit the model to the data.*

In any case, *experimental verification* of the model should be performed with at least a second, independent experiment, and *limits of the model* should be clearly indicated. The two most important models used to describe failure mechanisms of electronic components, the *Arrhenius* and *Eyring models*, are introduced in Section 7.4 with *accelerated tests* (Eqs. (7.56)-(7.60)). Models to describe the influence of temperature and humidity in damp heat tests have been given with Eqs. (3.2) - (3.6). A new model for latent damages caused by ESD is given in [3.60 (1995)]. Table 3.5 summarizes some important failure mechanisms for ICs, specifying influencing factors and the approximate distribution of the failure mechanisms for plastic-packaged ICs in industrial applications (see also pp. 93 - 100 and 333 - 334). The percentage of misuse and mishandling failures can vary over a large range (20-80%) depending on the design engineer using the device, the equipment manufacturer and the end user. For ULSI-ICs one can expect that the percentage of failure mechanisms related to *oxide breakdown* and *hot carriers* will grow in the future. Comments on failure mechanisms are also in Sections 3.4, 8.2 & 8.3.

3.3.3 Failure Analysis of Electronic Components

The aim of a *failure analysis* is to investigate the *failure mechanisms* and find out possible *failure causes*. A procedure for failure analysis of complex ICs (from an user's point of view) is shown in Fig. 3.8. It is based on the following steps:

1. *Failure detection and description*: A careful description of the failure, as observed in situ, and of the surrounding circumstances (operating conditions at the failure occurrence) is important. Also necessary are information on the IC itself (type, manufacturer, manufacturing data, etc.), on the electrical circuitry in which it was used, on the operating time, and if possible on the tests to which the IC was submitted previous to the final use (evaluation of possible damages, e. g. ESD). In a few cases the failure analysis procedure can be terminated, if evident mishandling or misuse failure can be confirmed.
2. *Nondestructive analysis*: The nondestructive analysis begins with an *external visual inspection* (mechanical damage, cracks, corrosion, burns, overheating, etc.), followed by an *x-ray inspection* (evident internal fault or damage) and a

Table 3.5 Basic failure mechanisms of ICs in plastic package (see also pp. 93- 100 and 333- 334)

Failure mechanism	Short description	Causes	Acceleration factors	%
Bonding • Fatigue • Purple plague	Mechanical fatigue of bonding wires or bonding pads because of thermomechanical stress (also because of vibrations at the resonance frequency for hermetically sealed devices)	Different expansion coefficients of the materials in contact (for hermetically sealed devices also wire resonance)	Thermal cycles with $\Delta\theta > 150^\circ\text{C}$ (vibrations at res. freq. for hermetic dev.)	5
	Formation of an intermetallic layer at the interface between wire (Au) and metallization (Al) causing a brittle region (voids in Au due to diffusion) which can provoke bond lifting	Different interdiffusion constants of Au and Al, bonding temperature, contamination, too thick metallization	Temperature $> 180^\circ\text{C}$ ($E_a = 0.7 - 1.1 \text{ eV}$)	
Surface • Charge spreading (leakage currents, inversion)	Charge spread laterally from the metallization or along the isolation interface, resulting in an inversion layer outside the active region which can provide for instance a conduction path between two diffusion regions	Contamination with Na^+ , K^+ , etc., too thin oxide layer (MOS), package material	E, θ_j ($E_a = 0.5 - 1.2 \text{ eV}$, up to 2 eV for linear ICs)	5
Metallization • Corrosion • Metal migration	Electrochemical or galvanic reaction in the presence of humidity and ionic contamination (P, Na, Cl etc.), critical for PSG (SiO_2) passivation with $> 4\% \text{ P}$ ($< 2\% \text{ P}$ gives cracks)	Humidity, voltage, contamination (N^+ , Cl^- , K^+), cracks or pinholes in the passivation	RH, E, θ_j ($E_a = 0.5 - 0.7 \text{ eV}$)	10
	Migration of metal atoms in the presence of reactive chemicals, water, and bias, leading to conductive paths (dendrites) between electrodes	Humidity, voltage, migrating metals (Au, Ag, Pd, Cu, Pb, Sn), contaminant (encapsulant)		
• Electromigration (EM)	Migration of metal atoms (also of Si at contacts) in the direction of the electron flow, creating voids or opens in the structure	Current density ($> 10^6 \text{ A/cm}^2$), temperature gradient, anomalies in the metallization	j^n, θ_j ($n=2, E_a = 0.55 - 0.75 \text{ eV}$ for Al, $n=1-2, E_a = 0.7 - 1.1 \text{ eV}$ for Cu)	
Oxide • Time-dependent dielec. breakdown (TDDB) • Ion migration (parasitic transistors, inversion) • Negative bias temperature instability (NBTI)	Breakdown of thin oxide layers occurring suddenly when sufficient charge has been injected to trigger a runaway proc. Carrier injection in the gate oxide because of E and θ_j ; creation of charges in the SiO_2/Si -interface Generation of traps in the gate oxide - Si substrate interface at elevated temp. and negative gate voltage (PMOS devices)	High voltages, thin oxides, oxide defects ($10^7 - 10^8 \text{ V/cm}$) Contamination with alkaline ions, pinholes, oxide or diffusion defects High temperature, high negative gate voltages, thin oxide	E, θ_j ($e^{(V_g - V_o) \gamma_{TDDB}}, E_a = 0.6 - 0.9 \text{ eV}$ for intrinsic oxide) E, θ_j ($e^{(V_g - V_o) \gamma_{NBTI}}, E_a = 0.1 - 0.84 \text{ eV}$)	10
Others • Intermetallic compound • hot carriers (HCI) • α -particles • Latch-up, etc.	Formation of intermet. layer between metal. (Al) & substr. (Si) Injection of electrons because of high E ($10^4 - 10^5 \text{ V/cm}$) Generation of electron-hole pairs by α -particles (DRAMs) Activation of PNPN paths	Mask defects, overheating, pure Al Dimensions, diffusion profiles, E Package material, external radiation PNPN paths	$E, \theta_j, \text{r.h. cycl. } (\Delta\theta > 200^\circ\text{C})$ E (-0.1 to -0.2 eV , -50°C) External radiation Voltage overstress	10
Misuse / Mishandling	Electrical (ESD/EOS), thermal, mech., or climatic overstress	Application, design, handling, test	—————	60
E = electric field, RH = relative humidity, j = current density, θ_j = junction temperature, passivation (= glassivation), % = indicative distribution in percent				100

careful *electrical test* (Section 3.2.1). For ICs in hermetic packages, it can also be necessary to perform a seal test and if possible a dew-point test. The result of the nondestructive analysis is a careful description of the *external failure mode* and a first information about possible failure causes and mechanisms. For *evident failure causes*, the failure analysis can be terminated.

3. *Semidestructive analysis*: The semidestructive analysis begins by *opening the package*, mechanically for hermetic packages and with wet chemical (or plasma etching) for plastic ICs. A careful *internal visual* check is then performed with optical microscopes, conventional 1000× or stereo 100×. This evaluation includes opens, shorts, state of the passivation / glassivation, bonding, damage due to ESD, corrosion, cracks in the metallization, electromigration, particles, etc. If the IC is still operating (at least partially), other procedures can be used to *localize* more accurately the fault on the die. Among these are the *electron beam tester* (or other voltage contrast techniques), *liquid crystals* (LC), *infrared thermography* (IRT), *emission microscopy* (EMMI), or one of the methods to detect irregular recombination centers, like *electron beam induced current* (EBIC) or *optical beam induced current* (OBIC). For further investigations it is then necessary to use a *scanning electron microscope* (SEM). The result of the semidestructive analysis is a careful description of the *internal failure mode* and an improved information about possible failure causes and failure mechanisms. In the case of *evident failure causes*, the failure analysis procedure can be terminated.
4. *Destructive Analysis*: A destructive analysis is performed if the previous investigations yield unsatisfactory results and there is a *realistic chance* of success through further analyses. After removal of the passivation and other layers (as necessary) an inspection is carried out with a *scanning electron microscope* supported by a material investigation (e. g. *EDX spectrometry*). Analyses are then continued using methods of microanalysis (electron microprobe, ion probe, diffraction, etc.) and performing *microsections*. The destructive analysis is the last possibility to recognize the *original failure cause* and the *failure mechanisms* involved. However, it cannot guarantee success, even with skilled personnel and suitable analysis equipment.
5. *Failure mechanism analysis*: This step implies a correct interpretation of the results from steps 1 through 4. Additional investigations have to be made in some cases, but questions related to failure mechanisms can still remain open. In general, *feedback to the manufacturer* at this stage is mandatory.
6. *Final report*: All relevant results of the steps 1 to 5 above and the agreed corrective actions must be included in a (short and clear) final report.
7. *Corrective actions*: Depending on the identified failure causes, appropriate corrective actions should be started. These have to be discussed with the IC manufacturer as well as with the equipment designer, manufacturer, or user depending on the failure causes which have been identified.

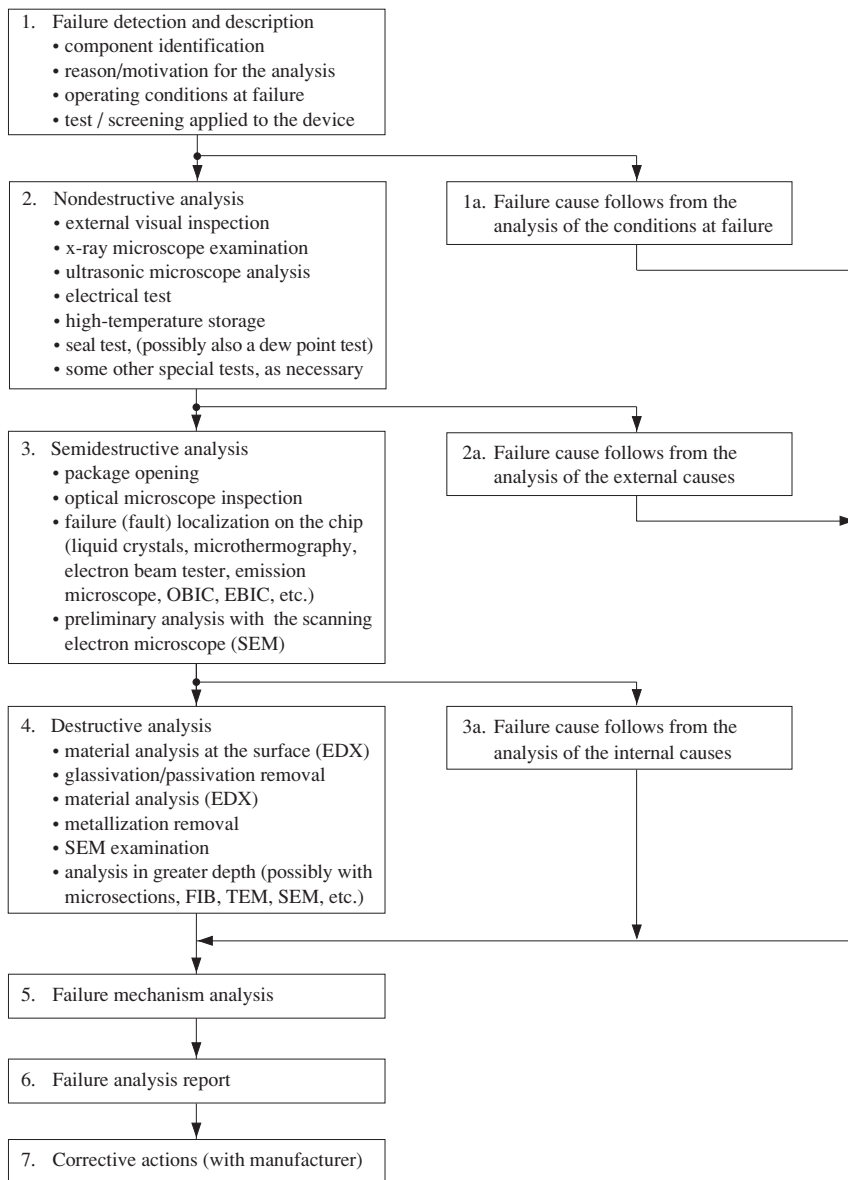


Figure 3.8 Basic procedure for failure analysis of complex ICs from an user's point of view (see e. g. [3.48 (2005/2009)] for greater details from a manufacturing's point of view)

The failure analysis procedure described in Section 3.3.3 for ICs can be applied to other electronic or mechanical components and extended to cover populated printed circuit boards (PCBs) as well as subassemblies or assemblies.

3.3.4 Present VLSI Production-Related Reliability Problems

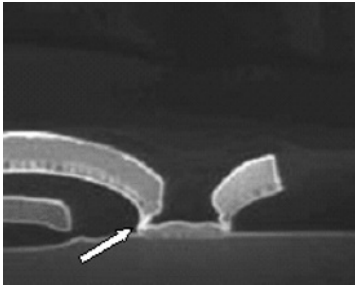
Production-related potential reliability problems, i.e., flaws or damages which can lead to failures, can occur for VLSI devices at packaging or soldering level (Fig. 3.10), as well as on silicon dies. Those on dies are often more difficult to identify. Following examples show some cases for production-related potential reliability problems on silicon dies, in grown difficulty with respect to their identification [3.48 (2005/2009)], see also Fig. 3.7a & b for further examples).

Fig. 3.9a shows a contact step coverage flaw. The contact to a diffusion in bulk silicon is made by the first metal layer, which usually is protected by a barrier against Al penetration into bulk-silicon. However, the first metal layer often must adapt itself to some topography. Design rules make sure that the contact is flat enough. However, if the contact slopes are too steep (e.g. etching process problem) the step coverage may be reduced. In this case, electric contact is often still given, but melting or electromigration may start, leading to a failure. OBIRCH (optical beam induced resistivity change) can help to detect such weak contacts.

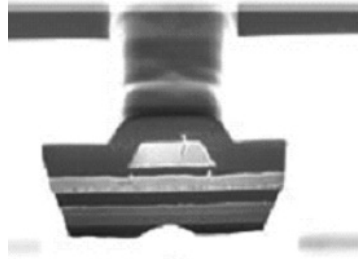
Fig. 3.9b shows a wafer processing flaw. Semiconductor devices include at least one poly-Si layer, which usually performs MOS-transistor gates. It is isolated versus bulk silicon by a thin (some nm) gate-oxide, or by a more thick field oxide in active regions. The isolation against further poly-Si layers is given by a self-grown re-oxidation of the poly-Si surface and (in part) by doped silicate-glass (PSG, BPSG). In the structuration process of poly-Si (usually photolithography and plasma etching), an improper etching process may result in poly-Si *residues* or particles, which during subsequent re-oxidation form an irregular and thin oxide around themselves. A short at $t=0$ will be avoided; however, a latent short path is created and a small voltage peak may be enough to breakdown the oxide causing a leakage path.

Figs. 3.9c and 3.9d show a ESD damage giving failures at $t=0$ or *latent failures*, formerly considered as mechanical surface damage. Silicon dies are often delivered as wafers to customers which perform subsequent pre-assembly processes (wafer dicing, back grinding, and pick & place). These operations can include great risks for electrostatic discharge from robotics equipment to the device via device passivation (e.g. when the picker setup of the pneumatic handler moves rapidly on a Teflon bearing). The term ESDFOS (electrostatic discharge from outside-to-surface) has been introduced to describe this failure cause. Like a lightning-strike, the electrostatic spark comes onto the passivation, cracks it, melts the aluminum of the top metal and cracks the interlevel dielectric (ILD), where the metal underneath locally melts and penetrates into the crack. Depending from the degree of Al penetration, the damage causes a failure at $t=0$ or a latent failure. Periodic audits with survey and location of air ionizer fans, grounding concepts, materials, etc. is an effective method against this damage.

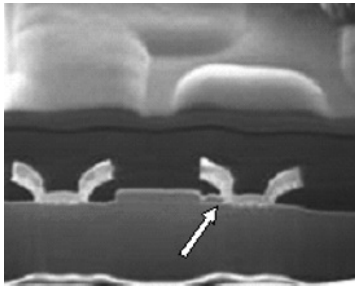
Further examples related to wafer sawing, poly-Si residues, and RFID devices are in [3.48 (2008, 2009)].



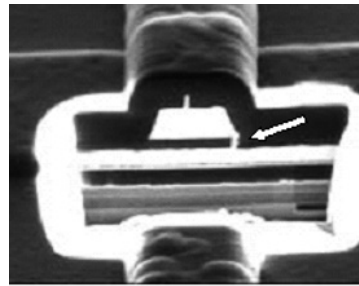
a) A steep slope topography causing a bad contact coverage with Al ($\times 5000$)



c) Latent ESDFOS damage, see also Fig. 3.9d ($\times 5000$)



b) Slightly oxidized poly residue (small white line) buried between a poly-Si-gate and a neighbored contact ($\times 5000$)



d) Short of two top metal layer as consequence of an ESDFOS damage ($\times 5000$)

Figure 3.9 Examples of *production-related* (hidden) *potential reliability problems* in Si-dies [3.48]; see also Figs. 3.7 & 3.10

3.4 Qualification Tests for Electronic Assemblies

As outlined in Section 3.2 for components, the purpose of a *qualification test* is to verify the suitability of a given item (electronic assemblies in this section) for a stated application. Such a qualification involves *performance, environmental & reliability* tests, and has to be supported by a careful *failures (faults) analysis*. To be efficient, it should be performed on *prototypes* which are *representative* for the production line in order to check not only the design but also the *production process*. Results of qualification tests are an important input to the *critical design review* (Table A3.3). This section deals with *qualification tests of electronic assemblies*, in particular of *populated printed circuit boards (PCBs)*.

The aim of the *performance test* is similar to that of the *characterization* discussed in Section 3.2.2 for complex ICs. It is an experimental analysis of the electrical properties of the given assembly, with the purpose of investigating the influence of the most *relevant electrical parameters* on the behavior of the assembly at *different ambient temperatures and power supply conditions* (see Section 8.3 for considerations on electrical tests of PCBs).

Environmental tests have the purpose of submitting the given assembly to stresses which can be more severe than those encountered in the field, in order to investigate *technological limits* and *failure mechanisms* (see Section 3.2.3 for complex ICs). The following *procedure*, based on the experience with a large number of equipment [3.76], can be recommended for assemblies of mixed technology used in *high reliability* (or safety) applications (total ≥ 10 assemblies):

1. Electrical behavior at extreme temperatures with functional monitoring, 100 h at -40°C , 0°C , and $+80^{\circ}\text{C}$ (2 assemblies, as reference also for failure analysis).
2. 4,000 thermal cycles $-40/+120^{\circ}\text{C}$ with functional monitoring, $\leq 5^{\circ}\text{C}/\text{min}$ or $\geq 20^{\circ}\text{C}/\text{min}$ within the components according to the field application, $\geq 10\text{min}$ dwell time at -40°C and $\geq 5\text{min}$ at 120°C after the thermal equilibrium has been reached within $\pm 5^{\circ}\text{C}$ (total dwell times of about 20 & 10 min, 40 & 20 min for lead-free solder; ≥ 3 assemblies, metallographic analysis after 2,000 and 4,000 cycles).
3. Random vibrations at low temperature, 1h with $2 - 6 g_{rms}$, 20 – 500 Hz at -20°C (2 assemblies).
4. EMC and ESD tests (2 assemblies).
5. Humidity tests, 240h 85/85 test (1 assembly).

Experience shows [3.76] that electronic equipment often behaves well even under extreme environmental conditions (operation at $+120^{\circ}\text{C}$ and -60°C , thermal cycles $-40/+120^{\circ}\text{C}$ with up to $60^{\circ}\text{C}/\text{min}$ within the components, humidity test 85/85, cycles of 4h 95/95 followed by 4h at -20°C , random vibrations 20 – 500 Hz at $4 g_{rms}$ and -20°C , ESD/EMC with pulses up to 15 kV). However, problems related to crack propagation *in solder joints* appear, and metallographic investigations on more than 1,000 microsections [3.76] confirm that *cracks* in solder joints are initiated by production flaws (Fig. 3.10 d – f) or by microvoids caused by creep. The above holds in particular for Sn-Pb solder. For lead-free solder, greater sensitivity to fast thermal cycles and vibrations can be expected, see e.g. [3.79 (2011), 3.90].

Many of the production flaws with *inserted components* (Fig. 3.10 a – c) cause only *minor* reliability problems and can often be avoided (for instance, voids can be eliminated by a better plating of the through-holes). Since even voids up to 50% of the solder volume do not severely reduce the reliability of solder joints, it is preferable to *avoid rework*. Poor wetting of the leads or the excessive formation of brittle intermetallic layers are *major* potential reliability problems for solder joints. This last kind of defects must be avoided through a better production process.

More critical are *surface mount devices* (SMD), for which clear *crack propagation* in solder joints often begins after some few thousand thermal cycles. Extensive investigations [3.79(1996)] show that crack propagation is almost independent of pitch, at least down to a pitch of 0.3 mm, and that solder joints of IC's with shrinking pitches are less critical (due to leads flexibility). A new model based on *creep* (intended as elevated temperature, time dependent deformation) to describe the *viscoplastic behavior* of SMT solder joints, proposed in [3.92] for Sn62Pb36Ag2, applies also to lead-free solder alloys, see e.g. [3.79(02, 05, 08, 11)]. The model outlines the strong impact of *deformation energy* on *damage evolution*. Besides *diffusion creep*, at very low stress (thermal gradient), basically two different *deformation mechanisms* are present, *grain boundary sliding* (GBS) at low thermal gradient and *dislocation climbing* (DC) at high thermal gradient. Each mechanism causes microvoids, in locally restricted recrystallized areas within the joint, that evolve to cracks. The strain rate in steady-state can be described by an Eyring model similar as for electromigration (Eq. (7.60)) with two additive terms and activation energies $E_{aG\text{SB}}$ & E_{aDC} [3.92,3.79(02,05,08,11)]; other models are e.g. in [3.90]. Hence,

attention must be paid in defining environmental and reliability tests or screening procedures for assemblies in SMT, mandatory is to activate only failure mechanisms which would also be activated in the field.

Dwell time during thermal cycles also plays an important role. It must be long enough to allow *relaxation* of the stresses, and depends on temperature, temperature swing, and materials stiffness; dwell times of about 20 min at -20°C and 10 min at 100°C (40 and 20min for lead-free) seems reasonable.

Reliability tests at assembly and higher integration level have as a primary purpose the detection of all *early failures* (Section 7.7) and an estimation of the *failure rate* (Section 7.2.3). Precise information on the failure rate shape is seldom possible from reliability tests, because of cost and time limits. If reliability tests are necessary, the following procedure can be used (total ≥ 8 assemblies):

1. 4,000 h dynamic burn-in at 80°C ambient temperature (≥ 2 assemblies, functional monitoring, intermediate el. tests at 24, 96, 240, 1,000, and 4,000 h).
2. 5,000 thermal cycles $-20/+100^{\circ}\text{C}$ with $\leq 5^{\circ}\text{C}/\text{min}$ for applications with slow heat up and $\geq 20^{\circ}\text{C}/\text{min}$ for rapid heat up, dwell time ≥ 10 min at -20°C and ≥ 5 min at 100°C after the thermal equilibrium has been reached within $\pm 5^{\circ}\text{C}$ (total dwell times of about 20 & 10 min, 40 & 20 min for lead-free solder; ≥ 3 assemblies, metallographic analysis after 1,000, 2,000, and 5,000 cycles; crack propagation can be estimated using a Coffin-Manson relationship of the form $N = A\varepsilon^n$ with $\varepsilon = (\alpha_B - \alpha_C)/\Delta\theta/d$, the parameter A has to be determined experimentally at different temperature swings).
3. 5,000 thermal cycles $0/+80^{\circ}\text{C}$, with temperature gradient as in point 2 above, combined with random vibrations $1g_{\text{rms}}$, 20–500 Hz (≥ 3 assemblies, metallographic analysis after 1,000, 2,000, and 5,000 cycles).

- a) Void caused by an s-shaped pin gassing out in the area A ($\times 20$)
- b) Flaw caused by the insertion of the insulation of a resistor network ($\times 20$)
- c) Defect in the copper plating of a hole in a multilayer printed board ($\times 50$)
- d) A row of voids along the pin of an SOP package ($\times 30$)
- e) Soldering defect in a surface mounted resistor ($\times 30$)
- f) Detail A of Fig. 3.10e ($\times 500$)

Figure 3.10 Examples of *production flaws* responsible for the initiation of *cracks in solder joints* **a) - c)** inserted devices, **d) - f)** SMD (Rel. Laboratory at the ETH Zurich); see also Figs. 3.7 & 3.9

Thermal cycles with random vibrations highly activate failure mechanisms at the assembly level, in particular *crack propagation in solder joints*. If such a stress clearly occurs in the field, insertion technology would be more appropriate for *high reliability or safety applications*. Figure 3.11 shows a comparative investigation of crack propagation [3.79 (1993)].

Preliminary results show that lead-free solder joints are more sensitive than Sn-Pb solder joints to manufacturing flaws or defects, in particular, to *mechanical vibrations and fast thermal cycles*, see e.g. [3.79 (02, 05, 11), 3.90]. For this reason, tests and / or screening on assemblies (PCBs) manufactured with lead-free solder should take care of the stress really encountered in the field (see also Sections 5.1.5.4 and 8.3).

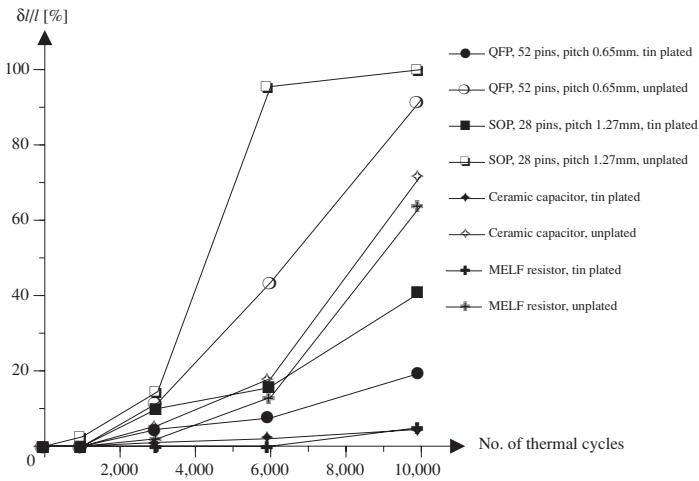


Figure 3.11 Crack propagation in different SMD solder joints as a function of the number of thermal cycles ($\delta l/l$ = crack length in % of the solder joint length, mean over 20 values, thermal cycles $-20/+100^\circ\text{C}$ with $60^\circ\text{C}/\text{min}$ inside the solder joint; Rel. Laboratory at the ETH Zurich)

4 Maintainability Analysis

At equipment and systems level, *maintainability* has a great influence on *reliability* and *availability*. This holds, in particular, if *redundancy* has been implemented and redundant parts *can be repaired (restored) on line*, i.e., without interruption of operation at system level. Maintainability is thus an important parameter in the optimization of *reliability*, *availability*, and *life-cycle cost*. Achieving high maintainability in complex equipment and systems requires appropriate activities which must be started *early in the design & development phase* and be coordinated by a *maintenance concept*. To this concept belong *failure detection & localization* (built-in tests), *partitioning* of equipment and systems into (as far as possible) independent *line replaceable units*, and *logistic support*. A maintenance concept has to be *tailored* to the equipment or system considered. Its definition and realization must be actively supported by the project manager. After some basic concepts, Section 4.2 deals with *a maintenance concept for complex equipment and systems*. Section 4.3 discusses maintainability aspects in *design reviews*. Section 4.4 gives methods and tools for *maintainability prediction*. *Spare parts provisioning & repair strategies* are carefully considered in Sections 4.5 & 4.6; *cost optimization* in Sections 4.5-4.7. *Design guidelines* for maintainability are given in Section 5.2. The influence of preventive maintenance, imperfect switching, and incomplete coverage on system's reliability & availability is investigated in Section 6.8. For simplicity, *delays* (administrative, logistic, technical) are neglected and *repair* is thus used for *restoration*.

4.1 Maintenance, Maintainability

Maintenance defines all those *actions* performed on the item to *retain* it in or to *restore* it to a specified state. Maintenance includes thus *preventive maintenance*, carried out at scheduled intervals, according to prescribed procedures to reduce the probability of failures or the degradation of the functionality of the item, and *corrective maintenance*, initiated after fault (defect or failure) detection and intended to bring the item into a state in which it can again perform the required function (Fig. 4.1). The aim of preventive maintenance must also be to detect and repair *hidden faults*, for instance undetected failures in redundant elements. Corrective maintenance is also known as *repair* (restoration) and can include any or all of following steps: *detection* (recognition), *localization* (isolation), *correction* (disassemble, remove, replace, reassemble, adjust), and *function checkout* (Fig. 4.1).

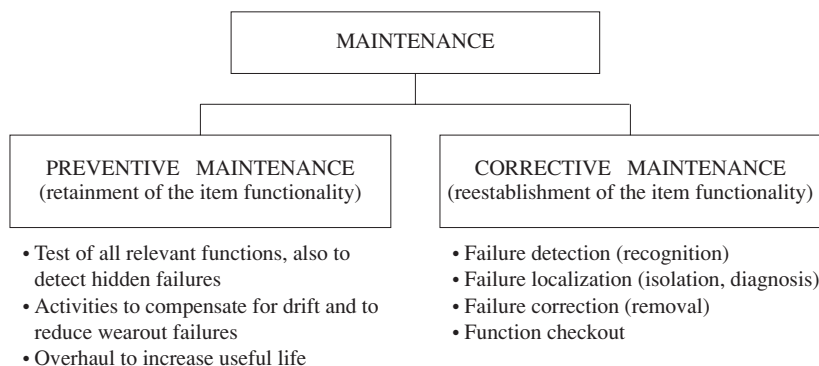


Figure 4.1 Basic *maintenance tasks*, disregarded from administrative, logistic, and technical delays (*fault* is to use if *failures and defects* have to be considered, allowing *errors / flaws* as possible causes as well)

The time elapsed from the failure occurrence until the start-up after function checkout, including all delays (administrative, logistic, technical), is often denoted as *restoration time* (see [A1.4] for a comprehensive maintenance time diagram). For simplicity, in this book delays are neglected (except in Example 6.7 (p. 203) and Fig. A7.12 (p. 512)); thus, *repair* will be used for *restoration*. The situation in which only a part of the item is repaired (minimal repair) is considered in Section 4.6.2.

Maintainability is a characteristic of the item, expressed by the *probability* that *preventive maintenance* (serviceability) or *repair* (repairability) of the item will be performed within a stated time interval by *given procedures and resources*. If τ' and τ'' are the (random) times required to carry out a repair and a preventive maintenance, respectively, then

$$\text{Repairability} = \Pr\{\tau' \leq x\} \quad \text{and} \quad \text{Serviceability} = \Pr\{\tau'' \leq x\}. \quad (4.1)$$

Considering τ' and τ'' as *interarrival times*, the variable x is used instead of t in Eq. (4.1). For a rough characterization, the means (expected values) of τ' and τ''

$$E[\tau'] = \text{MTTR} = \text{mean time to repair (mean time to restoration)}$$

$$E[\tau''] = \text{MTTPM} = \text{mean time to preventive maintenance}$$

are often used. Assuming x as a parameter, Eq. (4.1) gives the *distribution functions* of τ' and τ'' , respectively. These distribution functions characterize the *repairability* and the *serviceability* of the item considered. Experience shows that τ' and τ'' often exhibit a *lognormal distribution* (Eq. (A6.110)). The typical shape of the corresponding density is shown in Fig. 4.2. A characteristic of the lognormal density is the sudden increase after a period of time in which its value is practically zero, and the relatively fast decrease after reaching the maximum (modal value x_M).

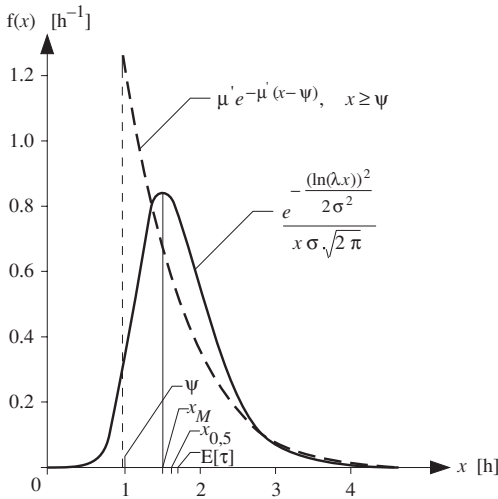


Figure 4.2 Density of the *lognormal* distribution function for $\lambda = 0.6 \text{ h}^{-1}$ and $\sigma = 0.3$ (dashed is the approximation given by a shifted exponential distribution with same mean)

This shape can be accepted, taking into consideration the main terms of a repair time (Fig. 4.1). However, calculations using a lognormal distribution can become time-consuming. In practical applications it is therefore useful to distinguish between one of the following two situations:

1. *Investigation of maintenance times*, often under assumption of ideal logistic support: In this case, the actual distribution function must be considered, see Sections 7.3 and 7.5 for some examples with a lognormal distribution.
2. *Investigation of the reliability and availability of repairable systems*: The exact shape of the repair time distribution has in general less influence on the reliability and availability values at system level, as long as the *MTTR* is *unchanged* and $MTTR \ll MTF$ holds (Examples 6.8, 6.9, 6.10); in this case, the actual repair time distribution function can often be *approximated* by an exponential function *with same mean* (Example 6.10).

A refinement of Point 2 above, is to use a shifted exponential distribution function (Examples 6.9 & 6.10, pp. 206 & 207). Figure 4.2 shows (dashed) an example with

$$\psi = x_M - \sqrt{\text{Var}[\tau']} = e^{-\sigma^2} / \lambda - (\sqrt{e^{2\sigma^2} - e^{\sigma^2}}) / \lambda.$$

The parameter μ' of the exponential d.f. follows from the equality of the mean values

$$MTTR = e^{\sigma^2/2} / \lambda = \psi + 1/\mu' \quad \rightarrow \quad \mu' = \lambda / (e^{\sigma^2/2} - \lambda\psi). \tag{4.2}$$

For the numerical example given in Fig. 4.2 ($\lambda = 0.6\text{h}^{-1}$, $\sigma = 0.3$; $MTTR \approx 1.75\text{h}$, $\text{Var} \approx 0.29\text{h}^2$) one obtains $\psi \approx 0.99\text{h}$ and $\mu' \approx 1.32\text{h}^{-1}$. A shift which considers equal mean and variance leads to $\mu' \approx 1.9\text{h}^{-1}$ & $\psi \approx 1.2\text{h}$. For a deeper investigation, one can refer to Examples 6.8-6.10. In some cases, an Erlang distribution (Eq. (A6.102)) with $\beta \geq 3$ can be assumed for repair times, yielding simple results.

As in the case of the failure rate $\lambda(x)$, for a statistical evaluation of repair times (τ') it would be preferable to omit data attributable to *systematic failures*. For the remaining data, a *repair rate* $\mu(x)$ can be obtained from the distribution function $G(x) = \Pr\{\tau' \leq x\}$, with density $g(x) = dG(x)/dx$, as per Eq. (A6.25)

$$\mu(x) = \lim_{\delta x \downarrow 0} \frac{1}{\delta x} \Pr\{x < \tau' \leq x + \delta x \mid \tau' > x\} = -\frac{g(x)}{1 - G(x)}, \quad (4.3)$$

(considering that τ' starts anew at each repair (restoration), x is used instead of t).

Maintenance is often performed by the user; thus, in evaluating the maintainability *achieved in the field*, the influence of the *logistic support* must be considered. *MTTR requirements* are discussed in Appendix A3.1. *MTTR estimation and demonstration* is considered in Section 7.3.

4.2 Maintenance Concept

Like for reliability, maintainability must be *built* into equipment and systems during the *design and development phase*. This, in particular, because maintainability cannot be easily predicted by analytical methods, and a maintainability improvement often requires important changes in layout or construction of the item (system) considered. For these reasons, attaining a prescribed maintainability in complex equipment and systems generally requires the *planning* and *realization* of a *maintenance concept*. Such a concept must be supported by the project manager, and deals with the following aspects (see e. g. [4.18] for greater details):

1. Fault *detection* and *localization*, including checkout after repair (localization can be subdivided in isolation and diagnosis, and fault is used to consider failures and defects).
2. Partitioning of the equipment or system into independent *line replaceable units* (LRUs), i.e., in spare parts at equipment and systems level (*line repairable*, *last repairable*, or *last replaceable* is often used for *line replaceable*).
3. Preparation of the user documentation (operating & maintenance manuals).
4. Training of operating and maintenance personnel.
5. Logistic support for the user, including after-sales service.

This section introduces the above points for the case of *complex equipment and systems with high maintainability requirements*.

4.2.1 Fault Detection (Recognition) and Localization

For complex equipment and systems, *detection* of partial faults (failures and defects) or of *hidden faults* (e. g. failures of redundant elements) can become difficult. For this reason, a *status test*, initiated by operating personnel, or an *operation monitoring*, running autonomously, must often be implemented. Properties, advantages, and disadvantages of both methods are summarized in Table 4.1. The choice between a *status test* or a more complete *operating monitoring* must consider cost, reliability, availability, and safety requirements at system level.

The goal of *fault localization* (isolation and diagnosis) is to isolate faults (failures and defects) down to the *line replaceable units* (LRUs), i.e., to the part which is considered as a *spare part* at equipment and systems level. LRUs are generally assemblies, e. g. populated printed circuit board, or units which for repair purposes are considered as an *entity* and replaced on a *plug-out / plug-in basis* to reduce repair times. Repair of LRUs is generally performed by specialized personnel and repaired LRUs are stored for *reuse*. Fault isolation should be performed using *built-in test* (BIT) facilities, if necessary supported by *built-in test equipment* (BITE). Use of external special tools should be avoided, however *check lists* and portable test equipment can be useful to limit the amount of built-in facilities.

Fault *detection* and fault *localization* are closely related. They characterize the *testability* and should be considered together using *common* hardware and/ or software. A high degree of automation should be striven for, and test results should

Table 4.1 Semiautomatic and automatic *fault* (failures and defects) *detection and localization*

	Status Test		Operation Monitoring
	Rough (quick test)	Complete (functional test)	
Properties	<ul style="list-style-type: none"> • Testing of all important functions, if necessary with help of external test equipment • Initiated by the operating personnel, then runs automatically 	<ul style="list-style-type: none"> • Periodic testing of all important functions • Initiated by the operating personnel, then runs automatically or semi-autom. (possibly without external stimulation or test equipment) 	<ul style="list-style-type: none"> • Monitoring of all important functions and automatic display of complete and partial faults • Performed with built-in means (BIT/BITE)
Advantages	<ul style="list-style-type: none"> • Lower cost • Allows fast checking of the functional conditions 	<ul style="list-style-type: none"> • Gives a clear status of the functional conditions of the item • Allows fault localization down to LRU level 	<ul style="list-style-type: none"> • Runs automatically on-line, i. e. in background • Allows fault localization down to LRU level
Drawbacks	<ul style="list-style-type: none"> • Limited fault localization (isolation and diagnosis) capability 	<ul style="list-style-type: none"> • Relatively expensive • Runs generally off-line (i. e. not in background) 	<ul style="list-style-type: none"> • Expensive

LRU = line replaceable unit; BIT = built-in test; BITE = built-in test equipment

be automatically recorded. A one-to-one correspondence between test messages and content of the *user documentation* (operating and maintenance manuals) must be assured.

Built-in tests (BIT) should be able to detect and localize also *hidden faults* (e. g. failures and defects in redundant elements) as well as *software defects*. This ability is generally characterized by the following *testability* parameters:

- degree of fault *detection* (*coverage*, e. g. 99% of all relevant failures),
- degree of fault *localization* (e. g. down to LRUs),
- *correctness* of the fault localization (e. g. 95%),
- test *duration* (e. g. 1s).

The first two parameters can be expressed by a *probability*, and distinction between *failures* and *defects* is important. As a measure of the *correctness* of the fault isolation capability, one can use the ratio between the number of correctly isolated faults and the number of isolation tests performed. This figure, similar to that of *test coverage*, must often remain at an empirical level, because of the lack of exact information about the defects and failures really present in the item considered. For the test duration, it is generally sufficient to work with mean values. *Failure* (fault) *modes* analysis methods (FMEA /FMECA, FTA, cause-to-effect charts, etc.) are useful to check the effectiveness of built-in facilities (Section 2.6). Models for incomplete failure (fault) coverage are investigated in Section 6.8.4.

Built-in test facilities, in particular built-in test equipment (BITE), must be defined taking into consideration not only of price/performance aspects but also of their *impact* on the *reliability* and *availability* of the equipment or system in which they are used. Standard BITE can often be integrated into the equipment or system considered. However, project specific BITE is generally more efficient than standard solutions. For such a selection, the following aspects are important:

1. *Simplicity*: Test sequences, procedures, and documentation should be as easy as possible.
2. *Standardization*: The greatest possible standardization should be striven for, in hardware and software.
3. *Reliability*: Built-in facilities should have a failure rate of at least one order of magnitude lower than that of the equipment or system in which they are used; their failure should not influence the item's operation (FMEA/FMECA).
4. *Maintenance*: The maintenance of BIT/BITE must be simple and should not interfere with that of the equipment or system; the user should be connected to the *field data change service* of the manufacturer.

For some applications, it is important that fault localization (or at least part of the diagnosis) can be *remotely controlled*. Such a requirement can often be satisfied, if stated early in the design phase. *Remote diagnosis* must be investigated on a case-by-case basis, using results from a careful failure modes and effects analysis (FMEA).

A further step on above considerations leads to maintenance concepts which allow automatic or semiautomatic *reconfiguration* of the item after failure.

Preliminary investigations on a new approach for mission oriented high safety systems (superimposing periodic check to the preventive maintenance) are in [4.26]; see also [4.4] for diagnostic aspects.

Design guidelines for maintainability are given in Section 5.2. Effects of imperfect switching and incomplete coverage are investigated in Section 6.8.

4.2.2 Equipment and Systems Partitioning

The consequent *partitioning* of complex equipment and systems into (as far as possible) independent *line replaceable units* (LRUs) is important for good maintainability. Partitioning must be performed *early in the design phase*, because of its impact on layout and construction of the equipment or system considered. LRUs should constitute *functional units* and have *clearly defined interfaces* with other LRUs. Ideally, LRUs should allow a *modular construction* of the equipment or system, i. e., constitute autonomous units which can be tested each one independently from every other, for hardware as well as for software.

Related to the above aspects are those of *accessibility*, *adjustment*, and *exchangeability*. Accessibility should be easy for LRUs with *limited useful life*, high failure rate, or wear out. The use of digital techniques largely reduces the need for *adjustment* (alignment). As a general rule, hardware adjustment in the field should be avoided. *Exchangeability* can be a problem for equipment and systems with long *useful life*. *Spare parts provisioning* and aspects of *obsolescence* can in such cases become mandatory (Section 4.5).

4.2.3 User Documentation

User (or product) documentation for complex equipment and systems can include all of the following Manuals or Handbooks

- General Description
- Operating Manual
- Preventive Maintenance (Service) Manual
- Corrective Maintenance (Repair) Manual
- Illustrated Spare Parts Catalog
- Logistic Support.

It is important for the content of the user documentation to be *consistent* with the hardware and software status of the item considered. Emphasis must be placed on a clear and concise presentation, with block diagrams, flow charts, check lists. The language should be easily understandable to *non-specialized personnel*. Procedures should be self sufficient and contain checkpoints to prevent the skipping of steps.

4.2.4 Training of Operation and Maintenance Personnel

Suitably equipped, well trained, and motivated maintenance personnel are an important prerequisite to achieve short maintenance times and to avoid *human errors*. Training must be comprehensive enough to cover present needs. However, for complex systems it should be periodically updated to cover technological changes introduced in the system and to further motivate operation and maintenance personnel.

4.2.5 User Logistic Support

For complex equipment and systems, customers (users) generally expect from the manufacturer a *logistic support* during the useful life of the item under consideration. This can range from support on an *on-call basis* up to a *maintenance contract* with manufacturer's personnel located at the user site. One important point in such a logistic support is the definition of *responsibilities*. For this reason, maintenance is often subdivided into different levels (four for military applications (Table 4.2) and three for industry, in general). The *first level* concerns simple maintenance work such as the status test, fault detection and fault localization down to the subsystem level. This task is generally performed by *operating personnel*. At the *second level*, fault localization is refined, the defective LRU is replaced by a good one, and the functional test is performed. For this task *first line maintenance personnel* is often required. At the *third level*, faulty LRUs are repaired by *maintenance personnel* and stored for reuse. The *fourth level* is generally relates to

Table 4.2 Maintenance levels in the defense area

	logistic level	Location	Carried out by	Tasks
Advanced maintenance service	Level 1	Field	Operating personnel	<ul style="list-style-type: none"> • Simple maintenance work • Status test • Fault detection (recognition) • Fault localization down to subsystem level
	Level 2	Cover	First line maintenance personnel	<ul style="list-style-type: none"> • Preventive maintenance • Fault localization down to LRU level • First line repair (LRU replacement) • Functional test
Back-up maintenance service	Level 3	Depot	Maintenance personnel	<ul style="list-style-type: none"> • Difficult maintenance • Repair of LRUs
	Level 4	Arsenal or Industry	Specialists from arsenal or industry	<ul style="list-style-type: none"> • Reconditioning work • Important changes or modifications

LRU = line replaceable unit (spare part at system level); *fault* includes failures and defects

overhaul or *revision* (essentially for mechanical parts subjected to wear, erosion, scoring, etc.) and performed at the manufacturer's site by *specialized personnel*.

For large mechanical systems, maintenance can account for over 30% of the operating cost. A careful optimization of these cost may be necessary in many cases. The part contributed by preventive maintenance is more or less deterministic. For the corrective maintenance, cost equations weighted by probabilities of occurrence can be established from considerations similar as those given in Sections 1.2.9 and 8.4, see also Sections 4.5, 4.6, and 4.7.

Table 4.3 Catalog of questions which can be used to generate *project specific checklists* for the evaluation of *maintainability aspects in preliminary design reviews* (Appendices A3, A4) of complex equipment & systems with high maintainability requirements (fault used for failure & defect, p. 79 for rel.)

1. Has the equipment or system been conceived with modularity in mind? Are the modules functionally independent and separately testable?
2. Has a concept for fault detection and localization been planned and realized? Is fault detection automatic? Which kind of faults are detected? How does fault localization work? Is localization down to *line replaceable units* (LRUs) possible? How large are values for fault detection and fault localization (coverage)?
3. Can redundant elements be repaired on-line?
4. Are enough test points provided? Do they have pull-up/pull-down resistors?
5. Have hardware adjustments (or alignments) been reduced to a minimum? Are the adjustable elements clearly marked and easily accessible? Is the adjustment uncritical?
6. Has the amount of external test equipment been kept to a minimum?
7. Has the standardization of components, materials, and maintenance tools been considered?
8. Are *line replaceable units* (LRUs) identical with spare parts? Can they be easily tested? Is a spare parts provisioning concept available?
9. Are all elements with limited useful life clearly marked and easily accessible?
10. Are access flaps (and doors) easy to open (without special tools) and self-latching? Have plug-in unit guide rails self-blocking devices? Can a standardized extender for PCBs be used?
11. Have indirect connectors been used? Is the plugging-out/plugging-in of PCBs (LRUs) easy? Are power supplies and ground distributed across different contacts?
12. Have wires and cables been conveniently placed? Also with regard to maintenance?
13. Are sensitive elements sufficiently protected against mishandling during maintenance?
14. Can preventive maintenance be performed on-line? Does preventive maintenance also allow the detection of hidden faults?
15. Have maintainability tests been planned? What does this test program include? Has a test strategy from incoming inspection to system test been conceived? It is appropriate?
16. Which part of the item (system) can be considered as-good-as-new after a maintenance action?
17. Have man-machine, ergonomic, and human aspects been sufficiently considered to avoid mistakes at operation or maintenance?
18. Have all safety aspects also for operating and maintenance personnel been considered? Also in the case of failure (FMEA/FMECA, FTA, etc.)?
19. Is remote control, detection, diagnosis, maintenance possible? Which of them and how?
20. Has the predicted maintainability been calculated? How?

4.3 Maintainability Aspects in Design Reviews

Design reviews are important to point out, discuss, and eliminate *design weaknesses*. Their objective is also to *decide about continuation or stopping* of the project on the basis of objective considerations (*feasibility checks* in Tables A3.3 & 5.3 and Fig. 1.6). The most important design reviews (PDR & CDR) are described in Table A3.3 for hardware and in Table 5.5 for software. To be effective, design reviews must be supported by *project specific checklists*. Table 4.3 gives a catalog of questions which can be used to generate project specific checklists for maintainability aspects in design reviews (see Table 2.8 for reliability and Appendix A4 for other aspects). As shown in Table 4.3, checking maintainability during a design review deals with all involved aspects, including adherence to given design guidelines, testability, coverage, man-machine and human factors, logistic support, remote maintenance, and predicted maintainability.

4.4 Predicted Maintainability

Knowing the reliability structure of a system and the reliability and maintainability of its elements, it is possible to calculate the maintainability of the system considered as a *one-item structure* (e. g. calculating the reliability function and the point availability at system level and extracting $g(t)$ as the density of the repair time at system level using Eqs. (6.14) and (6.18)). However, such a calculation soon becomes laborious for arbitrary systems (Chapter 6). For many practical applications it is often sufficient to know the *mean time to repair* at system level $MTTR_S$ (expected value of the repair (renewal) time at system level) as a function of the system reliability structure, and of the mean time to failure $MTTF_i$ and mean time to repair $MTTR_i$ of its elements. Such a calculation is discussed in Section 4.4.1. Section 4.4.2 deals then with the calculation of the *mean time to preventive maintenance* at system level $MTTPM_S$. The method used in Sections 4.4.1 and 4.4.2 is easy to understand and delivers mathematically exact results for $MTTR_S$ and $MTTPM_S$. Use of statistical methods to estimate or demonstrate a maintainability or an $MTTR$ are discussed in Sections 7.2.1, 7.3, 7.5, and 7.6.

4.4.1 Calculation of $MTTR_S$

Let us first consider a *system without redundancy*, with elements E_1, \dots, E_n in series as given in Fig. 6.4. $MTTF_i$ and $MTTR_i$ are the *mean time to failure* and the *mean time to repair* of element E_i , respectively ($i=1, \dots, n$). Assume now that each

element works for the same *cumulative operating time* T (the system is disconnected during repair, or repair times are neglected because of $MTTR_i \ll MTTF_i$) and let T be *arbitrarily large*. In this case, the mean (expected value) of the number of failures of element E_i during T is given by (Eq. (A7.27))

$$\frac{T}{MTTF_i}.$$

The mean of the total repair time necessary to restore the $T/MTTF_i$ failures follows then from

$$MTTR_i \frac{T}{MTTF_i}.$$

For the whole system, there will be in *mean*

$$\sum_{i=1}^n \frac{T}{MTTF_i} \quad (4.4)$$

failures and a *mean* total repair time of

$$\sum_{i=1}^n MTTR_i \frac{T}{MTTF_i}. \quad (4.5)$$

From Eqs. (4.4) and (4.5) it follows then for the *mean time to repair* (restoration) at system level $MTTR_S$, the final value

$$MTTR_S = \frac{\sum_{i=1}^n MTTR_i / MTTF_i}{\sum_{i=1}^n 1 / MTTF_i}. \quad (4.6)$$

Equation (4.6) gives the *mathematically exact value for the mean repair time at system level* $MTTR_S$, under the assumption that at system down (during a repair) no further failures can occur and that switching is ideal (no influence on the reliability). From Eq. (4.6) one can easily verify that

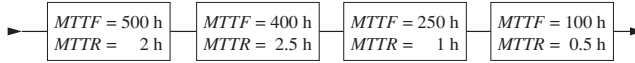
$$MTTR_S = MTTR, \quad \text{for} \quad MTTR_1 = \dots = MTTR_n = MTTR,$$

and

$$MTTR_S = \frac{1}{n} \sum_{i=1}^n MTTR_i, \quad \text{for} \quad MTF_1 = \dots = MTF_n.$$

Example 4.1

Give the mean time to repair at system level $MTTR_S$ for the following system.



How large is the mean of the *total system down time* during the interval $(0, t]$ for $t \rightarrow \infty$?

Solution

From Eq. (4.6) it follows that

$$MTTR_S = \frac{\frac{2 \text{ h}}{500 \text{ h}} + \frac{2.5 \text{ h}}{400 \text{ h}} + \frac{1 \text{ h}}{250 \text{ h}} + \frac{0.5 \text{ h}}{100 \text{ h}}}{\frac{1}{500 \text{ h}} + \frac{1}{400 \text{ h}} + \frac{1}{250 \text{ h}} + \frac{1}{100 \text{ h}}} = \frac{0.01925}{0.0185 \text{ h}^{-1}} \approx 1.04 \text{ h}.$$

The mean down time at system level is also 1.04 h, because for a *system without redundancy* it holds that down time = repair time. The *mean operating time* at system level in the interval $(0, t]$ can be obtained from the expression for the average availability AA_S (Eqs. (6.23), (6.24), (6.48), and (6.49))

$$\lim_{t \rightarrow \infty} E[\text{total operating time in } (0, t]] = t \cdot AA_S = t \cdot MTTF_S / (MTTF_S + MTTR_S).$$

From this, the mean of the *total system down time* during $(0, t]$ for $t \rightarrow \infty$ follows from

$$\lim_{t \rightarrow \infty} E[\text{total system down time in } (0, t]] = t - t \cdot AA_S = t \cdot MTTR_S / (MTTF_S + MTTR_S).$$

Numerical computation then leads to

$$t \cdot MTTR_S / (MTTF_S + MTTR_S) \approx t \cdot MTTR_S / MTTF_S = t \cdot 1.04 \text{ h} \cdot 0.0185 \text{ h}^{-1} \approx 0.019 t.$$

If every element exhibits a constant failure rate λ_i , then $MTTF_i = 1/\lambda_i$ and

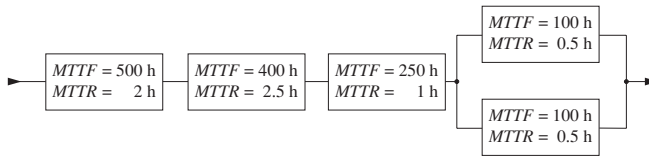
$$MTTR_S = \frac{\sum_{i=1}^n \lambda_i MTTR_i}{\sum_{i=1}^n \lambda_i} = \sum_{i=1}^n \frac{\lambda_i}{\lambda_S} MTTR_i, \quad \text{with } \lambda_S = \sum_{i=1}^n \lambda_i. \quad (4.7)$$

Equations (4.6) and (4.7) can also be used for systems with redundancy. However, in this case, a distinction at system level between *repair time* and *down time* is necessary. If the system contains only *active redundancy*, the *mean time to repair* at system level $MTTR_S$ is given by Eq. (4.6) or (4.7) by *summing over all elements* of the system, as if they were in series (a similar consideration holds for

spare parts provisioning). By assuming that failures of redundant elements are repaired without interruption of operation at system level, Eq. (4.6) or (4.7) can be used to obtain an *approximate value* of the *mean down time* at system level, by *summing only over all elements without redundancy* (series elements), see Example 4.2.

Example 4.2

How does the $MTTR_S$ of the system in Example 4.1 change, if an active redundancy is introduced to the element with $MTTF = 100\text{ h}$?



Under the assumption that the redundancy is repaired without interruption of operation at system level, is there a difference between the *mean time to repair* and the *mean down time* at system level?

Solution

Because of the assumed active redundancy, the operating elements and the reserve elements show the same mean number of failures. The mean system repair time follows from Eq. (4.6) by summing over all system elements, yielding

$$MTTR_S = \frac{\frac{2\text{ h}}{500\text{ h}} + \frac{2.5\text{ h}}{400\text{ h}} + \frac{1\text{ h}}{250\text{ h}} + \frac{0.5\text{ h}}{100\text{ h}} + \frac{0.5\text{ h}}{100\text{ h}}}{\frac{1}{500\text{ h}} + \frac{1}{400\text{ h}} + \frac{1}{250\text{ h}} + \frac{1}{100\text{ h}} + \frac{1}{100\text{ h}}} = \frac{0.02425}{0.0285\text{ h}^{-1}} \approx 0.85\text{ h}.$$

However, the system down time differs now from the system repair time. Assuming for the redundancy an availability equal to one (for constant failure rate $\lambda = 1/MTTF$, constant repair rate $\mu = 1/MTTR$, and one repair crew, Table 6.6 (p. 201) gives for the 1-out-of-2 active redundancy $PA = AA = \mu(2\lambda + \mu) / (2\lambda(\lambda + \mu) + \mu^2)$ yielding $AA = 0.99995$ for this example), the system down time is defined by the elements in series on the reliability block diagram (see Point 9 in Section 6.8.9 (Eq. (6.295)) for precise considerations), thus

$$\text{mean down time at system level} = MDT_S \approx \frac{\frac{2\text{ h}}{500\text{ h}} + \frac{2.5\text{ h}}{400\text{ h}} + \frac{1\text{ h}}{250\text{ h}}}{\frac{1}{500\text{ h}} + \frac{1}{400\text{ h}} + \frac{1}{250\text{ h}}} = \frac{0.01425}{0.0085} \approx 1.68\text{ h}.$$

Similarly to Example 4.1, the mean of the system down time during $(0, t]$ follows from

$$\lim_{t \rightarrow \infty} E[\text{total down time in } (0, t]] = t(1 - AA_S) \approx t \frac{MDT_S}{MTTF_S} = t \cdot 1.68\text{ h} \cdot 0.0085\text{ h}^{-1} \approx 0.014 t.$$

4.4.2 Calculation of $MTTPM_S$

Based on the results of Section 4.4.1, calculation of the *mean time to preventive maintenance* at system level $MTTPM_S$ can be performed for the following two cases:

1. Preventive maintenance is carried out at once for the *entire system*, one element after the other. If the system consists of elements E_1, \dots, E_n (arbitrarily grouped on the reliability block diagram) and the mean time to preventive maintenance of element E_i is $MTTPM_i$, then (Eq. (A6.68))

$$MTTPM_S = \sum_{i=1}^n MTTPM_i. \quad (4.8)$$

2. Every element E_i of the system is serviced for preventive maintenance *independently* of all other elements and has a mean time to preventive maintenance $MTTPM_i$. In this case, Eq. (4.6) can be used with $MTBPM_i$ instead of $MTTF_i$ and $MTTPM_i$ instead of $MTTR_i$, where $MTBPM_i$ is the *mean time between preventive maintenance* for the element E_i .

Case 2 has a practical significance when preventive maintenance can be performed without interruption of the operation at system level.

4.5 Basic Models for Spare Parts Provisioning

Spare parts provisioning is important for systems with long *useful life* or when short repair times and/or independence from the manufacturer is required (spare part is used here e.g. for *line replaceable unit* (LRU)). Basically, a distinction is made between centralized and decentralized logistic support. Also important is to take into account whether spare parts are repairable or not. This section presents the basic models for the provision of nonrepairable and of repairable spare parts. For nonrepairable spare parts, the cases of centralized and decentralized logistic support are considered in order to quantify the advantage of a centralized logistic support with respect to a decentralized one. More general maintenance strategies are discussed in Section 4.6, cost specific aspects in Sections 4.5-4.7.

4.5.1 Centralized Logistic Support, Nonrepairable Spare Parts

In *centralized logistic support*, spare parts are stocked at *one place*. The basic problem can be formulated as follows:

At time $t=0$, the first part is put into operation, it fails at time $t = \tau_1$ and is replaced (in a negligible time) by a second part which fails at time $t = \tau_1 + \tau_2$ and so forth; asked is the number n of parts which must be stocked in order that the requirement for parts during the cumulative operating time T is met with a given (fixed) probability γ .

To answer this question, the *smallest integer* n must be found for which

$$\Pr\{\tau_1 + \dots + \tau_n > T\} \geq \gamma \tag{4.9}$$

holds. In general, τ_1, \dots, τ_n are assumed to be independent positive random variables with the same distribution function $F(x)$, $F(0)=0$, density $f(x)$, and finite mean $E[\tau_i] = E[\tau] = MTTF$ & $\text{Var}[\tau_i] = \text{Var}[\tau]$. If the number of parts is calculated from

$$n = T / MTTF, \tag{4.10}$$

the requirement can only be covered (for T large) with a probability of 0.5. Thus, more than $T / MTTF$ parts are necessary to meet the requirement with $\gamma > 0.5$.

According to Eq. (A7.12), valid for renewal processes, the probability as per Eq. (4.9) can be expressed by the $(n - 1)$ th convolution of the distribution function $F(t)$ with itself, i.e.

$$\Pr\{\tau_1 + \dots + \tau_n > T\} = 1 - F_n(T),$$

with $F_1(T) = F(T)$ and $F_n(T) = \int_0^T F_{n-1}(T-x)f(x) dx, \quad n > 1.$ (4.11)

Of the distribution functions $F(x)$ used in reliability theory, a closed, simple form for the function $F_n(x)$ exists only for the *exponential*, *gamma*, and *normal* distribution functions, yielding a Poisson, gamma, and normal distribution, respectively. In particular, the exponential distribution $F(x) = 1 - e^{-\lambda x}$ leads to (Eq. (A7.39))

$$\Pr\{\sum_{i=1}^n \tau_i > T\} = \sum_{i=0}^{n-1} \frac{(\lambda T)^i}{i!} e^{-\lambda T}. \tag{4.12}$$

The important case of the *Weibull distribution* $F(x) = 1 - e^{-(\lambda x)^\beta}$ must be solved numerically. Figure 4.3 shows the results with γ and β as parameters [4.2 (1974)].

For n large, an *approximate solution* for a wide class of distribution functions $F(x)$ can be obtained using the *central limit theorem*. From Eq. (A6.148) it follows that (considering $\text{Var}[\tau] < \infty$)

$$\lim_{n \rightarrow \infty} \Pr\left\{ \sum_{i=1}^n \frac{\tau_i - E[\tau]}{\sqrt{n \text{Var}[\tau]}} > x \right\} = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-y^2/2} dy = 1 - \Phi(x) = \Phi(-x), \tag{4.13}$$

and thus, using $x \sqrt{n \text{Var}[\tau]} + n E[\tau] = T$,

$$\lim_{n \rightarrow \infty} \Pr \left\{ \sum_{i=1}^n \tau_i > T \right\} = \frac{1}{\sqrt{2\pi}} \int_{(T-nE[\tau])/\sqrt{n\text{Var}[\tau]}}^{\infty} e^{-y^2/2} dy = \gamma \tag{4.14}$$

Setting $(T - nE[\tau]) / \sqrt{n\text{Var}[\tau]} = -d$ it follows that for $n \rightarrow \infty$

$$n = \left[\kappa d / 2 + \sqrt{(\kappa d / 2)^2 + T / E[\tau]} \right]^2, \quad \text{with } \kappa = \sqrt{\text{Var}[\tau]} / E[\tau]. \tag{4.15}$$

A similar approximation can also be obtained from Eq. (A7.34).

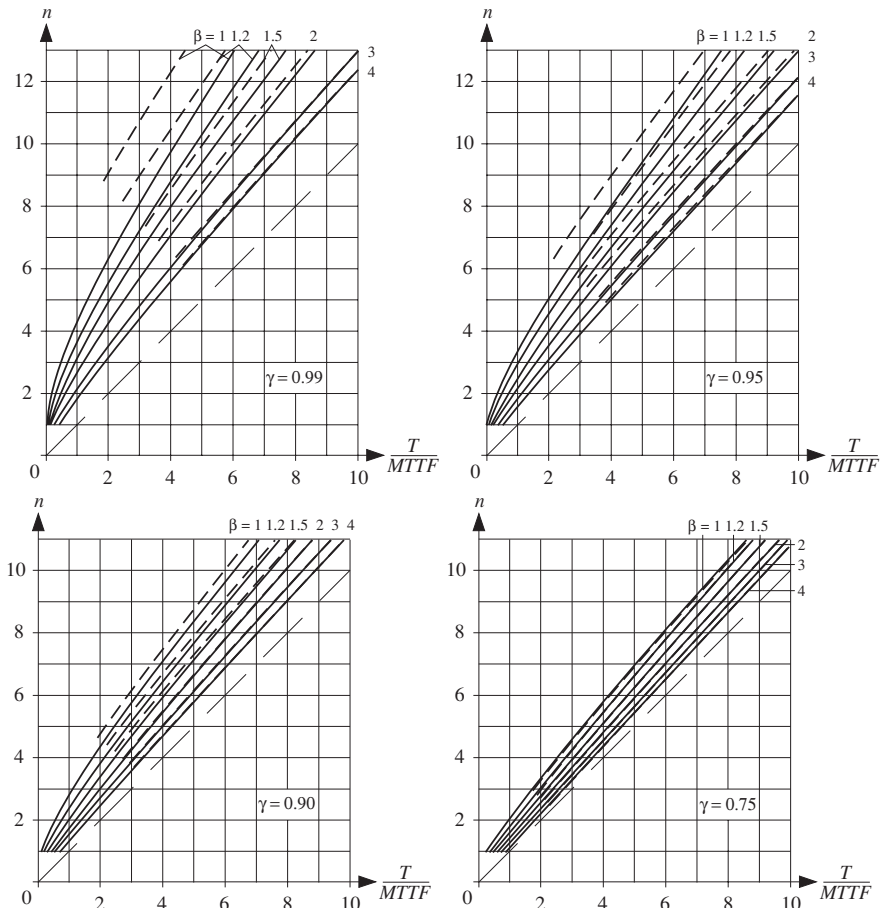


Figure 4.3 Number n of parts necessary to cover a cumulative operating time T with probability $\geq \gamma$, i.e. smallest n for which $\Pr\{\tau_1 + \dots + \tau_n > T\} \geq \gamma$ holds, with $\Pr\{\tau_i \leq x\} = 1 - e^{-(\lambda x)^\beta}$ and $MTTF = \Gamma(1 + 1/\beta) / \lambda$. (dashed results given by the central limit theorem as per Eq. (4.15); $\beta = 1$ yields the exponential distribution function)

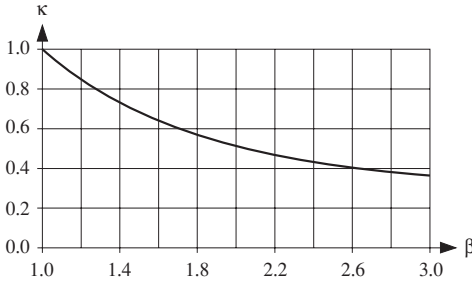


Figure 4.4 Coefficient of variation for the Weibull distribution for $1 \leq \beta \leq 3$

From Eqs. (4.13) to (4.15) one recognizes that d is the γ quantile of the *standard normal distribution* ($\gamma = 1 - \Phi(-d) = \Phi(d)$), yielding e. g. (Table A9.1)

$$\begin{array}{cccccc} \gamma = & 0.99 & 0.95 & 0.90 & 0.75 & 0.5 \\ d = & 2.33 & 1.64 & 1.28 & 0.67 & 0 \end{array}$$

Equation (4.15) gives for $\gamma \leq 0.95$ a good *approximation* of the number of parts n down to low values of n (see e. g. Fig. 4.3). $\kappa = \sqrt{\text{Var}[\tau] / \text{E}[\tau]}$ is the *coefficient of variation* ($\kappa=1$ for the exponential distribution and $\kappa = \sqrt{\Gamma(1+2/\beta) / (\Gamma(1+1/\beta))^2 - 1}$ for the Weibull distribution (Fig. 4.4)).

For the case of a Weibull distribution with $\beta \geq 1$, approximate values for n obtained using the central limit theorem (Eq. (4.15)) are shown *dashed* in Fig. 4.3. For $\beta=1$, deviation from the exact value is < 1.3 for $\gamma \leq 0.95$ and $n \geq 5$; this deviation drops off rapidly for increasing values of β ($F_n(x)$ already approaches a normal distribution for small n). From Eqs. (4.13) - (4.15) one recognizes that for $\gamma = 0.5$, $d = 0$ and thus, for n large, $n = T / \text{E}[\tau]$ (Eq. (4.10)).

Let us now consider the case in which *the same part occurs k times* in the system. For $F(x) = 1 - e^{-\lambda x}$, i.e. $\text{E}[\tau] = 1/\lambda$ and $\kappa = 1$, Eqs. (4.12) - (4.15) hold with

$$\lambda' = k \lambda, \quad k = 1, 2, \dots, \tag{4.16}$$

instead of λ . This is because the *sum of independent Poisson processes is a Poisson process* (Eq. (7.27)) and k parts must be operating for the required function. The same holds if l systems use the same part, one or more per system with total k parts of the same type, and *storage is centralized* (Example 4.3). Considering that $k \geq 1$ parts are available at $t=0$ (operating at $t=0$), it is reasonable to define as number of *spare parts* n_{sp} (at system level) the quantity

$$n_{sp} = n - k, \quad k = 1, 2, \dots, \tag{4.17}$$

where n is the number of parts obtained from Eq. (4.12) with $\lambda' = k \lambda$ instead of λ , see Examples 4.3 and 4.4 for practical applications.

Example 4.3

A part with constant failure rate $\lambda = 10^{-3} \text{ h}^{-1}$ is used three times in a system ($k = 3$). Give the number of spare parts n_{sp} which must be stored to cover a cumulative operating time $T = 10,000 \text{ h}$ with a probability $\gamma \geq 0.90$.

Solution

Considering $k\lambda T = 30$, the exact solution is given by the smallest integer $n_{sp} = n - 3$ for which

$$\sum_{i=0}^{n-1} \frac{30^i}{i!} e^{-30} \geq 0.9$$

holds (Eq. (4.12)). From Table A9.2 it follows, for $q = 1 - 0.9 = 0.1$ and $t_{v,q} = 2 \cdot 30 = 60$, the value $v = 75.2$ (lin. interpolation); thus, $v = 76$ and (Appendix A9.2 & Eq. (4.12)) $n = v / 2 = 38$ (same results from Fig. 7.3 for $m = 30$ & $\gamma = 0.9$, yielding $n = c + 1 = 38$, and with Eq. (4.15) for $\kappa = 1$ and $d = 1.28$, yielding $n = 38$ ($[0.64 + \sqrt{0.642 + 30}]^2 \approx 37.9$)). Thus, considering that 3 parts are operating at $t = 0$, it follows that (Eq. (4.17)) $n_{sp} = 38 - 3 = 35$.

4.5.2 Decentralized Logistic Support, Nonrepairable Spare Parts

For users who have the same system located at different places, spare parts are often stored *decentralized*, i. e., separately at each location (decentralized means that spare parts cannot be transferred from one location to another location). If there are l systems, each with a given part, and the storage of spare parts is decentralized at each system (or location), a first approach could be to store with each system the same number of spare parts obtained using Eqs. (4.9) and (4.17). In this case, the total number of parts would be $n \cdot l$, i. e. $(n - k) \cdot l$ spare parts. This number n of parts, which would be sufficient to meet, with a probability $> \gamma$ (often $\gg \gamma$) the needs of the l systems with a *centralized storage* (Example 4.4), would now in general be too small to meet all the individual needs at each location. In fact, assuming that failures at each location are independent, and that with n parts the probability of meeting the needs at any location individually is γ , then the probability of meeting the need at all locations is γ^l . Thus, to meet the need at the l locations with a probability γ

$$n_{dec} = l \cdot n_l \quad (4.18)$$

parts are required, where n_l is computed for each location individually with

$$\gamma_l = \sqrt[l]{\gamma}, \quad (4.19)$$

e. g. using Eq. (4.15) with d_l instead of d ($\Phi(d) = \gamma$, $\Phi(d_l) = \sqrt[l]{\gamma}$). To make a comparison between a centralized and a decentralized logistic support, let us assume that the part considered appears k times in each of the l locations, has *constant failure rate* λ , and $k\lambda T \gg d_l^2/4 > d^2/4$ holds. In this case, Eqs. (4.15) & (4.16) lead to

$$n \approx k\lambda T + d \sqrt{k\lambda T}, \quad k\lambda T \gg d^2/4, \quad k = 1, 2, \dots, \quad \text{probability } \gamma. \quad (4.20)$$

For *centralized logistic support*, Eq. (4.20) yields

$$n_{cen} \approx lk\lambda T + d\sqrt{lk\lambda T}, \quad lk\lambda T \gg d^2/4, \quad k, l = 1, 2, \dots, \text{ probability } \gamma. \quad (4.21)$$

For *decentralized logistical support*, Eq. (4.20) yields

$$n_{dec} \approx l(k\lambda T + d_l\sqrt{k\lambda T}), \quad k\lambda T \gg d_l^2/4, \quad k, l = 1, 2, \dots, \text{ probability } \gamma, \quad (4.22)$$

where d_l is obtained as for d in Eq. (4.15) with $\gamma_l = \sqrt[l]{\gamma}$ instead of γ (for example, $d = 1.64$ for $\gamma = 0.95$ and $d_l = 2.57$ for $l = 10$ i. e. for $\gamma_l = 0.9949$, see Table A9.1). From the above considerations it follows that for $k\lambda T \gg d_l^2/4 > d^2/4$ (Example 4.4)

$$\frac{n_{dec}}{n_{cen}} \approx \frac{1 + d_l/\sqrt{k\lambda T}}{1 + d/\sqrt{lk\lambda T}} \quad \text{or} \quad \frac{n_{spdec}}{n_{spcen}} \approx \frac{1 + (d_l/\sqrt{k\lambda T}) - 1/\lambda T}{1 + (d/\sqrt{lk\lambda T}) - 1/\lambda T}, \quad (4.23)$$

with $\Phi(d) = \gamma$ and $\Phi(d_l) = \sqrt[l]{\gamma}$. Setting $\lambda T = T/E[\tau] = T/MTTF$, Eq. (4.23) can be used for arbitrary distribution of the spare parts failure-free time τ (Appendix A7.8.3).

4.5.3 Repairable Spare Parts

In Sections 4.5.1 and 4.5.2 it was assumed that the spare parts (LRUs) were *nonrepairable*, i. e., that a new spare part was necessary at each failure. In many cases, spare parts can be repaired and then stored for *reuse*. Calculation of the number of spare parts which should be stored can be performed in a way similar to the investigation of a *k-out-of-n standby redundancy*, where k is the number of parts used in the system (as in Eq. (4.17)) and n is the smallest integer *to be determined* such that the requirement is met with a given (fixed) probability γ . Following two cases have to be considered:

Example 4.4

Let $\lambda = 10^{-4} \text{ h}^{-1}$ be the constant failure rate of a part in a given system. The user has 6 locations ($l = 6$) and would like to achieve a cumulative operating time $T = 50,000 \text{ h}$ at each location with a probability $\gamma \geq 0.95$. How many spare parts can be saved using a centralized logistic support?

Solution

From Fig. 4.3 ($T/MTTF = 5$, $\gamma = \sqrt[6]{0.95} \approx 0.99$), Fig. 7.3 ($m = 5$, $\gamma = 0.99$, $c = n_l - 1$), or from a χ^2 -Table ($t_{v,q} = 10$, $q = 1 - 0.99 = 0.01$, $v = 2n_l$) each user would need $n_l = 12$ parts ($n_l = 14$ using Eq. (4.15) with $d = d_l = 2.33$ and $\lambda T = 5$); thus $n_{dec} = 6 \cdot 12 = 72$ parts and (Eq. (4.17)) $n_{spdec} = 72 - 6 = 66$ spare parts. Combining the storage ($l = 6$), it follows from Fig. 7.3 ($m = 30$, $\gamma = 0.95$, $c = n_{cen} - 1$) or from Table A9.2 ($t_{v,q} = 60$, $q = 0.05$, $v = 2n_{cen}$) that $n_{cen} = 40$ ($n_{cen} = 41$ using Eq. (4.15) with $d = 1.64$ and $\lambda T = 30$); thus, $n_{spcen} = 40 - 6 = 34$. A centralized storage would save $66 - 34$ (or $72 - 40$) = 32 spare parts (Eq. (4.23) gives 1.57 instead of 1.8 (left) and 1.67 instead of 1.94 (right), because $k\lambda T = 5$ is not $\gg d_l^2/4 = 1.36$).

Supplementary result: Provisioning independently for each location with $\gamma = 0.95$ yields $n_l = 10$ (Fig. 4.3 with $T/MTTF = 5$ & $\gamma = 0.95$) and thus $n = 6 \cdot 10 = 60$.

1. γ is the probability that a request for a spare part *at a time point* t can be met without time delay; in this case, γ can be considered as the *point availability* PA_S (in steady-state to simplify investigations) and n is the smallest integer such that $PA_S \geq \gamma$ for a given (fixed) γ .
2. γ is the probability that any request for a spare part *during the time interval* $(0, t]$ will be met without time delay; in this case, γ can be considered as the *reliability function* $R_{S0}(t)$ and n is the smallest integer such that $R_{S0}(t) \geq \gamma$ for given (fixed) γ and t .

If the *spare parts* have *constant failure rate* $\lambda = 1/MTTF$ and *constant repair rate* $\mu = 1/MTTR$, *birth-and-death processes* can be used (Section A7.5.5). To simplify investigations and to agree with results in Chapter 6, it is assumed that *only one spare part at a time can be repaired* (only 1 repair crew is available) and *no further failures are considered when a request for a spare part cannot be met* (corresponds to the assumption *no further failure at system down* (Fig. 6.13)).

For Case 1 above, Eq. (6.138) with $\lambda_r \equiv 0$ and Eq. (6.140) yield

$$PA_S = \sum_{j=0}^{n-k} P_j = 1 - P_{n-k+1} \geq \gamma \quad (4.24)$$

with

$$P_j = \frac{\pi_j}{\sum_{i=0}^{n-k+1} \pi_i} \quad \text{and} \quad \pi_i = (k\lambda/\mu)^i, \quad i = 0, \dots, n-k+1. \quad (4.25)$$

Asked is the smallest integer n which satisfies Eq. (4.24) for given (fixed) γ , k , λ , and μ . Often $n = k + 1$ (*one spare part*) or $n = k + 2$ (*two spare parts*) will be *sufficient*. In these cases, results of Table 6.8 yield

$$PA_{S1} = \frac{1}{1 + k^2\lambda^2 / (k\lambda\mu + \mu^2)} \approx 1 - (k\lambda/\mu)^2, \quad (4.26)$$

$n_{sp} = n - k = 1$ spare part, 1 repair crew, Case 1,

$$PA_{S2} = \frac{1}{1 + k^3\lambda^3 / (k^2\lambda^2\mu + k\lambda\mu^2 + \mu^3)} \approx 1 - (k\lambda/\mu)^3, \quad (4.27)$$

$n_{sp} = n - k = 2$ spare parts, 1 repair crew, Case 1.

If PA_{S2} is still $< \gamma$, more than 2 spare parts are necessary. A good approximation for the number n_{sp} of spare parts can be obtained using the smallest integer $n_{sp} = n - k$ satisfying (Table 6.8)

$$PA_{S_{n_{sp}}} \approx 1 - (k\lambda/\mu)^{n_{sp}+1} \geq \gamma, \quad n_{sp} = n - k \text{ spare parts, 1 repair crew, Case 1.} \quad (4.28)$$

Using results of Appendix A7.5.5 (Eq. (A7.157)) and for $k\lambda \ll \mu$, it can be shown that approximations per Eqs. (4.27) & (4.28) hold also if the assumption "no further failures are considered when a request for a spare part cannot be met" is not made.

The case in which $n_{sp}+1$ repair crews are available (instead of 1 repair crew) is considered by Eq. (4.32) for comparative investigations.

For Case 2 above, the reliability function can be approximated by an exponential function (Eq. (6.93)), yielding (Eqs. (6.144) & (6.145) with $v_i = k\lambda$)

$$R_{S0_1}(t) \approx e^{-t(k\lambda)^2/\mu}, \quad n_{sp} = n - k = 1 \text{ spare part, 1 repair crew, Case 2,} \quad (4.29)$$

$$R_{S0_2}(t) \approx e^{-t(k\lambda)^3/\mu^2}, \quad n_{sp} = n - k = 2 \text{ spare parts, 1 repair crew, Case 2.} \quad (4.30)$$

If $R_{S0_2}(t)$, with t as mission time, is still $< \gamma$, more than 2 spare parts are necessary. A good approximation for the number n_{sp} of spare parts can be obtained using the smallest integer $n_{sp} = n - k$ satisfying (Table 6.8)

$$R_{S0_{n_{sp}}}(t) \approx e^{-t\mu(k\lambda/\mu)^{n_{sp}+1}} \geq \gamma, \quad n_{sp} = n - k \text{ spare parts, 1 repair crew, Case2.} \quad (4.31)$$

For Eqs. (4.29) to (4.31) it holds necessarily that no further failures are considered when a request for a spare part cannot be met (system down states are made absorbing for reliability calculations). The case in which n_{sp} repair crews are available is considered by Eq. (4.33) for comparative investigations. Example 4.5 gives a practical application.

Assuming for comparative investigations that each of the $n_{sp} = n - k$ spare parts can be repaired *independently* from each other ($n_{sp}+1$ repair crew) and no further failures when a request for a spare part cannot be met, results of Section A7.5.5, with $v_i = k\lambda$, $i = 0, \dots, n - k$, and $\theta_i = i\mu$, $i = 1, \dots, n - k + 1$, yield (see also Eq. (6.149))

Example 4.5

A system contains $k = 100$ identical parts (LRUs) with a constant failure rate $\lambda = 10^{-5} \text{ h}^{-1}$ and which can be repaired with a constant repair rate $\mu = 10^{-1} \text{ h}^{-1}$. (i) Give the number of spare parts which must be stored in order to meet without any time delay and with a probability $\gamma \geq 0.99$ a request for a spare part at a time point t (consider the steady-state only, one repair crew, and no further failure when a request for a spare part cannot be met). (ii) If one spare part is stored ($n = k + 1$), how large is the probability that any request for a spare part during the time interval $(0, 10^4 \text{ h}]$ will be met without any time delay?

Solution

(i) Taking $n = k + 1$ (1 spare part), Eq. (4.26) yields

$$PA_{S1} = \frac{1}{1 + 10^4 \cdot 10^{-10} / (100 \cdot 10^{-5} \cdot 10^{-1} + 10^{-2})} \approx 1 - \left(\frac{100 \cdot 10^{-5}}{10^{-1}}\right)^2 \approx 0.9999.$$

Thus only one spare part ($n_{sp} = 1$) must be stored.

(ii) For $n = k + 1$, Eq. (4.29) yields $R_{S0_1}(t) \approx e^{-0.00001 t}$ and thus $R_{S0_1}(10^4 \text{ h}) \approx e^{-0.1} \approx 0.91$.

Supplementary result: To reach $R_{S0}(10^4) \geq 0.99$ one needs $n_{sp} = 2$ spare parts ($R_{S0_2}(10^4) = 0.999$).

$$PA_{S n_{sp}} \approx 1 - (k\lambda/\mu)^{n_{sp}+1} / (n_{sp}+1)!, \quad \begin{array}{l} n_{sp} = n-k \text{ spare parts,} \\ n_{sp}+1 \text{ repair crews, Case 1,} \end{array} \quad (4.32)$$

and, with v_i as before and $\theta_i = i\mu$, $i = 1, \dots, n-k$,

$$R_{S0 n_{sp}}(t) \approx e^{-t\mu} (k\lambda/\mu)^{n_{sp}+1} / (n_{sp}+1)!, \quad \begin{array}{l} n_{sp} = n-k \text{ spare parts,} \\ n_{sp} \text{ repair crews, Case 2.} \end{array} \quad (4.33)$$

Using results of Appendix A7.5.5 (Eq. (A7.157)), and for $k\lambda \ll \mu$, it can be shown that the approximation per Eqs. (4.32) holds also if the assumption "no further failures are considered when a request for a spare part cannot be met" is not made. For Eq. (4.33) it holds necessarily that no further failures are considered when a request for a spare part cannot be met (system down states are absorbing).

Generalization of the repair rate leads to semi-regenerative processes with $n-k+1$ regeneration and $n-k$ not regeneration states (Section 6.5.2, Appendix A7.7). For instance, assuming for the repair time a density $g(t)$, a mean $MTTR$, and a variance $\text{Var}[\tau]$, Eq. (6.110) with $k\lambda$ instead of λ and $\lambda_r \equiv 0$ (see supplementary results in Example A7.12) and $\tilde{g}(\lambda)$ per Eq. (6.113), lead to

$$\begin{aligned} PA_{S1} &= \frac{k\lambda}{(k\lambda)^2 MTTR + k\lambda \tilde{g}(k\lambda)} \approx \frac{1}{1 + (k\lambda)^2 (MTTR^2 + \text{Var}[\tau]) / 2} \\ &\approx 1 - (k\lambda MTTR)^2 (1 + \text{Var}[\tau] / MTTR^2) / 2 \gtrsim 1 - (k\lambda MTTR)^2, \end{aligned} \quad (4.34)$$

$n_{sp} = n-k = 1$ spare part, 1 repair crew, Case 1.

Similarly, Eq. (6.108) with $k\lambda$ instead of λ and $\lambda_r \equiv 0$ and Eq. (6.114) lead to

$$R_{S01}(t) \approx e^{-tk\lambda(1-\tilde{g}(k\lambda))} \approx e^{-t(k\lambda)^2 MTTR}, \quad (4.35)$$

$n_{sp} = n-k = 1$ spare part, 1 repair crew, Case 2.

The last approximation in Eq. (4.34) assumes for the coefficient of variation κ that

$$\kappa^2 = \text{Var}[\tau] / E^2[\tau] \leq 1, \quad (4.36)$$

which holds for distribution functions used for repair times (increasing repair rate). Assuming $MTTR = 1/\mu$, i. e., the same mean time to repair disregarding the distribution of the repair time, the last approximations in Eqs. (4.34) and (4.35) yield the same result as given by Eqs. (4.26) and (4.29), showing, once more, the *small influence of the repair time distribution on results at system level*. The last approximation in Eq. (4.35) is obtained by assuming $k\lambda MTTR \ll 1$, i. e. using $\tilde{g}(k\lambda) \approx 1 - k\lambda MTTR$ (Eq. (6.114)). For the approximation in Eq. (4.34) it was necessary to use $\tilde{g}(k\lambda) \approx 1 - k\lambda MTTR + (k\lambda)^2 (MTTR^2 + \text{Var}[\tau]) / 2$ (Eq. (6.113)).

Taking $R_S(t) = e^{-t/MTTF_S}$ in Eqs. (4.31), (4.33) & (4.35), and PA_S as in Eqs. (4.28), (4.32) & (4.34), PA_S can be expressed as (Eq. (A7.189))

$$PA_S \approx 1 - MTTR_S / MTTF_S, \quad (4.37)$$

with $MTTR_S = 1/\mu$, $MTTR_S = 1/(n-k+1)\mu$ & $MTTR_S = MTTR$, respectively.

The results of Sections 4.5.1-4.5.3, in particular those on *decentralized logistic support*, can be extended to cover the case of systems with *different spare parts*.

4.6 Maintenance Strategies

Maintenance strategies can be very different according to the objective to be reached (choice between maintenance policies, minimization of system down time or spare parts, availability maximization by given cost and/or logistic support, etc.). Among possible maintenance strategies [2.34, 4.0, 4.1, 4.2, 4.6, 4.8, 4.14, 4.18, 4.30, 6.3, A7.4(1962)], this section unifies and extends basic repair/replacement policies. Preliminary investigations on a new approach for mission oriented high safety systems (superimposing a periodic check to the preventive maintenance) are in [4.26]. Cost aspects are considered in this section and in Section 4.7. For undetected fault times, e. g. by uncovered (latent) failures, one can refer to Eqs. (A6.30) & (6.223).

In the following it is assumed that the item is new at $t=0$, its failure-free time $\tau > 0$ has distribution function $F(x)$, density $f(x)$, $E[\tau]$ & $\text{Var}[\tau] < \infty$ and, in Sections 4.6.1 & 4.6.2, repairs/replacements are performed in a negligible time. Section 4.6.1 considers the case in which the item is *as-good-as-new* after each maintenance action, planned (preventive maintenance) or at failure. In section 4.6.2, the item is *as-good-as-new* only after planned maintenance actions, but *as-bad-as-old* after repairs (*minimal repair* at failure). Further considerations are in Section 4.6.3. ⁺

4.6.1 Complete renewal at each maintenance action

In this section it is assumed that each maintenance action, planned or at failure, brings the item considered to *as-good-as-new* (see e.g. remarks on pp. 8 and 171 for complex items), yielding to a *renewal point* for the underlying point process.

Among possible strategies to avoid *wear out failures* or *effects of sudden failures*, replacements ⁺⁺ can be performed basically

- (a) at a given (fixed) operating time T_{PM} or at failure if the operating time is shorter than T_{PM} (*age replacement*, Fig. 4.5a),
- (b) at given (fixed) time points $T_{PM}, 2T_{PM}, \dots$ or at failure (*block replacement*, Fig. 4.5b),
- (fix) only at given (fixed) time points $T_{PM}, 2T_{PM}, \dots$ (*fix replacement*, Fig. 4.5c),
- (of) only at failure (ordinary renewal process without truncation).

⁺ Considering the remarks to Eqs. (A6.27)-(A6.29), preventive maintenance is useful (necessary) only for items with *increasing failure rate*, tacitly assumed here.

⁺⁺ Replacement is used here instead of *renewal*, to agree with established literature.

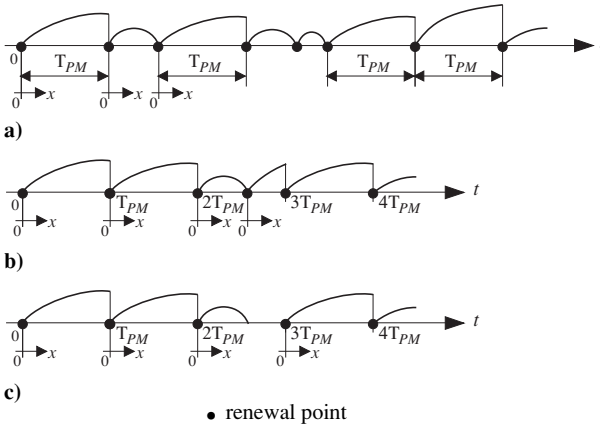


Figure 4.5 Possible time schedules for a *repairable item with preventive maintenance (PM) and repair (renewal) times of negligible length* (item new at $t = 0$ and at each repair or PM, x starts by 0 at each renewal point): **a)** After T_{PM} operating hours or at failure (age replacement); **b)** At fixed times $T_{PM}, 2T_{PM}, \dots$ or at failure (block replacement); **c)** At times $T_{PM}, 2T_{PM}, \dots$ (fix replacement)

Considering first the case of *age replacement* (Fig. 4.5a), results of Appendix A7.2 for renewal processes and Section 4.5 for spare parts provisioning can be used, taking for the failure-free time τ_{repl_a} the truncated distribution function $F_{repl_a}(x)$

$$F_{repl_a}(x) = \Pr\{\tau_{repl_a} \leq x\} = \begin{cases} F(x) & \text{for } 0 < x < T_{PM}, \\ 1 & \text{for } x \geq T_{PM}, \end{cases} \quad F(0) = F_{repl_a}(0) = 0. \dots \quad (4.38)$$

Taking care of $\Pr\{\tau_{repl_a} = T_{PM}\} = 1 - F(T_{PM})$, the mean time to replacement follows as

$$E[\tau_{repl_a}] = \int_0^{T_{PM}} x f(x) dx + (1 - F(T_{PM})) T_{PM} = \int_0^{T_{PM}} (1 - F(x)) dx < T_{PM}. \quad (4.39)$$

Defining as $v_a(t)$ the number of renewals in $(0, t]$ on age replacement policy (replacements at failure & preventive maintenance), it follows from Eq. (A7.15) that

$$E[v_a(t)] = H_a(t), \quad t > 0, \quad v_a(0) = H_a(0) = 0, \quad (4.40)$$

(with $F_1(x) = F(x) = F_{repl_a}(x)$ in Eq. (A7.15)). Furthermore, Eq. (A7.27) yields

$$\lim_{t \rightarrow \infty} E[v_a(t)] = t / E[\tau_{repl_a}] = t / \int_0^{T_{PM}} (1 - F(x)) dx, \quad (4.41)$$

in the proportion $F(T_{PM})$ for replacements at failure and $1 - F(T_{PM})$ for replacements at age. Thus, with c_f and c_{ar} as cost for replacement at failure and at age, the mean total cost per unit time (cost rate) is

$$\lim_{t \rightarrow \infty} E[c_a / t] = [c_f F(T_{PM}) + c_{ar} (1 - F(T_{PM}))] / \int_0^{T_{PM}} (1 - F(x)) dx. \quad (4.42)$$

From Eq. (4.42) one recognizes that $E[c_a/t] \rightarrow \infty$ for $T_{PM} \rightarrow 0$ and $\rightarrow c_f/E[\tau]$ for $T_{PM} \rightarrow \infty$; with $E[\tau]$ as mean of the failure-free time τ of the item considered (Eq. (A6.38)). Optimization of c_a/t is considered with Eq. (4.49). Reliability and availability is investigated in Section 6.8.2 (Eqs. (6.192) - (6.195)).

For the case of *block replacement* (Fig 4.5b), one or more failures can occur during an interval $(kT_{PM}, (k+1)T_{PM})$ ($k=0,1,\dots$), with consequent repair. For the expected total number of renewals in $(0, nT_{PM})$ on block replacement policy (replacements at failure and preventive maintenance) it follows that

$$E[v_b(nT_{PM})] = nH(T_{PM}) + n, \quad n=1,2,\dots, T_{PM} > 0, v_b(0) = H(0) = 0, \quad (4.43)$$

where $H(T_{PM})$ is the renewal function at T_{PM} (Eq. (A7.15) with $F_1(x)=F(x)$ as distribution function of the failure-free time of the item considered. With c_f & c_{br} as cost for replacement at failure and at $T_{PM}, 2T_{PM}, \dots$, respectively, the mean total cost per unit time is

$$E[c_b/nT_{PM}] = [c_f H(T_{PM}) + c_{br}] / T_{PM}, \quad T_{PM} > 0, H(0) = 0. \quad (4.44)$$

From Eq. (4.44) one recognizes that $E[c_b/nT_{PM}] \rightarrow \infty$ for $T_{PM} \rightarrow 0$ and, using Eq. (A7.27), $E[c_b/nT_{PM}] \rightarrow c_f/E[\tau]$ for $T_{PM} \rightarrow \infty$; with $E[\tau]$ as mean of the failure free time τ of the item considered. Optimization of c_b is considered with Eq. (4.52).

For *fix replacement* (Fig. 4.5c), i. e., replacement only at times $T_{PM}, 2T_{PM}, \dots$ (taking in charge that for a failure in $(kT_{PM}, (k+1)T_{PM})$ ($k=0,1,\dots$) the item is down from failure time to $(k+1)T_{PM}$), the expected number of renewals in $(0, nT_{PM})$ is

$$E[v_{fix}(nT_{PM})] = n, \quad n=1,2,\dots, T_{PM} > 0, v_{fix}(0) = 0. \quad (4.45)$$

With c_{fix} as cost for replacement at $T_{PM}, 2T_{PM}, \dots$, the mean total cost per unit time is

$$E[c_{fix}/nT_{PM}] = c_f / T_{PM}. \quad (4.46)$$

The number of failures in $(0, nT_{PM})$ has a binomial distribution. Setting c_d = cost per unit down time, Eq. (A6.30) yields $E[c_{fix}/nT_{PM}] = [c_f + c_d \int_0^{T_{PM}} F(x) dx] / T_{PM}$.

The *replacement only at failure* leads to an ordinary renewal process (Appendix A7.2), yielding results of Section 4.5 on spare parts provisioning, in particular,

$$\lim_{n \rightarrow \infty} E[v_{of}(nT_{PM})] = nT_{PM} / E[\tau], \quad n=1,2,\dots, T_{PM} > 0, v_{of}(0) = 0, \quad (4.47)$$

with $E[\tau]$ as mean of the failure-free time τ of the item considered, and

$$\lim_{n \rightarrow \infty} E[c_{of}/nT_{PM}] = c_f / E[\tau], \quad n=1,2,\dots, T_{PM} > 0. \quad (4.48)$$

One recognizes that for large nT_{PM} , $E[v_{of}(nT_{PM})] \leq E[v_a(nT_{PM})] \leq E[v_b(nT_{PM})]$. This follows for v_{of} versus v_a by comparing Eqs. (4.41) and (4.47), and for v_a versus v_b heuristically from Fig. 4.5 (at least one failure-free time will be truncated for large n and the probability for a truncation is greater for case b) than for case a)) or by considering $H(t) \geq t / (\int_0^t (1-F(x)) dx) - 1$, for increasing failure rate [2.34 (1965)].

For age and block replacement policy it is basically possible to *optimize* T_{PM} . Setting the derivative with respect to T_{PM} equal to 0, Eq. (4.42) yields for $T_{PMa_{opt}}$

$$\lambda(T_{PMa_{opt}}) \int_0^{T_{PMa_{opt}}} (1 - F(x)) dx - F(T_{PMa_{opt}}) = \frac{c_{ar}}{c_f - c_{ar}}, \quad c_f > c_{ar}, \quad (4.49)$$

with $\lambda(x)$ as failure rate of the item considered (Eq. (A6.25)), and thus (Eq. (4.42))

$$\lim_{t \rightarrow \infty} E[c_{a_{opt}} / t] = (c_f - c_{ar}) \lambda(T_{PMa_{opt}}), \quad (4.50)$$

if $T_{PMa_{opt}} < \infty$ exist. For *strictly increasing failure rate* $\lambda(x)$, $T_{PMa_{opt}} < \infty$ exist for

$$\lambda(\infty) > c_f / (E[\tau](c_f - c_{ar})), \quad (4.51)$$

see Example 4.6. $\lambda(\infty) \leq c_f / (E[\tau](c_f - c_{ar}))$, $\lambda(x) = \lambda$, or $c_f \leq c_{ar}$ leads to a replacement only at failure ($T_{PM} = \infty$). Similarly, Eq. (4.44) yields

$$T_{PMb_{opt}} h(T_{PMb_{opt}}) - H(T_{PMb_{opt}}) = c_{br} / c_f, \quad (4.52)$$

with $h(x) = dH(x) / dx$ as renewal density (Eq. (A7.18)), and thus (Eq. (4.44))

$$\lim_{t \rightarrow \infty} E[c_{b_{opt}} / t] = c_f h(T_{PMb_{opt}}), \quad (4.53)$$

if $T_{PMb_{opt}} < \infty$ exist. Equation (4.52) is a necessary condition (only). For *strictly increasing failure rate*, at least one $T_{PMb_{opt}} < \infty$ exist for

$$1 - \text{Var}[\tau] / E^2[\tau] > 2 c_{br} / c_f, \quad \text{implying also} \quad c_f > 2 c_{br}, \quad (4.54)$$

see Example 4.6. $1 - \text{Var}[\tau] / E^2[\tau] \leq 2 c_{br} / c_f$ or $\lambda(x) = \lambda$ leads to a replacement only at failure ($T_{PM} = \infty$).

Example 4.6

Investigate Eqs. (4.49) and (4.52).

Solution

- (i) To Eq. (4.49), with $T_{PMa_{opt}}$ replaced by T for simplicity, one can recognize that for *strictly increasing failure rate* $\lambda(x)$, $\lambda(T) \int_0^T (1 - F(x)) dx - F(T)$ is *strictly increasing in* T , from 0 to $\lambda(\infty)E[\tau] - 1$. In fact, for $T_2 > T_1$ it holds that

$$\lambda(T_2) \int_0^{T_1} (1 - F(x)) dx + \lambda(T_2) \int_{T_1}^{T_2} (1 - F(x)) dx - F(T_1) - \int_{T_1}^{T_2} f(x) dx > \lambda(T_1) \int_0^{T_1} (1 - F(x)) dx - F(T_1),$$

considering $\lambda(T_2) > \lambda(T_1)$ and $\int_{T_1}^{T_2} f(x) dx = \int_{T_1}^{T_2} \lambda(x)(1 - F(x)) dx < \lambda(T_2) \int_{T_1}^{T_2} (1 - F(x)) dx$. Thus, $T < \infty$ exist for $\lambda(\infty)E[\tau] - 1 > c_{ar} / (c_f - c_{ar})$, i.e. for $\lambda(\infty) > c_f / (E[\tau](c_f - c_{ar}))$. However, an analytical expression for $T_{PMa_{opt}}$ is rarely possible, see e.g. [4.8] for numerical solutions.

- (ii) To Eq. (4.52) one can recognize that for *strictly increasing failure rate* $\lambda(x)$, $Th(T) - H(T) \rightarrow (1 - \text{Var}[\tau] / E^2[\tau]) / 2 > 0$ for $T \rightarrow \infty$ and thus, considering $H(0) = 0$, at least one $T < \infty$ exist for $(1 - \text{Var}[\tau] / E^2[\tau]) / 2 > c_{br} / c_f$. This follows from Eqs. (A7.28) & (A7.31) by considering $\text{Var}[\tau] < E^2[\tau]$ for strictly increasing failure rate [2.34 (1965)], see e.g. Fig. 4.4.

Comparison of cost per unit time is straightforward for fix replacement versus replacement only at failure (Eqs. (4.46) & (4.48)), but can become laborious for age replacement versus block replacement and / or replacement only at failure (Eqs. (4.42), (4.44)), (4.48), and (4.49) - (4.54)). In general, it must be performed on a case-by-case basis, often taking care that $c_f > c_{ar} > c_{br}$ and of other aspects like e.g. the importance to avoid wear out or sudden failures. Besides remarks to Eqs. (4.51) & (4.54) for $\lambda(x) = \lambda$, the following general results can be given for large t or nT_{PM} :

1. For strictly increasing failure rate $\lambda(x)$ and $\lambda(\infty) > c_f / (E[\tau](c_f - c_{ar}))$ (Eq. (4.51)), $T_{PMa_{opt}} < \infty$ exist (see e.g. [4.8] for numerical solutions) and, for large t , optimal age replacement (Eq. (4.50)) is better (cheaper) than replacement only at failure ($E[c_a / t]$ per Eq. (4.42) crosses from above $E[c_{of} / t] = c_f / E[\tau]$).
2. Considering Eq. (A7.28) for an ordinary renewal process ($MTTF_A = MTTF = E[\tau]$), it follows that $H(T_{PM}) \rightarrow T_{PM} / E[\tau] + (\text{Var}[\tau] / E^2[\tau] - 1) / 2$ for $T_{PM} \rightarrow \infty$. Thus, considering Eqs. (4.53) & (4.48), for $c_{br} / c_f < (1 - \text{Var}[\tau] / E^2[\tau]) / 2$ optimal block replacement *can be better* (cheaper) than replacement only at failure; however, this implies $\text{Var}[\tau] / E^2[\tau] < 1$ (strictly increasing failure rate) and $c_f > 2 c_{br}$.
3. For $c_f > c_{br} \geq c_{ar}$ optimal age replacement is better (cheaper) than optimal block replacement [4.1]; however, often one has $c_{br} < c_{ar}$.
4. For $c_{ar} = c_{br} = c_f$, $E[c_{of} / nT_{PM}] \leq E[c_a / nT_{PM}] \leq E[c_b / nT_{PM}]$ (follows from $E[v_{of}(nT_{PM})] \leq E[v_a(nT_{PM})] \leq E[v_b(nT_{PM})]$, see remarks to Eq. (4.48)).

4.6.2 Block replacement with minimal repair at failure

Let now consider the situation in which the item is *as-good-as-new* after planned replacements, but *as-bad-as-old* after repairs; i.e., *minimal repair* is performed, and the item's failure rate after repair is *assumed to be the same as just before failure* [2.34.6.1]. However, minimal repair means that only the failed part E_i of the item is repaired to as-good-as-new; $\lambda_i(x)$ restarts at $\lambda_i(0)$, and for $\lambda_i(x) \neq \lambda_i(0)$ the item's failure rate can only approximately be the same as just before the failure (see also pp. 427 & 519).

One can recognize that the case of *maintenance only at failure* leads to a *non-homogeneous Poisson* process with intensity $m(t)$ equal the failure rate $\lambda(t)$ of the item considered and mean value function $M(t) = \int_0^t \lambda(x) dx$, i.e. (considering $F(0) = 0$)

$$m(t) = \lambda(t) = \frac{f(t)}{1 - F(t)} \quad \text{and} \quad M(t) = \int_0^t m(x) dx = \int_0^t \frac{f(x)}{1 - F(x)} dx = -\ln(1 - F(t)), \quad (4.55)$$

see Point 2 on p. 519. For this reason, minimal repair can not be considered for a *maintenance only at failure*, because for strictly increasing failure rate the item continue to degenerate and at a given time it will be necessary to reestablish the as-good-as-new situation for the whole item.

Similar is for *age replacement*, in particular for T_{PM} large. For an exact evaluation, results from Appendices A7.4 (p. 479) and A7.6 (p. 514) on regenerative processes can be used (successive occurrence of replacements at age constitute a cycle).

For *block replacement with minimal repair*, change with respect to Section 4.6.1 is the fact that between consecutive replacements at $T_{PM}, 2T_{PM}, \dots$ the involved point process is a nonhomogeneous Poisson process (Eq.(4.55), Appendix A7.8.2). Defining c_{br} and $c_{f_{mr}}$ as cost for replacement at block and minimal repair, respectively, the total cost per unit time follows as (see also Eqs. (4.44) & (4.55))

$$E[c_{b_{mr}} / nT_{PM}] = \frac{c_{f_{mr}} M(T_{PM}) + c_{br}}{T_{PM}} = \frac{-c_{f_{mr}} \ln(1 - F(T_{PM})) + c_{br}}{T_{PM}}. \quad (4.56)$$

From Eq. (4.56) one recognizes that $E[c_{b_{mr}} / nT_{PM}] \rightarrow \infty$ for $T_{PM} \rightarrow 0$ and $\rightarrow c_{f_{mr}} \lambda(\infty)$ for $T_{PM} \rightarrow \infty$. Optimization of T_{PM} yields (considering $\partial / \partial T_{PM} = 0$ and Eq. (4.55))

$$T_{PMb_{mr}opt} \lambda(T_{PMb_{mr}opt}) - \int_0^{T_{PMb_{mr}opt}} \lambda(t) dt = c_{br} / c_{f_{mr}}. \quad (4.57)$$

and thus Eqs. (4.55) & (4.56))

$$E[c_{b_{mr}opt} / nT_{PMb_{mr}opt}] = c_{f_{mr}} \lambda(T_{PMb_{mr}opt}), \quad (4.58)$$

if $T_{PMb_{mr}opt} < \infty$ exist. For $\lambda(t)$ strictly increasing, with $\lambda(0) = 0$, $T \lambda(T) - \int_0^T \lambda(t) dt$ is strictly increasing in T and can cross from below $c_{br} / c_{f_{mr}}$ at $T = T_{PMb_{mr}opt} < \infty$. This occurs for $\lambda(\infty) = \infty$; for $\lambda(\infty) = \lambda < \infty$, $T_{PMb_{mr}opt} < \infty$ exist for

$$\lim_{t \rightarrow \infty} [\lambda t - \int_0^t \lambda(x) dx] > c_{br} / c_{f_{mr}}, \quad \lambda = \lambda(\infty). \quad (4.59)$$

No solution exist for $\lambda(t)$ constant. Taking as an example a *Weibull* distribution (Eq. A.6.89), for which $\lambda(t) = \beta \lambda^\beta t^{\beta-1}$ and $E[\tau] = \Gamma(1+1/\beta) / \lambda$ one obtains for $\beta > 1$

$$T_{PMb_{mr}opt} = \frac{\sqrt[\beta]{c_{br} / ((\beta - 1) c_{f_{mr}})}}{\lambda} \quad \text{and} \quad E[c_{b_{mr}opt} / nT_{PMb_{mr}opt}] \approx \frac{\beta c_{br}}{(\beta - 1) T_{PMb_{mr}opt}}. \quad (4.60)$$

Cost comparison with results of Section 4.6.1 has to be performed on a case-by-case basis. For the Weibull distribution, Eqs. (4.60) and (4.48) show, for instance, that for $c_{f_{mr}} > ((\beta - 1) / c_{br})^{\beta-1} (c_f / \Gamma(1/\beta))^\beta$ replacement only at failure is better (cheaper) than block replacement with minimal repair (using $(\Gamma(1+1/\beta))^\beta = (\Gamma(1/\beta))^\beta / \beta^\beta$).

4.6.3 Further considerations on maintenance strategies

For the case of non negligible repair and preventive maintenance times, with mean $MTTR$ and $MTTPM$, *asymptotic & steady-state overall availability* OA_S (Eq. (6.196)) can be optimized with respect to preventive maintenance period T_{PM} .

In fact, considering Eq. (4.41), Eq. (6.196) leads to $OA_S = E[\tau_{repl_a}] / [E[\tau_{repl_a}] + F(T_{PM})MTTR + (1-F(T_{PM}))MTTPM]$ for *age replacement*, Eq. (4.43) to $OA_S = T_{PM} / [T_{PM} + H(T_{PM})MTTR + MTTPM]$ for *block replacement*, and Eq. (4.56) to $OA_S = T_{PM} / [T_{PM} + MTTR \int_0^{T_m} \lambda(x) dx + MTTPM]$ for *block replacement with minimal repair*. Optimization follows using $\partial PA_S / \partial T_{PM} = 0$, and leads to Eqs. (4.49), (4.52), (4.57) with c_{ar} & c_{br} replaced by $MTTPM$, c_f by $MTTR$, c_{fmr} by $MTTMR$, respectively ($MTTMR =$ mean time to minimal repair).

Besides the previous replacement strategies, a further possibility is to assume that at times $T_{PM}, 2T_{PM}, \dots$ the system is inspected, and replacement at $(k+1)T_{PM}$ is performed only if a failure is occurred between kT_{PM} and $(k+1)T_{PM}$. If the failure-free time τ is > 0 with $F(x) = \Pr\{\tau \leq x\}$, the replacement time τ_{rep} has distribution

$$\Pr\{\tau_{rep} = kT_{PM}\} = F(kT_{PM}) - F((k-1)T_{PM}), \quad k=1, 2, \dots, F(0) = 0. \quad (4.61)$$

This case has been investigated in [6.17] with cost considerations. If $c_i =$ inspection cost, $c_r =$ cost for replacement, and $c_d =$ cost for unit of time (h) in which the system is down waiting for replacement ($c_i, c_r, c_d > 0$), the total cost C per unit time is for $t = nT_{PM} \rightarrow \infty$ given by

$$C = \frac{nc_i}{nT_{PM}} + \frac{c_r nT_{PM} / E[\tau_{rep}]}{nT_{PM}} + \frac{c_d E[\tau_{rep} - \tau]}{E[\tau_{rep}]} = \frac{c_i}{T_{PM}} + \frac{c_r}{E[\tau_{rep}]} - \frac{c_d MTF}{E[\tau_{rep}]} + c_d, \quad (4.62)$$

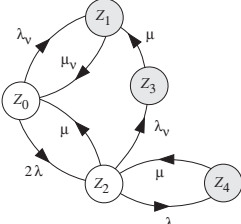
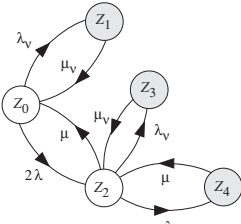
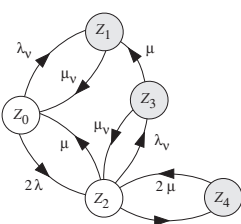
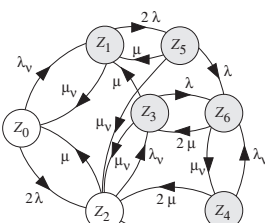
where $MTF = E[\tau]$. For $T_{PM} \rightarrow \infty$, $E[\tau_{repl}] \rightarrow \infty$ and $C \rightarrow c_d$. Thus, inspection is useful for $C < c_d$. For given $F(x)$ it is possible to find a T_{PM} which minimizes C [6.17].

For the *mission availability* and *work-mission availability*, as defined by Eqs. (6.28) and (6.31), it can be asked in some applications that the number of repairs (replacements) be limited to N (e.g. because only N spare parts are available). In this case, the summation in Eqs. (6.29) and (6.32) goes up to $n = N + 1$. If k elements E_1, \dots, E_k with constant failure rates $\lambda_1, \dots, \lambda_k$ and constant repair rates μ_1, \dots, μ_k are in series, a good approximation for the work-mission availability with *limited repairs* is obtained by multiplying the probability for total system down time $\leq x$ for unlimited repairs (Eq. (7.22) with $\lambda = \lambda_S$ and $\mu = \mu_S$ from Table 6.10 (2 nd row)) with the k probabilities that N_i spare parts will be sufficient for element E_i [6.11].

A strategy can also be based on the repair time τ itself. Assuming, for instance, that if the repair is not finished at time Δ the failed element is replaced at time Δ by a new one in a negligible time, the distribution function $G(x)$ of the repair times τ is truncated at Δ (Eq. (4.38)). For the case of const. repair rate μ , the Laplace transform of $G(x)$ to be used in reliability computations is given by (Appendix A9.7) $\tilde{G}(s) = (\mu + s \cdot e^{-(s+\mu)\Delta}) / s(s+\mu)$, yielding $E[\tau] = (1 - e^{-\mu\Delta}) / \mu$ as per Eq. (4.39).

Further maintenance strategies are, for instance, in [2.34, 4.18, 4.30, A7.4 (62)]. A comparison between some different maintenance strategies with respect to reliability and availability is given in Table 4.4 for a basic reliability structure (Fig. 6.15). Expression for MTF_{S0} is the same for all cases in Table 4.4 and given by Eq. (6.157).

Table 4.4 Four repair strategies applied to a 1-out-of-2 active redundancy in series with E_v as per Figs. 6.15 & A7.6 (constant failure and repair rates ($\lambda, \lambda_v \ll \mu, \mu_v$), ideal failure detection & switch, Markov processes, no FF=no further failures at system down for cases a-c, $PA_S=AA_S$ =asymptotic & steady-state point and average availability; same $MTTF_{S0}$ given by Eq. (6.157) for a-d)

 <p>a) One repair crew, no repair priority, no FF</p>	<p>$PA_S = AA_S$, obtained by solving (see Eq. (1.157) for $MTTF_{S0}$)</p> $(2\lambda + \lambda_v)P_0 = \mu_v P_1 + \mu P_2, \quad \mu_v P_1 = \lambda_v P_0 + \mu P_3, \quad \mu P_3 = \lambda_v P_2,$ $(\lambda + \lambda_v + \mu)P_2 = 2\lambda P_0 + \mu P_4, \quad P_0 + P_1 + P_2 + P_3 + P_4 = 1,$ <p>is given by (Eq. (6.162))</p> $PA_S = AA_S = P_0 + P_2 = \frac{1}{1 + \lambda_v / \mu_v + 2\lambda^2 (1 + \lambda_v / \lambda) / \mu^2 (1 + 2\lambda + \lambda_v) / \mu}$ $\approx 1 - \lambda_v / \mu_v - 2(\lambda / \mu)^2 - 2\lambda \lambda_v / \mu^2 + 2\lambda (2\lambda^2 + 3\lambda \lambda_v + \lambda_v^2) / \mu^3$
 <p>b) One repair crew, repair priority on E_v, no FF</p>	<p>$PA_S = AA_S$, obtained by solving (see Eq. (1.157) for $MTTF_{S0}$)</p> $(2\lambda + \lambda_v)P_0 = \mu_v P_1 + \mu P_2, \quad \mu_v P_1 = \lambda_v P_0, \quad \mu_v P_3 = \lambda_v P_2,$ $(\lambda + \lambda_v + \mu)P_2 = 2\lambda P_0 + \mu_v P_3 + \mu P_4, \quad P_0 + P_1 + P_2 + P_3 + P_4 = 1,$ <p>is given by (Eq. (6.160))</p> $PA_S = AA_S = P_0 + P_2 = \frac{1}{1 + \lambda_v / \mu_v + 2\lambda^2 / \mu^2 (1 + 2\lambda / \mu)}$ $\approx 1 - \lambda_v / \mu_v - 2(\lambda / \mu)^2 + 4(\lambda / \mu)^3$
 <p>c) 2 repair crews, no priority, no FF</p>	<p>$PA_S = AA_S$, obtained by solving (see Eq. (1.157) for $MTTF_{S0}$)</p> $(2\lambda + \lambda_v)P_0 = \mu_v P_1 + \mu P_2, \quad \mu_v P_1 = \lambda_v P_0 + \mu P_3, \quad (\mu + \mu_v)P_3 = \lambda_v P_2,$ $(\lambda + \lambda_v + \mu)P_2 = 2\lambda P_0 + \mu_v P_3 + 2\mu P_4, \quad P_0 + P_1 + P_2 + P_3 + P_4 = 1,$ <p>is given by</p> $PA_S = AA_S = P_0 + P_2 = \frac{1}{1 + \lambda_v / \mu_v + \lambda^2 / \mu^2 (1 + 2\lambda / \mu + \lambda_v / (\mu + \mu_v))}$ $\approx 1 - \lambda_v / \mu_v - (\lambda / \mu)^2 + 2(\lambda / \mu)^3 + \lambda^2 \lambda_v / \mu^2 (\mu + \mu_v)$
 <p>d) Totally independent elements, i.e. 3 repair crews</p>	<p>$PA_S = AA_S$, obtained by solving (see Eq. (1.157) for $MTTF_{S0}$)</p> $(2\lambda + \lambda_v)P_0 = \mu_v P_1 + \mu P_2, \quad (2\lambda + \mu_v)P_1 = \lambda_v P_0 + \mu P_3 + \mu P_5,$ $(\lambda + \lambda_v + \mu)P_2 = 2\lambda P_0 + \mu_v P_3 + 2\mu P_4 + \mu_v P_5, \quad (\lambda + \mu + \mu_v)P_5 = 2\lambda P_1,$ $(\lambda + \mu + \mu_v)P_3 = \lambda_v P_2 + 2\mu P_6, \quad (\lambda_v + 2\mu)P_4 = \lambda P_2 + \mu_v P_6, \quad P_0 + \dots + P_6 = 1,$ <p>(or directly using Eq. (2.48) or Table 6.9), is given by</p> $PA_S = AA_S = P_0 + P_2 = \frac{1}{1 + \lambda_v / \mu_v} \left(\frac{2}{1 + \lambda / \mu} - \frac{1}{(1 + \lambda / \mu)^2} \right)$ $\approx 1 - \lambda_v / \mu_v - (\lambda / \mu)^2 + 2(\lambda / \mu)^3 + \lambda^2 \lambda_v / \mu^2 \mu_v$

approximations given up to $(\lambda / \mu)^3$; considering $(3\lambda + \lambda_v) < \mu$ it holds that $PA_{S(a)} \leq PA_{S(b)} \leq PA_{S(c)} \leq PA_{S(d)}$; for case d, failures at system down possible (7 instead of $2^3=8$ states because of 2 identical redundant elements)

4.7 Basic Cost Considerations

Cost considerations are important in practical applications and apply, in particular, to spare parts provisioning (Section 4.5) and maintenance strategies (Section 4.6). In addition to the considerations in Sections 4.5 and 4.6, this section considers two basic models based on homogeneous Poisson processes (HPP) with fixed and random costs.

As a first example consider the case in which a constant cost c_0 is related to each repair of a given item. Assuming that repair duration is negligible and times between successive failures are independent and exponentially distributed with parameter λ , the failure flow is a homogeneous Poisson process and the probability for n failures during the operating time t is given by (Eq.(A7.41))

$$\Pr\{n \text{ failures in } (0,t] \mid \lambda\} = \Pr\{v(t) = n \mid \lambda\} = \frac{(\lambda t)^n}{n!} e^{-\lambda t}, \quad n=0,1,2,\dots, \quad t > 0, v(0)=0. \quad (4.63)$$

Eq. (4.63) is also the probability that the cumulated repair cost over t is $C = n c_0$. Mean and variance of C are (Eqs. (A6.40) and (A6.46) with Eq. (A7.42))

$$E[C] = c_0 \lambda t \quad \text{and} \quad \text{Var}[C] = c_0^2 \lambda t. \quad (4.64)$$

For large λt , C is approximately normally distributed (Eqs. (A6.105)) with mean and variance as per Eq. (4.64), see e.g. [A8.8].

If repair cost is a random variable $\xi_i > 0$ distributed according to $F(x) = \Pr\{\xi_i \leq x\}$ ($F(0) = 0$, $i = 1, 2, \dots$), ξ_1, ξ_2, \dots are mutually independent and independent of the count function $v(t)$ giving the number of failures in the *operating time* interval $(0,t]$, and ξ_t is the sum of ξ_i over $(0,t]$, it holds that (Eq. (A7.218))

$$\xi_t = \sum_{i=1}^{v(t)} \xi_i, \quad v(t) = 1, 2, \dots, \quad t > 0, v(0) = 0, \quad \xi_t = 0 \text{ for } v(t) = 0. \quad (4.65)$$

ξ_t is distributed as the (cumulative) repair time for failures occurred in a total operating time t of a repairable item, and is thus given by the *work-mission availability* $WMA_{S0}(T_0, x)$ (Eq. (6.32) with $T_0 = t$). Assuming that the failures flow is a homogeneous Poisson process (HPP) with parameter λ , all ξ_i are mutually independent, independent of $v(t)$, and have the same exponential distribution with parameter μ , Eq. (6.32) with constant failure and repair rates $\lambda(x) = \lambda$ and $\mu(x) = \mu$ and $T_0 = t$ yields (Eqs. (6.33), (A7.219))

$$\begin{aligned} \Pr\{\xi_t \leq x\} &= WMA_{S0}(t, x) = e^{-\lambda t} + \sum_{n=1}^{\infty} \left[\frac{(\lambda t)^n}{n!} e^{-\lambda t} \left(1 - \sum_{k=0}^{n-1} \frac{(\mu x)^k}{k!} e^{-\mu x} \right) \right] \\ &= 1 - e^{-(\lambda t + \mu x)} \sum_{n=1}^{\infty} \left[\frac{(\lambda t)^n}{n!} \sum_{k=0}^{n-1} \frac{(\mu x)^k}{k!} \right], \quad t > 0 \text{ given, } x > 0, \Pr\{\xi_t = 0\} = e^{-\lambda t}. \quad (4.66) \end{aligned}$$

Mean and variance of ξ_t follow as (Eq. (A7.220), see also Eqs. (4.66), (A6.38), (A6.45), (A6.41))

$$E[\xi_t] = \lambda t / \mu \quad \text{and} \quad \text{Var}[\xi_t] = 2\lambda t / \mu^2. \quad (4.67)$$

Furthermore, for $t \rightarrow \infty$ the distribution of ξ_t approach a normal distribution with mean and variance as per Eq. (4.67). Moments of ξ_t can also be obtained for arbitrary $F(x) = \text{Pr}\{\xi_i \leq x\}$, with $F(0) = 0$ (Example A7.14, Eq. (A7.221))

$$E[\xi_t] = E[v(t)] E[\xi_i] \quad \text{and} \quad \text{Var}[\xi_t] = E[v(t)] \text{Var}[\xi_i] + \text{Var}[v(t)] E^2[\xi_i]. \quad (4.68)$$

Of interest in some practical applications can also be the distribution of the time τ_C at which the cumulative cost ξ_t crosses a give (fixed) barrier C . For the case given by Eq. (4.66) (in particular for $\xi_i > 0$), the events

$$\{\tau_C > t\} \quad \text{and} \quad \{\xi_t \leq C\} \quad (4.69)$$

are equivalent. Form Eq. (4.66) it follows then (Eq. (A7.223))

$$\text{Pr}\{\tau_C > t\} = 1 - e^{-(\lambda t + \mu C)} \sum_{n=1}^{\infty} \left[\frac{(\lambda t)^n}{n!} \sum_{k=0}^{n-1} \frac{(\mu C)^k}{k!} \right], \quad C > 0 \text{ given, } t > 0, \quad (4.70)$$

(in Eq. (4.70), C has dimension of μ^{-1}).

More general cost optimization strategies are often necessary in practical applications. For example, spare parts provisioning has to be considered as a parameter in the *optimization* between performance, reliability, availability, logistic support and *cost*, taking care of *obsolescence* aspects as well. In some cases, one parameter is given (e.g. cost) and the best logistic structure is sought to maximize system availability or system performance. Basic considerations, as discussed above and in Sections 1.2.9, 8.4, A6.10.7, A7.5.3.3, apply. However, even assuming constant failure and repair rates, numerical solutions can become necessary (see e.g. [4.32]).

5 Design Guidelines for Reliability, Maintainability, and Software Quality

Reliability, maintainability, and software quality *have to be built into complex equipment and systems* during the design and development phase. This has to be supported by *analytical investigations* (Chapters 2, 4, 6) as well as by *design guidelines* and *tests* (Chapters 5, 3, 7, 8). Developing design guidelines demands practical experience and engineering feeling. Adherence to such guidelines limits the influence of those aspects which can invalidate the models assumed for analytical investigations, and improve the *inherent* reliability, maintainability, and safety of both hardware & software. Each industry producing equipment and systems with high reliability (RAMS) requirements is aware of the necessity for such guidelines. This chapter gives a comprehensive list of design guidelines for reliability, maintainability (incl. human and safety aspects), and software quality of complex electronic and electromechanical equipment and systems, harmonized with industry's needs [1.2 (1996)] (see e. g. also [1.22, 5.0, 5.14, 5.28, 6.82] for military applications).

5.1 Design Guidelines for Reliability

Reliability analysis in the design and development phase (Chapter 2) gives an estimate of an item's true reliability, based on some assumptions regarding data used, interface problems, dependence between components, compatibility between materials, environmental influences, transients, EMC, ESD, etc., as well as on the quality of manufacture and the user's skill level. To consider exhaustively all these aspects is difficult. The following design guidelines can be used to alleviate intrinsic weaknesses and improve the inherent reliability of complex equipment and systems.

5.1.1 Derating

Thermal and electrical stresses greatly influence the failure rate of electronic components. *Derating* is mandatory to improve the inherent reliability of equipment and systems. Table 5.1 gives recommended *stress factors* S (Eq. (2.1)) to be used

Table 5.1 Recommended derating values for electronic components at ambient temperature $20^{\circ}\text{C} \leq \theta_A \leq 40^{\circ}\text{C}$

Component	Power	Voltage	Current	Internal Temperature	Frequency
Resistors • Fixed • Variable • Thermistors	0.6 0.6 0.4			0.8 0.7 0.7	
Capacitors • Film, Ceramic • Ta (solid) • Al (wet)		0.5 0.5 0.8		0.5 0.5 0.5	
Diodes • Gen. purpose • Zener	0.6	0.5*	0.6	0.7 0.7	
Transistors		0.5*	0.7	0.7	$0.1 f_T$
Thyristors, Triacs		0.6*	0.6	0.7	
Optoelectronic devices		0.5**	0.5	0.8	
ICs • Linear • Voltage reg. • Digital bipolar • Digital MOS		0.7	0.8+ 0.7+ 0.8+ 0.8+	0.7 ^x 0.7 ^x 0.7 ^x 0.7 ^x	0.9 0.9
Coils, Transf.	0.5				
Switches, Relays			0.4–0.7 ⁺⁺	0.7	0.5
Connectors		0.7	0.6	0.8	0.5

* breakdown voltage; ** isolation voltage (0.7 for U_{in});

+ sink current; ++ low values for inductive loads; ^x $\theta_J \leq 100^{\circ}\text{C}$

for industrial applications (40°C ambient temperature θ_A , G_B as per Table 2.3). For $\theta_A > 40^{\circ}\text{C}$, a further reduction of S is necessary, in general, linearly up to the limit temperature, as shown in Fig. 2.3. Too low values of S ($S < 0.1$) can also cause problems. $S = 0.1$ can be used in many cases to calculate the failure rate in a standby or dormant state. As rule of thumb, $0.1 \lesssim S \lesssim 0.5$ is a good choice for reliability.

5.1.2 Cooling

As a general rule, the junction temperature θ_J of semiconductor devices should be kept as near as possible to the ambient temperature θ_A of the equipment or system

in which they are used; if not possible,

$\theta_J \leq 100^\circ\text{C}$ is recommended for a reliable design.

In a steady-state situation, i.e. with constant power dissipation P , the following relationships

$$\theta_J = \theta_A + R_{JA} P \quad (5.1)$$

or

$$\theta_J = \theta_A + (R_{JC} + R_{CS} + R_{SA})P \quad (5.2)$$

can be established and used to define the allowed thermal resistance

$$\begin{array}{ll} R_{JA} & \text{for junction – ambient} \\ R_{CS} & \text{for case – surface} \end{array} \quad \begin{array}{ll} R_{JC} & \text{for junction – case} \\ R_{SA} & \text{for surface – ambient,} \end{array}$$

where *surface* is used for *heat sink*.

Example 5.1

Determine the thermal resistance R_{SA} of a heat sink by assuming $P = 400\text{ mW}$, $\theta_J = 70^\circ\text{C}$, $\theta_A = 40^\circ\text{C}$, and $R_{JC} + R_{CS} = 35^\circ\text{C/W}$.

Solution

From Eq. (5.2) it follows that

$$R_{SA} = \frac{\theta_J - \theta_A}{P} - R_{JC} - R_{CS} \quad \text{and thus} \quad R_{SA} = \frac{30^\circ\text{C}}{0.4\text{ W}} - 35^\circ\text{C/W} = 40^\circ\text{C/W}.$$

For many practical applications, thermal resistance can be assumed to be independent of the temperature. However, R_{JC} generally depends on the *package* used (lead frame, packaging form and type), R_{CS} varies with the kind and thickness of *thermal compound* between the device package and the heat sink (or device support), and R_{SA} is a function of the heat-sink dimensions and form as well as of the type of cooling used (free convection, forced air, liquid-cooled plate, etc.). Indicative *thermal resistance values* R_{JC} and R_{JA} for free convection in ambient air without heat sinks are given in Table 5.2. The values of Table 5.2 are *indicative* and have to be replaced with specific values for exact calculations.

Cooling problems should not only be considered locally at the component level, but be integrated into a *thermal design concept* (thermal management). In defining the layout of an assembly, care must be taken in placing high power dissipation parts *away* from temperature sensitive components like wet Al capacitors and optoelectronic devices (the *useful life* is reduced by a factor of 2 for a $10\text{--}20^\circ\text{C}$ increase of the ambient temperature). In placing the assemblies in a rack, the cooling flow should be directed from the parts with low toward those with high power dissipation.

Table 5.2 *Indicative thermal resistance values for semiconductor component packages*

Package form	Package type	R_{JC} [$^{\circ}\text{C}/\text{W}$]	R_{JA} [$^{\circ}\text{C}/\text{W}$]**
DIL	Plastic	10 - 40	30 - 100
DIL	Ceramic/Cerdip	7 - 20	30 - 100
PGA	Ceramic	6 - 10*	20 - 40*
SOL, SOM, SOP	Plastic (SMT)	20 - 60*	70 - 240*
PLCC	Plastic	10 - 20*	30 - 70*
QFP	Plastic	15 - 25*	30 - 80*
TO	Plastic	2 - 20	60 - 300
TO	Metal	2 - 5	—

JC = junction to case; JA = junction to ambient; *lower values for > 64 pins;

**free convection at 0.15 m/s (factor 1.5 – 2 lower for forced cooling at 4 m/s)

5.1.3 Moisture

For electronic components in non hermetic packages, *moisture* can cause *drift* and activate various failure mechanisms such as *corrosion* and *electrolysis* (see pp. 98-100 for considerations on ICs). Critical in these cases is not the water itself, but the impurities and gases dissolved in it. If high relative humidity can occur, care must be taken to avoid the formation of galvanic couples as well as condensation or ice formation on the component packages or on conductive parts.

As stated in Section 3.1.3, the *use of ICs in plastic packages* can be allowed if one of the following conditions is satisfied:

1. Continuous operation, relative humidity < 70%, noncorrosive or marginally corrosive environment, junction temperature $\leq 100^{\circ}\text{C}$, and equipment useful life less than 10 years.
2. Intermittent operation, relative humidity < 60%, noncorrosive environment, no moisture condensation on the package, junction temperature $\leq 100^{\circ}\text{C}$, and equipment useful life less than 10 years.

For ICs with silicon nitride *passivation*, intermittent operation holds also for Point 1.

Drying materials should be avoided, in particular if chlorine compounds are present. *Conformal coating* on the basis of acrylic, polyurethane, epoxy, silicone or fluorocarbon resin 25 – 125 μm thick, filling with gel, or encapsulation in epoxy or similar resins are currently used (attention must be given to thermomechanical stresses at hardening). The use of *hermetic enclosures* for assemblies or equipment should be avoided if condensation cannot be excluded. Indicators for moisture are increasing leakage current or decreasing insulation resistance. In a corrosive environment, the contact of metals with different electrical affinity should be avoided.

5.1.4 Electromagnetic Compatibility, ESD Protection

Electromagnetic compatibility (EMC) is the ability of the item to function properly in its intended electromagnetic environment without introducing unacceptable electromagnetic noise (disturbances) into that environment. EMC has thus two aspects, *susceptibility* and *emission*. Agreed susceptibility and emission levels are given in international standards (IEC 61000 [3.8]). *Electrostatic discharge* (ESD) protection is a part of an *electromagnetic immunity concept*, mandatory for semiconductor devices (p. 94). Causes for EMC problems in electronic equipment and systems are, in particular,

- switching and transient phenomena,
- electrostatic discharges,
- stationary electromagnetic fields.

Coupling can be

- conductive (galvanic),
- through common impedance,
- by radiated electromagnetic fields.

In the context of ESD or EMC, disturbances often appears as electrical pulses with rise times t_r in the range 0.1 to 10kV / ns, peak values of 0.1 to 10kV, and energies of 0.1 to 10^3 mJ (high values for equipment). EMC aspects, in particular ESD *protection*, have to be considered early in the design and development of equipment and systems. The following *design guidelines* can help to avoid problems:

1. For high speed logic circuits ($f > 50$ MHz) use a whole *plane* (layer of a *multilayer*), or at least a tight grid for ground and power supply, to minimize inductance and to ensure a distributed decoupling capacitance (4 layers as signal / V_{CC} / ground / signal or better 6 layers as shield / signal / V_{CC} / ground / signal / shield are recommended).
2. For low frequency digital circuits, analog circuits, and power circuits use a *single-point ground* concept, and wire all different grounds separately to a *common ground point* at system level (across antiparallel suppressor diodes).
3. Use *low inductance decoupling capacitors* (generally 10nF ceramic capacitors, placed where spikes may occur, i.e., at every IC for fast logic and bus drivers, every 4 ICs for HCMOS) and a 1 μ F metallized paper (or a 10 μ F electrolytic) capacitor per board; in the case of a highly pulsed load, locate the voltage regulator on the same board as the logic circuits.
4. Avoid logic which is *faster* than necessary and ICs with widely *different rise times*; adhere to required rise times and use Schmitt-trigger inputs if necessary.

5. Pay attention to *dynamic stresses* (in particular of *breakdown voltages* on semiconductor devices) as well as of *switching phenomena* on inductors or capacitors; implement noise reduction measures near the noise source (preferably with *Zener diodes* or *suppressor diodes*).
6. *Match* signal lines whose length is greater than $v \cdot t_r$, also when using differential transmission (often possible with a series resistor at the source or a parallel resistor at the sink, v = signal propagation speed $\approx c / \sqrt{\epsilon_r \mu_r}$); for HCMOS also use a 1 to 2 k Ω pull-up resistor and a pull-down resistor equal to the line impedance Z_0 , in series with a capacitor of about 200 pF per meter of line.
7. Capture *induced noise* at the beginning and at the end of long signal lines using *parallel suppressors* (suppressor diodes), series protectors (ferrite beads) or series/parallel networks (RC), in that order, taking into account the required rise and fall times.
8. Use *twisted pairs* for signal and return lines (one twist per centimeter); ground the *return line at one end* and the *shield at both ends* for *magnetic shielding* (at more points to shield against *electric fields*); provide a closed (360°) contact with the shield for the ground line; clock leads should have adjacent ground returns; for clock signals leaving a board consider the use of fiber optics, coax, trileads, or twisted pairs in that order.
9. Avoid *apertures in shielded enclosures* (many small holes disturb less than a single aperture having the same area); use *magnetic material* to shield against low-frequency *magnetic fields* and materials with good *surface conductivity* against *electric fields*, plane waves, and high frequency magnetic fields (above 10 MHz, *absorption loss* predominates and shield thickness is determined more for its mechanical rather than for its electrical characteristics); *filter or trap all cables* entering or leaving a shielded enclosure (filters and cable shields should make very low inductance contacts to the enclosure); RF parts of analog or mixed signal equipment should be appropriately shielded (air core inductors have greater emission but less reception capability than magnetic core inductors); all signal lines entering or leaving a circuit should be investigated for common mode emission; minimize *common mode currents*.
10. Implement *ESD current-flow paths* with *multipoint grounds* at least for plug-in populated printed circuit boards (PCBs), e. g. with guard rings, *ESD networks*, or suppressor diodes, making sure in particular that all signal lines entering or leaving a PCB are sufficiently *ESD* protected (360° contact with the shield if shielded cables are used, latched and strobed inputs, etc.); ground to *chassis ground* all exposed metal, if necessary use secondary shields between sensitive parts and chassis; design *keyboards, consoles, and other operating parts* to be immune to *ESD*.

5.1.5 Components and Assemblies

5.1.5.1 Component Selection

1. Pay attention to *all* specification limits given by the manufacturer and company-specific rules, in particular dynamic parameters and breakdown limits.
2. Limit the number of entries in the *list of preferred parts* (QPL) and, wherever possible, ensure a *second source* procurement; if *obsolescence* problems are possible (very long warranty or operation time), observe this aspect in the QPL and/or in the design / layout of the equipment or system considered.
3. Use *non-qualified* parts and components only after checking the *technology and reliability risks* involved (the *learning phase* at the manufacturer's plant can take more than 6 months); in the case of critical applications, intensify the *feedback* to the manufacturer and plan appropriate *incoming inspections*.

5.1.5.2 Component Use

1. Tie *unused logic inputs* to the power supply or to the ground, usually through *pull-up / pull-down resistors* (100k Ω for CMOS), also to improve testability; pull-up / pull-down resistors are also recommended for inputs driven by three-state outputs; respect fan-out capabilities; unused outputs are generally open, but a default value must be assigned to unselected lines (e.g. bus).
2. Protect all *CMOS terminals* from or to a *connector* with a 100k Ω *pull-up / pull-down resistor* and a 1 to 10k Ω *series resistor* (latch-up) for an *input*, or an appropriate *series resistor* for an *output* (add diodes if V_{in} and V_{out} cannot be limited between $-0.3V$ and $V_{DD} + 0.3V$); observe *power-up* and *power-down sequences*, make sure that the ground and power supply are *applied before* and *disconnected after* the signals.
3. Analyze the *thermal stress* (internal operating temperature) of each part and component carefully, placing dissipating devices away from temperature-sensitive ones, and adequately cooling components with high power dissipation (failure rates double generally for a temperature increase of 10–20°C); for semiconductor devices, design for a *junction temperature* $\theta_J \leq 100^\circ\text{C}$ (if possible keep $\theta_J \leq 80^\circ\text{C}$).
4. Pay attention to *transients*, especially in connection with *breakdown voltages* of transistors ($V_{BEO} \leq 5V$; stress factor $S < 0.5$ for V_{CE} , V_{GS} , and V_{DS}).
5. Derate *power devices* more than signal devices (stress factor $S < 0.4$ if more than 10^5 power cycles occur during the useful life).
6. Avoid *special diodes* (tunnel, step-recovery, pin, varactor, which are 2 to 20 times less reliable than normal Si diodes); *Zener diodes* are about one half as reliable as Si switching diodes, their stress factor should be > 0.1 .

7. Allow a $\pm 30\%$ drift of the coupling factor for *optocoupler* during operation; regard optocouplers and *LEDs* as having a limited useful life (generally $> 10^6$ h for $\theta_J < 40^\circ\text{C}$ and $< 10^5$ h for $\theta_J > 80^\circ\text{C}$), design for $\theta_J \leq 70^\circ\text{C}$ (if possible keep $\theta_J < 40^\circ\text{C}$); pay attention to optocoupler voltage ($S \leq 0.3$).
8. Observe operating temperature, voltage stress (DC and AC), and technological suitability of *capacitors* for a given application: *Foil capacitors* have a reduced impulse handling capability; *wet Al capacitors* have a limited useful life (which halves for every 10°C increase in temperature), a large series inductance, and a moderately high series resistance; for *solid Ta capacitors* the AC impedance of the circuitry as viewed from the capacitor terminals should not be too small (the failure rate is an order of magnitude higher with $0.1\Omega/V$ than with $2\Omega/V$, although new types are less sensitive); use a $10 - 100\text{nF}$ *ceramic capacitor* parallel to each electrolytic capacitor; avoid electrolytic capacitors $< 1\mu\text{F}$.
9. Cover *EPROM windows* with metallized foils, also when stored.
10. Avoid the use of *variable resistors* in final designs (50 to 100 times less reliable than fixed resistors); for *power resistors*, check the internal operating temperature as well as the voltage stress.

5.1.5.3 PCB and Assembly Design (see also Section 5.2)

1. Design all *power supplies* to handle *permanent short* circuits and monitor for under/ over voltage (protection diode across the voltage regulator to avoid $V_{out} > V_{in}$ at power shutdown); use a 10 to 100nF *decoupling ceramic capacitor* parallel to each electrolyte capacitor.
2. Clearly define, and implement, *interfaces* between *different logic families*.
3. Establish *timing diagrams* using *worst-case conditions*, also taking the effects of *glitches* into consideration.
4. Pay attention to *inductive and capacitive coupling* in parallel signal leads ($0.5 - 1\mu\text{H/m}$, $50 - 100\text{pF/m}$); place signal leads *near to ground returns* and away from power supply leads, in particular for *clocks*; for high-speed circuitries, investigate the necessity for *wave matching* (parallel resistor at sink, series at source); introduce *guard rings* or *ground tracks* to limit coupling.
5. Place all *input / output drivers* close together, near the connectors, but away from clock circuitry and power supply lines (inputs latched and strobed).
6. Observe the *power-up and power-down sequences*, especially in the case of different power supplies (no signals applied to unpowered devices).
7. Protect PCBs against damage through *insertion or removal under power*.
8. For critical redundancies, verify carefully failure modes and possible protections; avoid to use the same power supply and to put all on the same PCB.

9. For PCBs employing *surface mount technology* (SMT), make sure that the component spacing is not smaller than 0.5 mm and that the lead width and spacing are not smaller than 0.25 mm; test pads and solder-stop pads should be provided; for large leadless ceramic ICs, use an appropriate lead frame (problems in SMT arise with soldering, heat removal, mismatch of expansion coefficients, pitch dimensions, pin alignment, cleaning, and contamination); pitch < 0.3 mm can give production problems.
10. Assure appropriate labeling of each hardware part, homogeneous orientation of ICs, and enough spacing between components for clips or test probes; as a general rule, *testability* of PCBs and assemblies should be considered early in the design of the layout (number and dimension of test points, pull-up/ pull-down resistors, activation/ deactivation of three-state outputs, see also Section 5.2); manually extend the capability of CAD tools, if necessary.
11. Make sure that the *mechanical fixing* of power devices is appropriate, in particular of those with high power dissipation; avoid having current carrying contacts under thermomechanical stress.
12. Avoid the need for special manufacturing processes (i.e. of processes which quality can't be tested directly on the product, have high requirements with respect to reproducibility, or can have an important negative effect on the product quality or reliability).

5.1.5.4 PCB and Assembly Manufacturing

1. *Ground* with 1M Ω resistors tools and personnel for *assembling, soldering, and testing*; avoid touching active parts of components during assembling; use soldering irons with transformers and grounded tips.
2. When using *automatic placing machines*, verify that for inserted devices only the parts of pins free from insulation goes into the soldering holes and IC pins are not bent into the soldering holes (Fig. 3.10). For *surface mount devices* (SMD), make sure that the correct quantity of solder material is deposited, and that the stand-off height between the component body and the printed circuit surface is not less than 0.25 mm (pitch < 0.3 mm can give production problems); see also Section 3.4 for further aspects.
3. For *lead-free solder* (as per EU Directive 2002/95/EC), a major problem is the higher eutectic temperature (217°C for Sn-Ag-Cu, 226°C for Sn-Ag-Cu-Sb, against 183°C for Sn-Pb), yielding peak solder temperatures up to 270°C (245°C for Sn-Pb); careful attention to rules 4-8 is asked (it seems reasonable, at present, to agree that for standard industrial applications (p. 35) with low thermal gradient ($\leq 5^\circ\text{C}/\text{min}$) no new important reliability problems arise with lead-free solder (see also Sections 3.4 & 8.3 and, e.g., [3.79, 3.90] as well as IPC-STDs for greater details); however, more *defects/damages* (barrel & foil cracking, voiding, bridging, etc.) are possible.

4. Control the *soldering temperature profile*; choose the best compromise between soldering time and soldering temperature (for Sn-Ag-Cu about 3 s at 260°C for *wave* and 60 s at 235°C for *reflow*), as well as an appropriate *preheating* (about 60 s to reach 150°C); check the solder bath periodically.
5. For *surface mount technology* (SMT) give preference to *IR reflow soldering* and provide good *solder-stop pads* (vapor-phase can be preferred for substrates with metal core or PCBs with high component density); avoid having inserted and surface mounted devices (SMD) on the same (two-sided) PCB (thermal shock on the SMD with consequent crack formation and possible ingress of flux to the active part of the component, in particular for ceramic capacitors greater than 100 nF and large plastic ICs).
6. For high reliability application pay attention to *mitigate whisker growth*, e. g. prefer satin Sn layers and avoid the use of hot air solder leveling (HASL).
7. For high reliability applications, *wash* PCBs and assemblies after soldering (deionized water ($< 5\mu\text{S}/\text{cm}$), in any case with halogen-free liquids); check periodically the *washing liquid* for contamination; use ultrasonic cleaning only when resonance problems in components are excluded.
8. Avoid having more than *one heating* process that reaches the soldering temperature, and hence any kind of *rework*; for temperature sensitive devices, consider the possibility of protection during soldering (e. g. cooling ring).
9. Avoid soldering *gold-plated pins*; if not possible, tin-plate the pins in order to reduce Au concentration to $< 4\%$ in the solder joint (intermetallic layers) and $< 0.5\%$ in the solder bath (contamination), $0.2\mu\text{m} < \text{Au thickness} < 0.5\mu\text{m}$.
10. Avoid any kind of *electrical overstress* when testing components, PCBs or assemblies; avoid removal and insertion under power.

5.1.5.5 Storage and Transportation

1. Keep *storage temperature* between 10 and 30°C, *relative humidity* between 40 and 60%; avoid dust, corrosive atmospheres, and mechanical stresses; use *hermetically sealed containers* only for high-humidity environments.
2. Limit the storage time by implementing *first-in / first-out* rules (storage time should be no longer than two years, just-in-time shipping is often only possible for a stable production line).
3. Ensure *antistatic storage and transportation* of all ESD sensitive electronic components; use metallized, unplasticized bags, avoid PVC for bags.
4. Transport PCBs & assemblies in *antistatic containers* with connectors shorted.

5.1.6 Particular Guidelines for IC Design and Manufacturing

1. Reduce *latch-up sensitivity* by increasing critical distances, changing local doping, or introducing vertical thick-oxide isolation.

2. Avoid significant *voltage drops* along resistive leads (poly-Si) by increasing line conductivity and/or dimensions or by using *multilayer metallizations*.
3. Give sufficient size to the *contact windows* and avoid large contact depth and thus sharp edges (slopes); ensure material compatibility, in particular with respect to metallization layers.
4. Take into account *chemical compatibility* between materials and tools used in sequential processes; limit the use of *planarization processes* to uncritical metallization line distances; employ preferably *stable processes* (low-risk processes) which allow a reasonable parameter deviation; control carefully the *wafer raw material* (CZ/FZ material, crystal orientation, O₂ conc., etc.).

5.2 Design Guidelines for Maintainability

Maintainability, even more than reliability, *must be built into complex equipment and systems*. This has generally to be performed project specific with a *maintenance concept*. However, a certain number of *design guidelines for maintainability* apply quite generally. These will be discussed in this section for the case of complex electronic equipment and systems with high maintainability requirements (see e. g. also [1.22, 5.0, 5.14, 5.28, 6.82] for military applications).

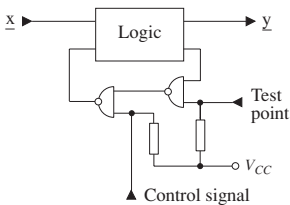
5.2.1 General Guidelines

1. *Partition* the equipment or system into *line replaceable units* (LRUs), often PCBs for electronic systems, and apply techniques of *modular construction*, starting from the functional structure; make modules *functionally independent* and *electrically as well as mechanically separable*; develop easily identifiable and replaceable LRUs which can be tested with commonly available test equipment.
2. Plan and implement a concept for automatic *faults* (failures and defects) *detection* and automatic or semiautomatic *faults localization* (isolation and diagnosis) down to the *line replaceable unit* (LRU) level, including *hidden faults* (failures & defects) and *software defects* as far as possible.
3. Aim for the greatest possible *standardization* of parts, tools, and testing equipment; keep the need for external testing facilities to a minimum.
4. Consider *environmental conditions* (thermal, climatic, mechanical) in field operation as well as during transportation and storage (see Section 5.2.5 for human, ergonomic and safety aspects).
5. Plan and realize an appropriate logistic support including user documentation, training of operating & maintenance personnel, and logistic support in field.

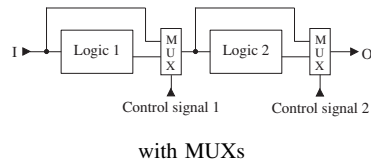
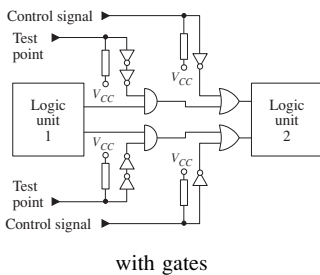
5.2.2 Testability (see also Section 5.1.5.3)

Testability includes the degrees of faults (failure and defects) *detection* and *localization*, the correctness of test results, and test duration (Section 4.2.1). High testability can be achieved by improving *observability* (the possibility to check internal signals at the outputs) and *controllability* (the possibility to modify internal signals from the inputs).

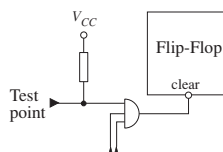
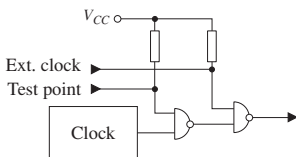
1. Avoid *asynchronous logic* (asynchronous signals should be latched and strobed at the inputs); use only one master clock.
2. Avoid WIRED-ORs and simplify *logical expressions* as far as possible.
3. Improve testability of connection paths and simple circuitry using ICs with *boundary-scan* (IEEE STD 1149 [4.13]).
4. Separate *analog and digital circuit* paths, as well as circuitries with different supply voltages; make power supplies mechanically separable.
5. Make *feedback paths* separable



6. Realize *modules* as self-contained as possible, with small sequential depth, el. separable and individually testable, in particular where redundancy appears; for mechanically separable modules, assure easy removal and mech. keying.



7. Allow for *external initialization* of sequential logic



8. Fix *acceptable limits* for all measurable parameters; identify all only indirectly measurable parameters and define appropriate measurement (test) procedures.
9. Introduce *built-in test* (BIT) and corresponding BITE, as necessary to reach the required coverage level, in particular for critical functions and to satisfy operation monitoring (Table 4.1), i.e. implement *built-in self-test* (BIST); however, minimize the amount of data to be recorded for monitoring purposes.
10. Design BIT/BITE considering worst-case operating conditions, and so that their failure *does not influence system's operation* (FMEA); for critical functions, introduce redundancy also for BIT/BITE.
11. Implement means to identify whether hardware or software has caused a failure message, wherever possible.
12. Introduce *test modi* also for the detection of *hidden faults* (e. g. failures or defects in redundant elements); if not possible, give appropriate test procedures in the user documentation.
13. Provide manual test sequences to support testability, and describe them clearly in the user documentation.
14. Rely to a connector critical nodes of LRUs (to avoid internal probing access) and locate I/O test points close to each other, wherever possible.
15. Provide enough *test points* (at a minimum on functional-unit inputs and outputs, as well as on bus lines) and support them with pull-up/pull-down resistors (Point 2 on p.150, Point 10 on p.152); provide access for a probe, taking into account the capacitive and/or resistive load, reflections, and possible problems related to buffers; document all test points in the user documentation.
16. Make use of a *scan path* to reduce test time, wherever possible; the basic idea of a scan path is shown on the right-hand side of Fig. 5.1, the test procedure is:
 1. Activate the MUX control signal (connect Z to B).
 2. Scan-in with n clock pulses an appropriate n -bit test pattern, this pattern appears in parallel at the FF outputs and can be read serially with $n - 1$ additional clock pulses (repeat this step to completely test MUXs & FFs).
 3. Scan-in with n clock pulses a first test pattern for the combinatorial logic (feedback part) and apply an appropriate pattern also to the input \underline{x} (both patterns are applied to the combinatorial circuit and generate corresponding results which appear at the output \underline{y} and at the inputs A of the MUXs).
 4. Verify the results at the output \underline{y} .
 5. Deactivate the MUX control signal (connect Z to A).
 6. Give one clock pulse (feedback results appear parallel at the FF outputs).
 7. Activate the MUX control signal (connect Z to B).
 8. Scan-out with $n - 1$ clock pulses and verify the results, at the same time a second test pattern for the combinatorial circuit can be scanned-in.
 9. Repeat steps 3 – 8 up to a satisfactory test of the combinatorial part of the circuit (see e. g. [4.17, 4.31] for special test algorithms).

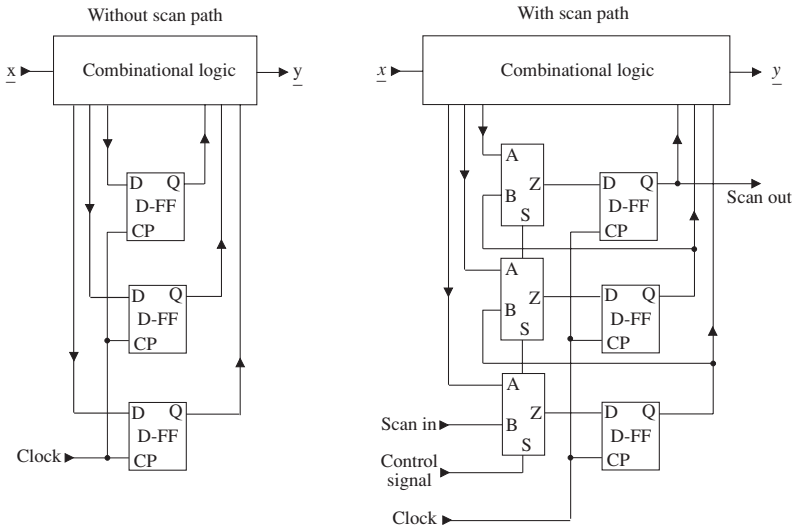


Figure 5.1 Basic structure of a synchronous sequential circuit, without (left) and with (right) a scan path ($n = 3$)

5.2.3 Connections, Accessibility, Exchangeability

1. Use preferably *indirect plug connectors*; distribute power supply and ground over several contacts (20%, far from signal leads); standardize pin assignment; plan to have *reserve contacts* (e. g. for test stimuli); avoid any external mechanical stress on connectors; define only one kind of extender for PCBs and plan its use; use fiber-optic connections for critical applications.
2. Standardize connectors and wires color as far as possible.
3. For not soldered or screwed connections, give preference to wire wrap.
4. Route wires and cables connections as clearly as possible, avoiding unnecessary overlapping and mechanical strains.
5. Provide *self-latching* access flaps of sufficient size.
6. Avoid the use of more than 4 fasteners to fix case or covers and the need for *special tools*; use clamp fastening with torque-set.
7. Assure *accessibility* to LRUs by considering the frequency of maintenance tasks, and make them accessible without removal of other LRUs.
8. Provide for *speedy replaceability* by means of plug-out/plug-in techniques.
9. Prevent *faulty installation or connection* of (not interchangeable) LRUs through mechanical keying.
10. Provide good access to degrading parts (also for cleaning & lubrication).
11. Locate LRU's identification and modification plates so as to be easily readable.

5.2.4 Adjustment

1. Limit any form of *hardware adjustment* (or alignment) in the field.
2. If an adjustment becomes unavoidable, describe the procedure carefully in the user documentation, make the adjustment easily accessible, and avoid sensitive adjustments.

5.2.5 Human, Ergonomic, and Safety Aspects

Human and ergonomic factors can have a great influence on the reliability, maintainability, availability, and safety of complex equipment and systems. Experience shows that safety critical failures at system level are often caused by human errors related to design, manufacturing, installation (incl. handling & transportation), operation, or maintenance.

Errare humanum est should always be considered by a designer. Thus, because of the difficulties in modeling human's behavior in emergency situations, *prevention must be preferred to modeling* and, as for software quality, extensive requirements and design rules become important (see e.g. [5.14, 6.82] for military applications). The following are basic design rules useful to avoid human errors during development, manufacturing, installation, and use of complex equipment and systems with high reliability and/or safety requirements, or at least to limit their effects (see pp. 10, 294 - 298 for modeling and further considerations).

1. Clearly define which subfunctions (of the required function) will be performed by machine and which by human.
2. Analyze the tasks assigned to the human and partition them in appropriate subtasks, separating operation and maintenance tasks (analysis focuses on input information to human, evaluation process, action to be taken, environments & constraints, tools & job aids, skill required, feedback).
3. For safety critical decisions or subtasks, *bypass the human wherever possible*, e.g. using *majority redundancy* also for actuators (series for close, parallel for open) or, at least, introduce *two-step actions* (the first step being reversible).
4. Design *go/no-go* or *fail-safe circuitries* to warn from (or avoid) safety critical failures.
5. Make alarms (acoustic and/or visual), clear, different for each relevant malfunction, and so that they can be correctly interpreted by operators & maintainers, taking care of their reaction time (use preferably tones for status indications and speech for all other information); minimize the number of alarms.
6. Use visual presentation for information which are long, complex, or needed later.
7. Limit the use of color-coded information (if necessary, combine color information with appropriate acoustical signals).
8. Describe system status, detected fault, and action to be accomplished concisely in *full text* and make them easily readable.

9. Consider *ergonomic* as well as *man-machine aspects* to avoid mistakes at operation or maintenance; in particular, select carefully shape & placement of control knobs and the *layout of operating consoles*.
10. Adapt control and display elements to the *required skill* for operators and maintainers.
11. In displaying information, consider that the optimal visual field is 15 degrees up, down, left, and right (order information left to right and top to bottom).
12. *Simplify* as far as possible operation and maintenance.
13. Use high *standardization* in selecting operational and maintenance tools.
14. Make any labeling simple and clear.
15. Conceive operation and maintenance procedures *to be as simple as possible*, taking care also of the user's skill level; order all steps in a *logical sequence*; document, wherever possible, the steps by a visual feedback, and describe them clearly and concisely in the user documentation.
16. *Fix in the user documentation all assumptions* (requirements) regarding skill, training, motivation, and work conditions for operators and maintainers, as well as related organizational controls.

5.3 Design Guidelines for Software Quality

Software plays an increasingly role in equipment and systems, both in terms of technical relevance and of development cost (often higher than 70% even for small systems). Unlike hardware, software does not go through a *production phase*. Also, software cannot break or wear-out. However, it can *fail* to satisfy its required function because of *defects* which manifest themselves while the system is operating (*dynamic defects*). A *fault* in the software is thus caused by a *defect*, even if it appears *randomly* in time, and software problems are basically

quality problems which have to be solved with quality assurance tools (defect prevention, configuration management, testing, and quality data reporting system, as given in Section 1.3.3, see also Appendix A3.3.5).

This also because questions like "*what is a software failure?*" and "*do software reliability models serve their intended purpose?*" are still open, see e.g. [5.48, 5.78, 5.83].

For equipment and systems exhibiting high reliability or safety requirements, software should be conceived and developed to be *defect tolerant* (Table 5.4), i.e., to be able to continue operation despite the presence of software defects. For this purpose, *redundancy* considerations are necessary, in *time domain* (protocol with retransmission, cyclic redundancy check, assertions, exception handling, etc.), *space domain* (error correcting codes, parallel processes, etc.), or as a combination of both. Moreover, if the interaction between hardware and software in the realization of the

required function at the system level is large (embedded software), redundancy considerations should also be extended to cover hardware defects and *failures*, i.e., to make the system *fault tolerant* (Sections 2.3.7 and 6.8.3 - 6.8.8). In this context, effort should be devoted to the investigation of *causes-to-effects* aspects (FMEA/FMECA) of hardware and software *faults* from a *system level* point of view, including hardware, software, human factors, and logistic support as well.

This section introduces basic concepts and tools for *software quality assurance*, with particular emphasis on design guidelines and *preventive actions*. Because of their utility in *debugging* complex software packages, models for *software quality growth* are also discussed (Section 5.3.4). Greater details for *SQ assurance plans* can be found in [A2.8, 5.41 - 5.83], in particular [A2.8 (730), 5.54, 5.60, 5.70, 5.76].

A first difference between hardware and software appears in the *life-cycle phases* (Table 5.3). In contrast to Fig. 1.6, the production phase does not appear in the software life-cycle phases, since software can be copied without errors.

A second basic distinction between hardware and software is given by the *quality attributes* (Table 5.4). The definitions of Table 5.4 extend those in Appendix A1 and take care of established *standards* [A2.8, 5.60- 5.62]. Not all quality attributes of Table 5.4 can be *fulfilled* at the same time. In general,

a priority list of quality attributes must be established and consequently followed by all engineers involved in a project.

A further difficulty is the *quantitative evaluation* (assessment) of software quality attributes, i.e., the definition of *software quality metrics*. An attempt to aggregate (as user) some of the attributes in Table 5.4 is in [5.55], see also IEEE Std 1061 [5.61].

From the above considerations,

- (i) *software quality (SQ) can be defined as the degree to which a software package possesses a stated combination of quality attributes, and*
- (ii) *mandatory for software quality assurance is a partition of the software life-cycle into clearly defined phases, each of them closed with a comprehensive design review.*

If supported by an appropriate set of software quality metrics, this allows an *objective* assessment of the quality level achieved. However, since only a limited number of quality attributes can be reasonably well satisfied by a specific software package, the main purpose of software quality assurance is to *maximize the common part of the quality attributes needed, specified, and realized*. To reach this target, specific activities have to be performed during *all software life-cycle* phases. Many of these activities can be derived from hardware quality assurance tasks, in particular regarding *preventive actions* (defect prevention), *configuration management*, *testing*, and *corrective actions*, taking care that

auditing software quality assurance activities in a project must be more intensive and with a shorter feedback than for hardware (Fig.5.2,Tab.5.5).

Table 5.3 *Software life-cycle phases* (see Fig. 1.6 on p. 19 for *hardware life-cycle phases*)

Phase	Objective / Tasks	Input	Output
Concept	<ul style="list-style-type: none"> • Problem definition • Feasibility check 	<ul style="list-style-type: none"> • Problem description • Constraints on computer size, programming languages, I/O, etc. 	<ul style="list-style-type: none"> • System specifications for functional (what) and performance (how) aspects • Proposal for the definition phase
Definition	<ul style="list-style-type: none"> • Investigation of alternative solutions • Interface definitions 	<ul style="list-style-type: none"> • Feasibility check • System specifications • Proposal for the definition phase 	<ul style="list-style-type: none"> • Revised system specifications • Interface specifications • Updated estimation of cost and schedule • Feedback from users • Proposal for the design, coding, and testing phase
Design, Coding, Testing	<ul style="list-style-type: none"> • Setup of detailed specifications • Software design • Coding • Test of each module • Verification of compliance with module specifications (design reviews) • Data acquisition 	<ul style="list-style-type: none"> • Feasibility check • Revised system specifications • Interface specifications • Proposal for the design, coding, and testing phase 	<ul style="list-style-type: none"> • Definitive flowcharts, data flow diagrams, and data analysis diagrams • Test procedures • Completed and tested software modules • Tested I/O facilities • Proposal for the integration, validation, and installation phase • Software documentation
Integration, Validation, Installation	<ul style="list-style-type: none"> • Integration and validation of the software • Verification of compliance with system specifications (design reviews) • Setup of the definitive documentation 	<ul style="list-style-type: none"> • Feasibility check • Completed and tested software modules • Tested I/O facilities • Proposal for the integration, validation, and installation phase 	<ul style="list-style-type: none"> • Completed and tested software • Complete and definitive documentation
Operation, Maintenance	<ul style="list-style-type: none"> • Use/application of the software • Maintenance (corrective and perfective) 	<ul style="list-style-type: none"> • Completed and tested software • Complete and definitive documentation 	

With the design and development of complex equipment & systems, the separation between hardware and software quality assurance should be scaled down, *taking from each side the "good part" of methods and tools and putting them together for new "better" methods and tools* (strategy of wide applicability, see Appendix A3.3).

Table 5.4 Important *software quality attributes* and characteristics

Attribute	Definition
Compatibility	Degree to which two or more software modules or packages can perform their required functions while sharing the same hardware or software environment
Completeness	Degree to which a software module or package possesses the functions necessary and sufficient to satisfy user needs
Consistency	Degree of uniformity, standardization, and freedom from contradiction within the documentation or parts of a software package
Defect Freedom (Reliability)	Degree to which a software package can execute its required function without causing system failures
Defect Tolerance (Robustness)	Degree to which a software module or package can function correctly in the presence of invalid inputs or highly stressed environmental conditions
Documentation	Totality of documents necessary to describe, design, test, install, and maintain a software package
Efficiency	Degree to which a software module or package performs its required function with minimum consumption of resources (hardware and / or software)
Flexibility	Degree to which a software module or package can be modified for use in applications or environments other than those for which it was designed
Integrity	Degree to which a software package prevents unauthorized access to or modification of computer programs or data
Maintainability	Degree to which a software module or package can be easily modified to correct faults, improve the performance, or other attributes
Portability	Degree to which a software package can be transferred from one hardware or software environment to another
Reusability	Degree to which a software module can be used in another program
Simplicity	Degree to which a software module or package has been conceived and implemented in a straightforward and easily understandable way
Testability	Degree to which a software module or package facilitates the establishment of test criteria and the performance of tests to determine whether those criteria have been met
Usability	Degree to which a user can learn to operate, prepare inputs for, and interpret outputs of a software package

see also [A1.5]; *software module* is used here also for *software element*

5.3.1 Guidelines for Software Defect Prevention

Defects can be introduced in different ways and at different points along the life cycle phases of software. The following are some *causes for defects*:

1. During the concept and definition phase
 - misunderstandings in the problem definition, (the final user itself may have an incomplete vision of what is truly desired),

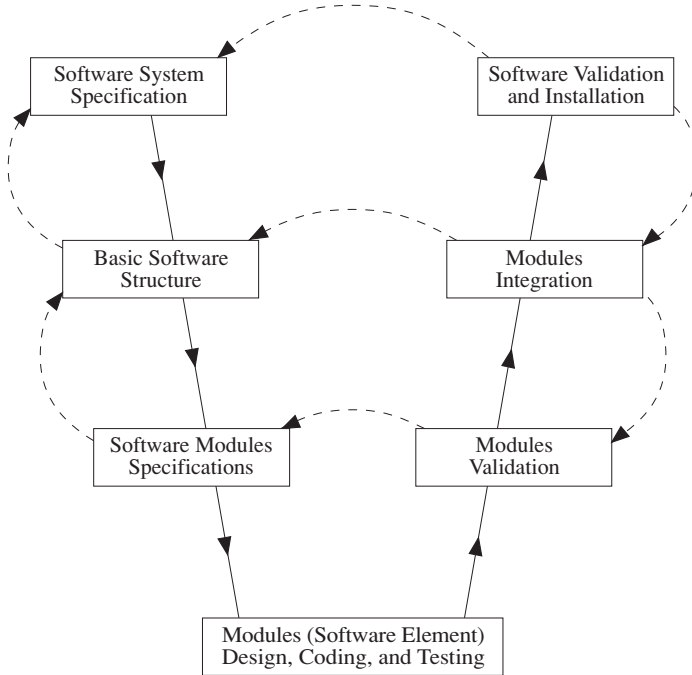


Figure 5.2 Procedure for *software development* (top-down design and bottom-up integration with vertical and horizontal control loops)

- constraints on CPU performance, memory size, computing time, I/O facilities or others,
 - inaccurate *interface specifications*,
 - too little attention to user needs and/or skills.
2. During the design, coding, and testing phase
 - inaccuracies in *detailed specifications*,
 - misinterpretation of detailed specifications,
 - inconsistencies in procedures or algorithms,
 - timing problems,
 - data conversion errors,
 - complex software structuring or large dependence between software modules.
 3. During the integration, validation, and installation phase
 - too large *interaction between software modules*,
 - errors during software corrections or modifications,
 - unclear or incomplete documentation,
 - changes in the hardware or software environment,
 - exceeding important resources (dynamic memory, disk, etc.).

Defects are thus generally caused by *human errors* (software developer or user). Their detection and removal become more expensive as the software life cycle progresses (often by a factor of 10 between each of the four main phases of Table 5.3, as in Fig. 8.2 for hardware). Considering that many defects can remain undiscovered for a long time after the software installation (since detected only by particular combinations of data and system states), the necessity for *defect prevention* through an appropriate *software quality assurance* becomes mandatory. Following *design guidelines* can be useful:

1. Fix *written procedures/rules* and follow them during software development, such rules specify quality attributes, with *project specific priority*, and corresponding quality assurance procedures.
2. Formulate *detailed specifications and interfaces* as carefully as possible, such specifications/interfaces should exist before coding begins.
3. Give priority to *object oriented programming*.
4. Use well-behaved *high-level programming languages*, assembler only when a problem cannot be solved in other way; use established CASE tools for program development and testing (see e.g. IEEE Std 14102-2010 [5.61]).
5. Partition software into *independent software modules* (modules should be individually testable, developed *top-down*, and integrated *bottom-up* (Fig.5.2)).
6. Take into account all constraints given by *I/O facilities*.
7. Develop software able to *protect itself* and its data; plan for automatic testing and validation of data.
8. Consider aspects of *testing / testability* as *early* as possible in the development phase; increase testability through the use of definition languages (Vienna, RTRL, PSL, IORL).
9. Improve *understandability* and readability of software by introducing appropriate *comments*.
- 10 Document software carefully and carry out sufficient *configuration management*, in particular with respect to *design reviews* (Table 5.5).

Software for on-line systems (embedded software) should further be conceived to be, as far as possible, *tolerant on hardware failures* and to allow a *system re-configuration*, particularly in the context of a *fail-safe concept* (hardware and software involved in fail-safe procedures should be periodically checked during the operation phase). For this purpose, *redundancy* considerations are necessary,

- in the *time domain* (protocol with retransmission, cyclic redundancy check, assertions, exception handling, etc.),
- in the *space domain* (error correcting codes, NVP, NVS, NSCP (N-self configuring programming) or parallel processing, used in a *majority redundancy*, etc.),

or in a combination of them. Moreover, if the interaction between hardware and software in the realization of the required function at the system level is large,

Table 5.5 *Software design reviews (IEEE Std 1028-1988 [A2.8])*

	Type	Objective
Evaluation	Management Review	Provide recommendations for the following <ul style="list-style-type: none"> • activities progress, based on an evaluation of product development status • changing project direction or identifying the need for alternate planning • adequate allocation of resources through global control of the project
	Technical Review	Evaluate a specific software element and provide management with evidence that <ul style="list-style-type: none"> • the software element conforms to its specifications • the design (or maintenance) of the software element is being done according to plans, <i>Standards</i>, and guidelines applicable for the project • changes to the software element are properly implemented and affect only those system areas identified by change specifications
Verification	Software Inspection	Detect and identify software element defects, in particular <ul style="list-style-type: none"> • verify that every software element satisfies its specifications • verify that every software element conforms to applicable <i>Standards</i> • identify deviations from standards and specifications • evaluate software engineering data (e. g. defect and effort data)
	Walk-through	Find defects, omissions, and contradictions in the software elements and consider alternative implementations (long associated with code examination, this process is also applicable to other aspects, e.g. architectural design, detailed design, test plans / procedures, and change control procedures)

software element is used here also for *software module*; see also Tab. A3.3 for *system oriented* design reviews; *gate review* is often used instead of *design review*

redundancy considerations should be extended *to cover hardware defects & failures*, i. e., to make the system *fault tolerant* (Sections 2.3.7, 6.8). In this context, effort should be devoted to the investigation of *causes-to-effects* aspects (criticality) of hardware & software *faults* from a *system level* point of view, including hardware, software, human factors, logistic support (Sections 2.6,4.2,6.10,[1.7,2.87,2.88,5.75]).

5.3.2 Configuration Management

Configuration management is an important *quality assurance tool* during the design and development of complex equipment and systems, *both for hardware and software*. Applicable methods and procedures are outlined in Section 1.3.3 and discussed in Appendices A3 and A4 for hardware. Some of these methods have been introduced in *software standards* [A2.8 (828-2012)]. Of particular importance for software are *design reviews*, as given in Table 5.5 (see also Table A3.3 for hardware aspects), and *configuration control*, i. e. the management of changes and modifications.

5.3.3 Guidelines for Software Testing

Planning for *software testing* is generally a difficult task, as even small programs can have an extremely large number of states which makes a complete test impossible. A *test strategy* is then necessary. The problem is also known for hardware, for which special design guidelines to increase *testability* have been developed (Section 5.2). The most important rule, which applies to both hardware and software, is the

partitioning of the item (hardware or software) into independent modules which can be individually tested & integrated bottom-up to build the system.

Many rules can be project specific. The following *design guidelines* can be useful in establishing a test strategy for software used in complex equipment and systems:

1. Plan software tests *early* in the design and coding phases, and integrate them step by step into a *test strategy*.
2. Use appropriate *tools* (debugger, coverage-analyzer, test generators, etc.).
3. Perform tests first at the *module level*, exercising all instructions, branches and logic paths.
4. Integrate and test successively the modules *bottom-up* to the system level.
5. Test carefully all *suspected paths* (with potential defects) and software parts whose incorrect running could cause *major* system failures.
6. *Account for all defects* which have been discovered with indication of running time, software & hardware environments at the occurrence time (state, parameter set, hardware facilities, etc.), changes introduced, and *debugging* effort.
7. Test the complete software in its *final* hardware and software environment.

Testing is the only practical possibility to find (and eliminate) *defects*. It includes *debug tests* (generally performed early in the design phase using breakpoints, desk checking, dumps, inspections, reversible executions, single-step operation, or traces) and *run tests*. Although costly (often up to 50% of the software development cost), tests cannot guarantee *freedom from defects*. A balanced distribution of the efforts between *preventive actions* (defect prevention) and *testing* must thus be found for each project.

5.3.4 Software Quality Growth Models

Since the beginning of the seventies, a large number of models have been proposed to describe the occurrence of *software defects* during operation of complex equipment and systems. Such an occurrence can generate a *failure at system level* and appears often *randomly distributed* in time. For this reason, modeling has been done in a similar way as for hardware failures, i. e., by introducing the concept of *software failure rate*. Such an approach may be valid to investigate *software quality*

growth during software validation and installation, as for the reliability growth models developed in the sixties for hardware (Section 7.7). However,

from the considerations in Sections 5.3.1 - 5.3.3, the main target should be the development of software free from defects, and thus to focus effort on defect prevention rather than on defect modeling, see e.g. [5.78].

Because of their use in investigating software quality growth, this section introduces briefly some basic models known for software defect modeling (see Section 7.7 for further possible models, and p. 168 for some critical remarks):

1. Between consecutive occurrence points of a software defect, the "failure rate" is a function of the number of defects present in the software. This model leads to a death process and is known as Jelinski-Moranda model. If at $t = 0$ the software contains n defects, the probability $P_i(t) = \Pr\{i \text{ defects have been removed up to the time } t \mid n \text{ defects were present at } t = 0\}$ can be calculated recursively from (Problem A7.4 in Appendix A11)

$$P_0(t) = e^{-n\lambda t}, \quad P_i(t) = \int_0^t (n-i+1)\lambda e^{-(n-i)\lambda x} P_{i-1}(t-x) dx, \quad i = 1, \dots, n, \quad (5.3)$$

or directly as

$$P_i(t) = \binom{n}{i} (1 - e^{-\lambda t})^i e^{-(n-i)\lambda t}, \quad i = 1, \dots, n. \quad (5.4)$$

Figure 5.3 shows $P_0(t)$ to $P_3(t)$ for $n=10$. This model can be easily extended to cover the case in which the parameter λ also depends on the number of defects still present in the software.

2. Between consecutive occurrence points of a software defect, the "failure rate" is a function of the number of defects still present in the software and of the time elapsed since the last occurrence point of a defect. This model generalizes Model 1 above and can be investigated using semi-Markov processes (Appendix A7.6).

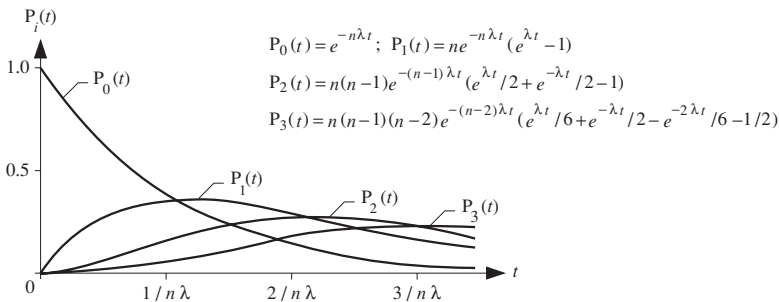


Figure 5.3 $P_i(t) = \Pr\{i \text{ defects have been removed up to the time } t \mid n \text{ defects were present at } t = 0\}$ for $i = 0 - 3$ and $n = 10$ (the time interval between consecutive occurrence points of a defect is exponentially distributed with parameter $\lambda_i = (n - i)\lambda$)

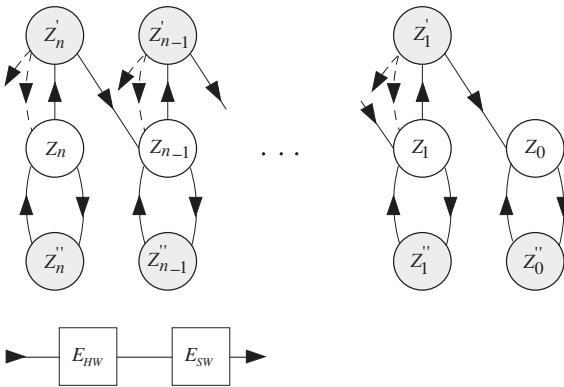


Figure 5.4 Simplified modeling for the time behavior of a system whose failure is caused by a hardware failure ($Z_i \rightarrow Z_i^{\cdot}$) or by the occurrence of a software defect ($Z_i \rightarrow Z_i^{\prime}$)

3. The *flow of occurrence* of software defects constitutes a *nonhomogeneous Poisson process* (Appendix A7.8.2). This model has been extensively investigated in the literature, together with reliability growth models for hardware, with different assumptions on the form of the process *intensity* (Section 7.7).
4. The *flow of occurrence* of software defects constitutes an arbitrary *point process*. This model is very general but difficult to investigate.

Models 1 and 2, above, may have a theoretical foundation. However, in practical applications they often suffer from the *lack of information*, for instance about the *number of defects actually present* in the software, and *data*. Also they do not take care of the *criticality* (effect at system level) of the defects still present in the software under consideration (several minor faults are in general less critical than just one major fault). The use of nonhomogeneous Poisson processes is discussed in Section 7.7, see e. g. also [6.1, A7.30] for some critical comments. *As a general rule,*

models based on the remaining number of defects in the software (errors at start), as well as oversimplified models, e. g. [5.80], should be avoided.

For systems with hardware and software, one can often assume that defects in the software will be detected and eliminated one after the other. Only hardware failures should remain. Figure 5.4 shows a possibility to take this into account [6.10]. However, interdependence between hardware and software can be greater as assumed in Fig. 5.4. Also is the number (n) of defects in the software at the time $t = 0$ unknown and by eliminating a software defect new defects can be introduced.

For all the above reasons, modeling software defects as well as systems with hardware and software is still in progress.

6 Reliability & Availability of Repairable Systems

Reliability and availability analysis of *repairable systems* is generally performed using stochastic processes, including *Markov*, *semi-Markov*, and *semi-regenerative processes*. A comprehensive introduction to these processes is in Appendix A7 with reliability applications in mind. Equations used for Markov and semi-Markov models are summarized in Table 6.2. This chapter investigates many of the reliability models useful for practical applications, some of which were developed for this book (Sections 6.8 & 6.10). Reliability figures at system level have indices S_i (e.g. $MTTF_{S_i}$), where S stands for system (the highest integration level of the item considered) and i is the state entered at $t=0$. After a discussion on assumptions & conclusions, Section 6.2 investigates the one-item structure under general conditions. Sections 6.3-6.6 deal with series, parallel, and series-parallel structures. To unify models and simplify calculations, it is assumed that the system has *only one repair crew* and *no further failures occur at system down*. Starting from *constant failure & repair rates* (Markov models), generalization is performed step by step (beginning with the repair rates) up to the case in which the process involved is *regenerative* with a minimum number of regeneration states. *Approximate expressions* for large series-parallel structures are investigated in Section 6.7. Section 6.8 considers systems with *complex structure* for which a reliability block diagram often *does not exist*. On the basis of *practical examples*, preventive maintenance, imperfect switching, incomplete coverage, elements with >2 states, phased-mission systems, common cause failures, and general reconfigurable fault tolerant systems with reward & frequency / duration aspects are investigated. Basic considerations on *network reliability* are given in Section 6.8.8 and a general procedure for complex structures is in Section 6.8.9. Section 6.9 introduces alternative investigation methods (dynamic FTA, BDD, event trees, Petri nets, computer-aided analysis), and gives a Monte Carlo approach useful for *rare events*. Human reliability is discussed in Section 6.10. Results are summarized in tables. *Asymptotic & steady-state* is used for *stationary*, *mean for expected value*, *independent for totally* (mutually, statistically, stochastically) *independent*. Selected examples illustrate the practical aspects.

6.1 Introduction, General Assumptions, Conclusions

Investigation of the *time behavior of repairable systems* spans a very large class of *stochastic processes*, from simple Poisson process through Markov and semi-Markov processes up to sophisticated regenerative processes with *only one or just a few regeneration states*. Nonregenerative processes are rarely considered because of mathematical difficulties. Important for the choice of the class of processes to be

used are the *distribution functions for the failure-free and repair times* involved. If failure and repair rates of all elements in the system are *constant* (time independent) *during the stay time in every state* (not necessarily at a state change, e.g. because of load sharing), the process involved is a time-homogeneous *Markov process* with a finite number of states, for which *stay time in every state* is *exponentially distributed*. The same holds if Erlang distributions occurs (supplementary states, Section 6.3.3). The possibility to transform a given stochastic process into a Markov process by introducing supplementary variables is not considered here. Generalization of the distribution functions for repair times leads to *semi-regenerative processes*, i.e., to processes with an *embedded semi-Markov process*. This holds, in particular, if the system has *only one repair crew*, since each termination of a repair is a regeneration point (because of the constant failure rates). Arbitrary distributions of repair and failure-free times lead in general to *nonregenerative stochastic processes*.

Table 6.1 shows the processes used in reliability investigations of repairable systems, with their possibilities and limits. Appendix A7 introduces these processes with particular emphasis on reliability applications. All equations necessary for the reliability and availability calculation of systems described by time-homogeneous Markov processes and semi-Markov processes are summarized in Table 6.2.

Besides the assumption about the involved distribution functions for failure-free and repair times, reliability and availability calculation is largely influenced by the maintenance strategy, logistic support, type of redundancy, and dependence between elements. Existence of a reliability block diagram is assumed in Sections 6.2-6.7, not necessarily in Sections 6.8-6.10. Results are expressed as functions of time by solving appropriate systems of differential (or integral) equations, or given by the mean time to failure or the steady-state point availability at system level ($MTTF_{Si}$ or PA_S) by solving appropriate systems of *algebraic equations*. If the system has no redundancy, the reliability function is the same as in the nonrepairable case. In the presence of redundancy, it is generally assumed that redundant elements will be *repaired on line*, i.e. *without operational interruption at system level*. Reliability investigations thus aim to find the occurrence of the *first system down*, whereas the *point availability* is the probability to find the system in an *up state* at a time t , independently of whether down states at system level have occurred before t .

In order to unify models and simplify calculations, the *following assumptions are made for analyses in Sections 6.2-6.7* (partly also in Sections 6.8-6.10).

1. *Continuous operation*: Each element of the system is in operating or reserve state, when not under repair or waiting for repair. (6.1)
2. *No further failures at system down* (no FF): At system down the system is repaired (restored) according to a given *maintenance strategy* to an up state at system level from which operation is continued, failures during a repair at system down are not considered. (6.2)
3. *Only one repair crew*: At system level only one repair crew is available, repair is performed according to a stated strategy (e.g. first-in/first-out). (6.3)

- 4. *Redundancy*: Failure detection & switch are ideal, and redundant elements are repaired *on line*, i.e. without interruption of operation at system level. (6.4)
- 5. *States*: Each *element in the reliability block diagram* has only two states (good or failed), and is *as-good-as-new* after each repair (restoration). (6.5)
- 6. *Independence*: Failure-free (failure-free operating) and repair (restoration) times of each element are stochastically independent, > 0 , and continuous random variables with finite mean ($MTTF, MTTR$) and variance. (6.6)
- 7. *Support*: Preventive maintenance is neglected and logistic support is ideal (repair time = restoration time = down time). (6.7)

The above assumptions holds for Sections 6.2- 6.7, and apply in many practical applications. However, assumption (6.5) must be *critically verified* for the aspect *as-good-as-new*, when repaired elements contain parts with time dependent failure rate which have not been replaced by new ones at repair; with (6.3), it applies at system level only if at each repair *all non-replaced parts have constant failure rates*.

At system level, reliability figures have indices S_i (e.g. $MTTF_{S_i}$), where S stands for system and i is the state entered at $t=0$, see Table 6.2 (*system* refers in this book, often in practical applications, to the highest integration level of the item considered; $t=0$ is the beginning of observations, $x=0$ for interarrival times). Assuming irreducible embedded Markov chains, *asymptotic & steady-state* is used for *stationary*.

Table 6.1 Basic stochastic processes used in *reliability & availability analysis of repairable systems*

Stochastic process	Can be used in modeling	Back-ground	Diffi-culty
Renewal process	One-item structures with <i>arbitrary failure rates, negligible repair times, new after repair</i>	Renewal theory	Medium
Alternating renewal proc. (SMP with 2 states)	One-item repairable structures with <i>arbitrary failure and repair rates, new after repair</i>	Renewal theory	Medium
Markov process (MP) (finite state space, time-homogeneous, regenerative at every time point t)	Systems of <i>arbitrary structure</i> whose elements have <i>constant failure and repair rates during the stay time in every state</i> (not necessarily at a state change, e. g. because of load sharing) *	Differential eqs. or Integral equations	Low
Semi-Markov process with >2 states (SMP) (regenerative at state change)	Some (few) systems with only <i>one repair crew</i> , whose elements have <i>constant failure and arbitrary repair rates</i> *	Integral equations	Medium
Semi-regenerative process (process with an embedded SMP with ≥ 2 states)	Systems of <i>arbitrary structure</i> with only <i>one repair crew</i> , whose elements have <i>constant failure and arbitrary repair rates</i> *	Integral equations	High
Regenerative process with just one regeneration state	Systems of <i>arbitrary structure</i> whose elements have <i>constant failure and arbitrary repair rates</i> * (in some cases const. failure rate only in a reserve state)	Integral equations	High to very high
Nonregenerative process	Systems whose elements have <i>arbitrary failure and repair rates</i>	Partial diff. eqs.	High to very high

repaired elements new after repair (yielding system new (with respect to a specific state) for constant failure rates of all elements and only one repair crew); * constant failure / repair rates can be extended to Erlang distribution (Fig. 6.6)

Table 6.2 Relationships for the reliability, point availability & interval reliability of systems described by time-homogeneous Markov processes or semi-Markov processes (Appendices A7.5 & A7.6)

	Reliability	Point Availability	Interval Reliability
Semi - Markov Processes (SMP)	$R_{S_i}(t) = 1 - Q_i(t) + \sum_{\substack{Z_j \in U \\ j \neq i}} \int_0^t q_{ij}(x) R_{S_j}(t-x) dx, \quad Z_i \in U, t > 0, \\ R_{S_i}(0) = 1$ $MTTF_{S_i} = T_i + \sum_{\substack{Z_j \in U \\ j \neq i}} p_{ij} MTTF_{S_j}, \quad Z_i \in U$ <p>with</p> $Q_{ij}(x) = \Pr\{\tau_{ij} \leq x \cap \tau_{ik} > \tau_{ij}, k \neq i, j\} = p_{ij} F_{ij}(x), \quad j \neq i, x > 0,$ $q_{ij}(x) = \frac{dQ_{ij}(x)}{dx} = p_{ij} \frac{dF_{ij}(x)}{dx}, \quad Q_i(x) = 0, \quad i, j \in \{0, \dots, m\},$ $p_{ij} = \Pr\{\tau_{ik} > \tau_{ij}, k \neq i, j\} = Q_{ij}(0), \quad p_{ii} = 0$ $F_{ij}(x) = \Pr\{\tau_{ij} \leq x \mid \tau_{ik} > \tau_{ij}, k \neq i, j\}, \quad F_{ij}(x) = Q_{ij}(x) = 0 \text{ for } x \leq 0$	$PA_{S_i}(t) = \sum_{\substack{Z_j \in U \\ j \neq i}} P_{ij}(t), \quad i = 0, \dots, m, t > 0, \\ PA_{S_i}(0) = 1 \text{ for } Z_i \in U$ $PA_S = \lim_{t \rightarrow \infty} PA_{S_i}(t) = \sum_{\substack{Z_j \in U \\ j \neq i}} P_j \quad (\text{see } IR_S(\theta) \text{ for } P_j)$ <p>with</p> $P_{ij}(t) = \delta_{ij}(1 - Q_j(t)) + \sum_{\substack{k=0 \\ k \neq i}}^m \int_0^t q_{ik}(x) P_{kj}(t-x) dx,$ $i, j \in \{0, \dots, m\}, t > 0, P_{ij}(0) = \delta_{ij}, \delta_{ij} = 1, \delta_{ij} = 0 \text{ for } j \neq i,$ $Q_i(x) = \sum_{\substack{j=0 \\ j \neq i}}^m Q_{ij}(x), \quad T_i = \int_0^{\infty} (1 - Q_i(x)) dx$	<p>Problem oriented calculation: for constant failure rates, following approximation can often be used in steady-state</p> $IR_{S_i}(\theta) \approx \sum_{\substack{Z_j \in U \\ j \neq i}} P_j R_{S_j}(\theta), \quad \theta > 0$ <p>with</p> $P_j = \lim_{t \rightarrow \infty} P_j(t) = \lim_{t \rightarrow \infty} P_{ij}(t) = \frac{T_j}{T_{ij}}, \quad T_j = \frac{1}{p_j} \sum_{k=0}^m q_{jk} T_k,$ $T_j = \int_0^{\infty} (1 - Q_j(x)) dx, \text{ and } p_j \text{ from } p_j = \sum_{\substack{i=0 \\ i \neq j}}^m q_{ji} p_i$ <p>$i, j \in \{0, \dots, m\}, p_j = 0, p_j > 0, \sum p_j = 1$ (one eq. for p_j, arbitrarily chosen, must be replaced by $\sum p_j = 1$); q_{ij} = steady-state prob. of the irreducible embedded Markov chain</p>
Time Homogeneous Markov Processes (method of integral equations)	$R_{S_i}(t) = e^{-p_i t} + \sum_{\substack{Z_j \in U \\ j \neq i}} \int_0^t p_{ij} e^{-p_i x} R_{S_j}(t-x) dx, \quad Z_i \in U, t > 0, \\ R_{S_i}(0) = 1$ $MTTF_{S_i} = \frac{1}{p_i} + \sum_{\substack{Z_j \in U \\ j \neq i}} \frac{p_{ij}}{p_i} MTTF_{S_j}, \quad Z_i \in U$ <p>with</p> $P_{ij} = \text{transition rate (see definitions below)}, \quad p_i = \sum_{\substack{j=0 \\ j \neq i}}^m P_{ij}$	$PA_{S_i}(t) = \sum_{\substack{Z_j \in U \\ j \neq i}} P_{ij}(t), \quad i = 0, \dots, m, t > 0, \\ PA_{S_i}(0) = 1 \text{ for } Z_i \in U$ $PA_S = \lim_{t \rightarrow \infty} PA_{S_i}(t) = \sum_{\substack{Z_j \in U \\ j \neq i}} P_j \quad (\text{see } IR_S(\theta) \text{ for } P_j)$ <p>with</p> $P_{ij}(t) = \delta_{ij} e^{-p_i t} + \sum_{\substack{k=0 \\ k \neq i}}^m \int_0^t p_{ik} e^{-p_i x} P_{kj}(t-x) dx,$ $i, j \in \{0, \dots, m\}, t > 0, P_{ij}(0) = \delta_{ij}, \delta_{ij} = 1, \delta_{ij} = 0 \text{ for } j \neq i$	$IR_{S_i}(t, t+\theta) = \sum_{\substack{Z_j \in U \\ j \neq i}} P_{ij}(t) R_{S_j}(\theta), \quad i = 0, \dots, m, \\ t, \theta > 0$ $IR_S(\theta) = \lim_{t \rightarrow \infty} IR_{S_i}(t, t+\theta) = \sum_{\substack{Z_j \in U \\ j \neq i}} P_j R_{S_j}(\theta), \quad \theta > 0$ <p>see below for P_j</p>

Table 6.2 (cont.)

<p>Time Homogeneous Markov Processes (method of differential equations)</p>	$R_{S_i}(t) = \sum_{Z_j \in U} P_{ij}^1(t), \quad Z_i \in U, \quad t > 0, \quad R_{S_i}(0) = 1$ $MTTF_{S_i} = \frac{1}{\rho_i} + \sum_{\substack{Z_j \in U \\ j \neq i}} \frac{\rho_{ij}}{P_i} \quad MTTFS_j, \quad Z_i \in U$ <p style="text-align: center;"><i>with</i></p> <p>$P_{ij}^1(t) = P_j^1(t)$ and $P_j^1(t)$ obtained from</p> $\dot{P}_j^1(t) = -\rho_j P_j^1(t) + \sum_{i=0, i \neq j}^m P_i^1(t) \rho_{ij}, \quad j=0, \dots, m, \quad t > 0,$ <p>$\rho_j = P_{jj}$ for $Z_i \in U$, $\rho_j^1 = 0$ for $Z_i \in \bar{U}$, $\rho_j^1 = \sum_{i=0, i \neq j}^m \rho_{ij}$, $P_j^1(0) = 1$, $P_j^1(0) = 0$ for $j \neq i$, $Z_i \in U$</p>	$PA_{S_i}(t) = \sum_{Z_j \in U} PA_{S_i}(t), \quad i=0, \dots, m, \quad t > 0$ $PA_{S_i}(0) = 1 \text{ for } Z_i \in U$ <p style="text-align: center;"><i>with</i></p> $PA_{S_i}(t) = \lim_{t \rightarrow \infty} PA_{S_i}(t) = \sum_{Z_j \in U} P_j \quad (\text{see } IR_{S_i}(\theta) \text{ for } P_j)$	$IR_{S_i}(t, t+\theta) = \sum_{Z_j \in U} P_{ij}^1(t) R_{S_j}(\theta), \quad i=0, \dots, m, \quad t, \theta > 0$ $IR_{S_i}(\theta) = \lim_{t \rightarrow \infty} IR_{S_i}(t, t+\theta) = \sum_{Z_j \in U} P_j R_{S_j}(\theta), \quad \theta > 0$ <p style="text-align: center;"><i>with</i></p> $P_j = \lim_{t \rightarrow \infty} P_j(t) = \lim_{t \rightarrow \infty} P_{ij}^1(t) \quad \text{from } \rho_j P_j = \sum_{i=0, i \neq j}^m P_i \rho_{ij},$ <p>$i, j \in \{0, \dots, m\}$, $P_j > 0$ (irreducible embedded Markov chain), $P_0 + \dots + P_m = 1$ (one equation for P_j, arbitrarily chosen, must be dropped and replaced by $P_0 + \dots + P_m = 1$)</p>
---	--	---	--

$R_{S_i}(t) = \text{Pr}\{\text{system up in } (0, t] \mid Z_i \text{ is entered at } t=0\}^*$, $Z_i \in U$; S stays for system; $U = \text{set of the up states}$, $\bar{U} = \text{set of the down states}$, $U \cup \bar{U} = \{Z_0, \dots, Z_m\}$
 $MTTF_{S_i} = E\{\text{system failure-free time} \mid Z_i \text{ is entered at } t=0\} = \int_0^\infty R_{S_i}(t) dt = \bar{R}_{S_i}(0)^*$, $Z_i \in U$; $\bar{R}_{S_i}(s) = \int_0^\infty R_{S_i}(t) e^{-st} dt = \text{Laplace transform of } R_{S_i}(t)$
 $PA_{S_i}(t) = \text{Pr}\{\text{system up at } t \mid Z_i \text{ is entered at } t=0\}^*$, $i=0, \dots, m$; $PA_S = \text{Pr}\{\text{system up at } t \text{ in steady-state or for } t \rightarrow \infty\} = \Delta A_S = \text{average av. in steady-state or for } t \rightarrow \infty$
 $IR_{S_i}(t, t+\theta) = \text{Pr}\{\text{system up in } [t, t+\theta] \mid Z_i \text{ is entered at } t=0\}^*$, $Z_i \in U$ (in general); $IR_{S_i}(\theta) = \text{Pr}\{\text{system up in } [t, t+\theta] \text{ in steady-state or for } t \rightarrow \infty\}$
 $T_i = \text{mean stay (sojourn) time in } Z_i$ ($= 1/\rho_i$ for Markov processes, $= \int_0^\infty (1-Q_i(x)) dx$ for SMP); $T_{ij} = \frac{T_i}{P_i} = \frac{1}{P_i} \sum_{k=0}^m q_k T_k = \text{mean recurrence time of } Z_i$
 $MDT_{S_i}^{**} = PA_{S_i} f_{i, \text{abs}} = \text{system mean up time}$; $MDT_{S_i} = (1-PA_S) / f_{i, \text{abs}} = \text{system mean down time}$; $f_{i, \text{abs}} = f_{i, \text{abs}} = 1 / (MU_{S_i} + MDT_{S_i}) = \sum_{Z_j \in U} P_j \rho_j$ for Markov processes
 $P_{ij}(t) = \text{Pr}\{\text{system in state } Z_j \text{ at } t \mid Z_i \text{ is entered at } t=0\}^*$; $P_j(t) = \text{Pr}\{\text{system in state } Z_j \text{ at } t\}$, $P_j = \lim_{t \rightarrow \infty} P_j(t) = P_j(t)$ in steady-state $= \lim_{t \rightarrow \infty} P_{ij}(t) = T_{ij} / T_j$
 $P_{ij} = \lim_{\delta t \downarrow 0} \frac{1}{\delta t} \text{Pr}\{\text{transition from } Z_i \text{ to } Z_j \text{ in } (t, t+\delta t)\}$ system in Z_i at t , holds for Markov processes only ($\rho_{ij} = P_i q_{ij}$, $P_{ii} = 0$), $t > 0$ arbitrary

^{*}for Markov processes (MP), Z_i is entered at $t=0$; ^{**} MU_{S_i} is the mean time between a transition $\bar{U} \rightarrow U$ and the successive $U \rightarrow \bar{U}$ in steady-state or for $t \rightarrow \infty$ (considering MU_{S_i} and MDT_{S_i} , one recognizes that in steady-state, or for $t \rightarrow \infty$, a system behaves like a one-item structure $MTTF = MU_{S_i}$, $MTTR = MDT_{S_i}$; for practical applications, $MU_{S_i} = MTTFS_0$; a repaired element is as-good-as-new, yielding for MP-system as-good-as-new with respect to the state considered; $t=0$ is the begin of the observation ($x=0$ for interarrival times); repair used for restoration)

Section 6.2 considers the one-item repairable structure under general assumptions, allowing a careful investigation of the *asymptotic and stationary behavior*. For basic reliability structures encountered in practical applications (series, parallel, and series-parallel), investigations in Sections 6.3 - 6.6 begin by assuming *constant failure and repair rates* for every element in the reliability block diagram. Distributions of repair times, and as far as possible of failure-free times, are then generalized step by step up to the case in which the process involved remains regenerative with a *mini-mum number of regeneration states*. This, also to show capability & limits of the models involved. For large series-parallel structures, *approximate expressions* are carefully developed in Section 6.7. Procedures for investigating *repairable systems with complex structure* (for which a reliability block diagram often does not exist) are given in Section 6.8 on the basis of practical examples, including imperfect switching, incomplete coverage, more than 2 states, phased-mission systems, common cause failures, and fault tolerant reconfigurable systems with reward & frequency/duration aspects. It is shown that tools developed in Appendix A7 (Tab. 6.2) can be used to solve many of the problems occurring in practical applications, on a *case-by-case basis* working with the *diagram of transition rates* or a *time schedule*. Alternative investigation methods, as well as computer-aided analysis are discussed in Section 6.9 and a Monte Carlo approach useful for rare events is given. Human reliability is considered in Section 6.10.

From the results of Sections 6.2 - 6.10, the following *conclusions* can be drawn:

1. As long as $MTTR_i \ll MTTF_i$ holds for each element E_i in the reliability block diagram, the *shape of the distribution function* of the repair time has small influence on $MTTF_S$ and $PA_S = AA_S$ (Examples 6.8, 6.9, 6.10).
2. As a consequence of Point 1, it is preferable to start investigations by assuming *Markov models* (constant failure & repair rates for all elements, Table 6.2); in a second step, more appropriate distribution functions can be considered (p. 277).
3. The assumption (6.2) of no further failure at system down *has no influence on the reliability function*; it allows a reduction of the state space and simplifies availability & interval reliability calculations (yielding good approximations).
4. Already for moderately large systems, use of Markov models can become time-consuming (up to $e \cdot n!$ states for a rel. block diagram with n elements); *approximate expressions* are thus important, and the *macro-structures* introduced in Section 6.7 (Table 6.10) adheres well to many practical applications.
5. For large systems or complex structures, following possibilities are available:
 - work directly with the diagram of transition rates (Section 6.8),
 - calculation of the mean time to failure and steady-state availability at system level only (Table 6.2, Eqs. (A7.126), (A7.173), (A7.131), (A7.178)),
 - use of approximate expressions (Sections 6.7 & 6.9.7, Tables 6.9 & 6.10),
 - use of alternative methods or of *Monte-Carlo simulation* (Section 6.9).
6. *Human reliability* has to be evaluated on a *case-by-case basis*; having in mind, as far as possible, to bypass or greatly support dangerous human decisions.

6.2 One-Item Structure

A *one-item structure* is an unit of arbitrary complexity, generally considered as an entity for investigations. Its reliability block diagram is a single element (Fig. 6.1). Considering that in practical applications a *repairable* one-item structure can have the complexity of a system, and also to use the same notation as in the following sections of this chapter,

reliability figures are given with indices S or S_i (e.g. $PA_S, R_{S_i}(t), MTTF_{S_i}$), where S stands for system and i specifies the state (Z_i) entered at $t=0$ (S alone for steady-state (PA_S, AA_S) and Z_0 for item (system) new at $t=0$).

Under the assumptions (6.1)–(6.3) and (6.5)–(6.7), the repairable one-item structure is completely characterized by the distribution function of the *failure-free times* $\tau_0, \tau_1, \dots > 0$

$$F_A(x) = \Pr\{\tau_0 \leq x\} \quad \text{and} \quad F(x) = \Pr\{\tau_i \leq x\}, \quad \begin{matrix} i=1,2,\dots, & x>0, \\ F_A(0)=F(0)=0, \end{matrix} \quad (6.8)$$

with densities

$$f_A(x) = \frac{d F_A(x)}{dx} \quad \text{and} \quad f(x) = \frac{d F(x)}{dx}, \quad (6.9)$$

the distribution function of the *repair times* $\tau'_0, \tau'_1, \dots > 0$

$$G_A(x) = \Pr\{\tau'_0 \leq x\} \quad \text{and} \quad G(x) = \Pr\{\tau'_i \leq x\}, \quad \begin{matrix} i=1,2,\dots, & x>0 \\ G(0)=G_A(0)=0, \end{matrix} \quad (6.10)$$

with densities

$$g_A(x) = \frac{d G_A(x)}{dx} \quad \text{and} \quad g(x) = \frac{d G(x)}{dx}, \quad (6.11)$$

and the probability p that the one-item structure is *up* at $t = 0$

$$p = \Pr\{up \text{ at } t = 0\} \quad (6.12)$$

or

$$1 - p = \Pr\{down \text{ (i.e. under repair) at } t = 0\},$$

respectively. τ_0 & τ'_0 belong to the same item, as τ_i & τ'_i ; all are *interarrival times*, and x is used instead of t . $MTTF = E[\tau_i]$, $MTTR = E[\tau'_i]$, $\text{Var}[\tau_i], \text{Var}[\tau'_i] < \infty$ ($i \geq 1$) are tacitly assumed. With these assumptions, the time behavior of the one-item structure can be investigated with an *alternating renewal process* (Appendix A7.3).

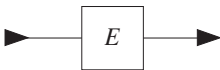


Figure 6.1 Reliability block diagram for a one-item structure

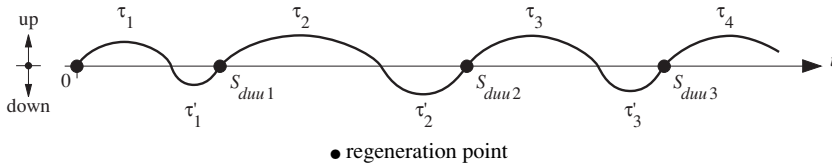


Figure 6.2 Possible time behavior for a *repairable one-item structure new at $t = 0$* (repair times greatly exaggerated, *alternating renewal process with regeneration points $0, S_{dnu1}, S_{dnu2}, \dots$* for a transition from down state to up state given that the item is up at $t = 0$ (marked by ●))

Section 6.2.1 considers the one-item structure *new at $t = 0$* , i.e., the case $p = 1$ and $F_A(x) = F(x)$, with arbitrary $F(x)$ and $G(x)$. Generalization of the initial conditions at $t = 0$ (Sections 6.2.3) allows in Sections 6.2.4 and 6.2.5 a depth investigation of the *asymptotic and steady-state behavior*.

6.2.1 One-Item Structure New at Time $t = 0$

Figure 6.2 shows the time behavior of a one-item structure new at $t = 0$. τ_1, τ_2, \dots are the failure-free times. They are statistically independent and distributed according to $F(x)$ as per Eq. (6.8). Similarly, τ'_1, τ'_2, \dots are the repair times, distributed according to $G(x)$ as per Eq. (6.10). Considering assumption (6.5), the time points $0, S_{dnu1}, \dots$ are *regeneration points* (see the footnote on p. 464) and constitute an ordinary *renewal process embedded* in the original alternating renewal process. Investigations of this Section are based on this property (S_{dnu} means a transition from *down* (repair) to *up* (operating) starting up at $t = 0$).

6.2.1.1 Reliability Function

The *reliability function* $R_{S0}(t)$ gives the probability that the item operates failure free in $(0, t]$ given *item new at $t = 0$*

$$R_{S0}(t) = \Pr\{\text{up in } (0, t] \mid \text{new at } t = 0\}. \tag{6.13}$$

Considering Eqs. (2.7) and (6.8) it holds that

$$R_{S0}(t) = \Pr\{\tau_1 > t\} = 1 - F(t), \tag{6.14}$$

yielding $R_{S0}(t) = e^{-\lambda t}$ for the case of constant failure rate λ . The *mean time to failure* given *item new at $t = 0$* follows from Eq. (A6.38)

$$MTTF_{S0} = \int_0^{\infty} R_{S0}(t) dt, \tag{6.15}$$

with upper limit of the integral T_L should the useful life of the item be limited to T_L ($R_{S_0}(t)$ jumps to 0 at $t=T_L$). In the following, $T_L=\infty$ is tacitly assumed, yielding $MTTF_{S_0} = 1/\lambda$ for the case of constant failure rate λ .

6.2.1.2 Point Availability

The *point availability* $PA_{S_0}(t)$ gives the probability of finding the item operating at time t given *item new at* $t=0$

$$PA_{S_0}(t) = \Pr\{up \text{ at } t \mid \text{new at } t=0\}. \quad (6.16)$$

For $PA_{S_0}(t)$ it holds that

$$PA_{S_0}(t) = 1 - F(t) + \int_0^t h_{duu}(x)(1 - F(t-x))dx. \quad (6.17)$$

$A(t)$ is often used instead of $PA_{S_0}(t)$. Equation (6.17) is derived in Appendix A7.3 (Eq. (A7.56)) using the theorem of total probability. $1 - F(t)$ is the probability of no failure in $(0, t]$, $h_{duu}(x)dx$ gives the probability that any one of the regeneration points $S_{duu1}, S_{duu2}, \dots$ lies in $(x, x + dx]$, and $1 - F(t-x)$ is the probability that no further failure occurs in $(x, t]$. Using *Laplace transform* (Appendix A9.7) and considering Eq. (A7.50) with $F_A(x) = F(x)$, Eq. (6.17) yields

$$\tilde{P}A_{S_0}(s) = \frac{1 - \tilde{f}(s)}{s(1 - \tilde{f}(s)\tilde{g}(s))}. \quad (6.18)$$

$\tilde{f}(s)$ and $\tilde{g}(s)$ are the Laplace transforms of the failure-free time and repair time densities, respectively (given by Eqs. (6.9) and (6.11)).

Example 6.1

- Give the Laplace transform of the point availability $PA_{S_0}(t)$ for the case of a *constant failure rate* λ ($\lambda(x) = \lambda$).
- Give the Laplace transform and the corresponding time function of the point availability for the case of *constant failure and repair rates* λ and μ ($\lambda(x) = \lambda$ and $\mu(x) = \mu$).

Solution

- With $F(x) = 1 - e^{-\lambda x}$ or $f(x) = \lambda e^{-\lambda x}$, Eq. (6.18) yields

$$\tilde{P}A_{S_0}(s) = 1 / (s + \lambda(1 - \tilde{g}(s))). \quad (6.19)$$

Supplementary results: $g(x) = \alpha(\alpha x)^{\beta-1} e^{-\alpha x} / \Gamma(\beta)$ (Eq. (A6.98)) yields

$$\tilde{P}A_{S_0}(s) = \frac{(s + \alpha)^\beta}{(s + \lambda)(s + \alpha)^\beta - \lambda \alpha^\beta}.$$

b) With $f(x) = \lambda e^{-\lambda x}$ and $g(x) = \mu e^{-\mu x}$, Eq. (6.18) yields

$$\tilde{P}A_{S_0}(s) = \frac{s + \mu}{s(s + \lambda + \mu)},$$

and thus (Table A9.7)

$$PA_{S_0}(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t} \approx (1 - \lambda/\mu) + \frac{\lambda}{\mu} e^{-\mu t} \approx 1 - \frac{\lambda}{\mu} (1 - e^{-\mu t}). \quad (6.20)$$

$PA_{S_0}(t)$ converges rapidly, exponentially with a time constant $1/(\lambda + \mu) \approx 1/\mu = MTTR$ to the asymptotic value $\mu/(\lambda + \mu) \approx 1 - \lambda/\mu$, see Section 6.2.4 for an extensive discussion.

Supplementary results: Because of $\lambda(t) = \lambda$, the probability to be up at time t and have a failure in $(t, t + \delta t]$ is given by $PA_{S_0}(t) \lambda \delta t$, see also the footnote on p. 475.

$PA_{S_0}(t)$ can also be obtained using *renewal process* arguments (Appendices A7.2, A7.3, A7.6). After the first repair the item is *as-good-as-new*. S_{dual} is a *regeneration point* and from this time point the process *restarts anew* as at $t = 0$. Therefore

$$\Pr\{up \text{ at } t \mid S_{dual} = x\} = PA_{S_0}(t - x). \quad (6.21)$$

Considering that the event

$$\{up \text{ at } t\}$$

occurs with exactly one of the following two mutually exclusive events

$$\{\text{no failure in } (0, t]\}$$

or

$$\{S_{dual} < t \cap up \text{ at } t\}$$

it follows that

$$PA_{S_0}(t) = 1 - F(t) + \int_0^t (f(x) * g(x)) PA_{S_0}(t - x) dx, \quad (6.22)$$

where $f(x) * g(x)$ is the density of the sum $\tau_1 + \tau_1'$ (see Fig 6.2 and Eq. (A6.75)). Equation (6.22) is the *integral equation* for $PA_{S_0}(t)$, and yields also to Eq. (6.18).

6.2.1.3 Average Availability

The *average availability* $AA_{S_0}(t)$ is defined as the expected proportion of time in which the item is operating in $(0, t]$ given *item new* at $t = 0$

$$AA_{S_0}(t) = \frac{1}{t} E[\text{total } up \text{ time in } (0, t] \mid \text{new at } t = 0]. \quad (6.23)$$

Considering $PA_{S_0}(x)$ from Eq. (6.17), it holds that

$$AA_{S_0}(t) = \frac{1}{t} \int_0^t PA_{S_0}(x) dx. \quad (6.24)$$

Eq. (6.24) has a great intuitive appeal. It can be proved by considering that the time behavior of the repairable item can be described by an indicator (binary process) $\zeta(t)$ taking values 1 for *up* and 0 for *down*. From this, $E[\zeta(t)] = 0 \cdot (1 - PA_{S_0}(t)) + 1 \cdot PA_{S_0}(t) = PA_{S_0}(t)$ and, taking care of $\int_0^t \zeta(x) dx = \text{total up time in } (0, t]$, it follows that (by Fubini's theorem [A6.6 (Vol. II)] and assuming existence of the integrals)

$$AA_{S_0}(t) = \frac{1}{t} E\left[\int_0^t \zeta(x) dx\right] = \frac{1}{t} \int_0^t E[\zeta(x)] dx = \frac{1}{t} \int_0^t PA_{S_0}(x) dx.$$

6.2.1.4 Interval Reliability

The *interval reliability* $IR_{S_0}(t, t+\theta)$ gives the probability that the item operates failure free during an interval $[t, t+\theta]$ given *item new at* $t = 0$

$$IR_{S_0}(t, t+\theta) = \Pr\{\text{up in } [t, t+\theta] \mid \text{new at } t = 0\}. \quad (6.25)$$

The same method used to obtain Eq. (6.17) leads to

$$IR_{S_0}(t, t+\theta) = 1 - F(t+\theta) + \int_0^t h_{duu}(x)(1 - F(t+\theta - x)) dx. \quad (6.26)$$

Example 6.2

Give the interval reliability $IR_{S_0}(t, t+\theta)$ for the case of a *constant failure rate* λ ($\lambda(x) = \lambda$).

Solution

With $F(x) = 1 - e^{-\lambda x}$ it follows that

$$IR_{S_0}(t, t+\theta) = e^{-\lambda(t+\theta)} + \int_0^t h_{duu}(x) e^{-\lambda(t+\theta-x)} dx = [e^{-\lambda t} + \int_0^t h_{duu}(x) e^{-\lambda(t-x)} dx] e^{-\lambda\theta}.$$

Comparison with Eq. (6.17) for $F(x) = 1 - e^{-\lambda x}$ yields

$$IR_{S_0}(t, t+\theta) = PA_{S_0}(t) \cdot e^{-\lambda\theta}, \quad \text{for } \lambda(x) = \lambda. \quad (6.27)$$

It must be pointed out that the *product rule* in Eq. 6.27, expressing $\Pr\{\text{up in } [t, t+\theta] \mid \text{new at } t=0\} = \Pr\{\text{up at } t \mid \text{new at } t=0\} \cdot \Pr\{\text{no failure in } (t, t+\theta] \mid \text{up at } t\}$, holds *only* because of *constant failure rate* $\lambda(x) = \lambda$ (*memoryless property*, Eq. (2.14)); in the general case, the second term is $\Pr\{\text{no failure in } (t, t+\theta] \mid (\text{up at } t \cap \text{new at } t=0)\}$, which differs from $\Pr\{\text{no failure in } (t, t+\theta] \mid \text{up at } t\}$. Also should the use of $IR(t_1, t_2)$ as reliability $R(t_1, t_2)$ be dropped, to avoid misuses (see remarks on pp. 40 and 426).

6.2.1.5 Special Kinds of Availability

In addition to the point and average availability (Sections 6.2.1.2 and 6.2.1.3), there are several other kinds of availability useful for practical applications [6.5 (1973)]:

1. *Mission Availability*: The mission availability $MA_{S0}(T_o, t_o)$ gives the probability that in a mission of total operating time (*total up time*) T_o each failure can be repaired within a time span t_o , given *item new at $t = 0$*

$$MA_{S0}(T_o, t_o) = \Pr\{\text{each individual failure occurring in a mission with total operating time } T_o \text{ can be repaired in a time } \leq t_o \mid \text{new at } t = 0\}. \quad (6.28)$$

Mission availability is important in applications where *interruptions of length* $\leq t_o$ can be accepted. Its computation considers all cases with $n = 0, 1, \dots$ failures, taking care that at the end of the mission the item is operating (to reach the given (fixed) operating time T_o).^{+) Thus, for given $T_o > 0$ and t_o ,}

$$MA_{S0}(T_o, t_o) = 1 - F(T_o) + \sum_{n=1}^{\infty} (F_n(T_o) - F_{n+1}(T_o)) (G(t_o))^n \quad (6.29)$$

holds. $F_n(T_o) - F_{n+1}(T_o)$ is the probability for n failures during the total operating time T_o (Eq. (A7.14) with $F_A(x) = F(x)$); $(G(t_o))^n$ is the probability that all n repair times will be shorter than t_o . For *constant failure rate* λ it holds that $F_n(T_o) - F_{n+1}(T_o) = (\lambda T_o)^n e^{-\lambda T_o} / n!$ (Eq. (A7.41)) and thus

$$MA_{S0}(T_o, t_o) = e^{-\lambda T_o (1 - G(t_o))}, \quad \text{for } \lambda(x) = \lambda. \quad (6.30)$$

2. *Work-Mission Availability*: The work-mission availability $WMA_{S0}(T_o, x)$ gives the probability that the *sum* of the repair times for all failures occurring in a mission of total operating time (*total up time*) T_o is $\leq x$, given *item new at $t = 0$*

$$WMA_{S0}(T_o, x) = \Pr\{\text{sum of the repair times for all failures occurring in a mission of total operating time } T_o \text{ is } \leq x \mid \text{new at } t = 0\}. \quad (6.31)$$

Similarly as for Eq. (6.29) it follows that for given (fixed) $T_o > 0$ and $x > 0$ ^{+) :}

$$WMA_{S0}(T_o, x) = 1 - F(T_o) + \sum_{n=1}^{\infty} (F_n(T_o) - F_{n+1}(T_o)) G_n(x), \quad (6.32)$$

where $G_n(x)$ is the distribution function of the sum of n repair times with distribution $G(x)$ (as per Eq. (A7.12)). As for the *mission availability*, the item is up at the end of the mission (to reach the given (fixed) operating time T_o). For constant failure and repair rates (λ, μ), Eq. (6.32) yields (Eq. (A7.219))

^{+) An unlimited number n of repair is assumed here, see e.g. Section 4.6 (p. 140) for n limited.}

^{++) See e.g. p. 522 for a possible application of Eq. (6.32) to a cumulative damage model.}

$$\text{WMA}_{S_0}(T_o, x) = 1 - e^{-(\lambda T_o + \mu x)} \sum_{n=1}^{\infty} \left[\frac{(\lambda T_o)^n}{n!} \sum_{k=0}^{n-1} \frac{(\mu x)^k}{k!} \right], \quad \begin{matrix} T_o > 0 \text{ given, } x > 0, \\ \text{WMA}_{S_0}(T_o, 0) = e^{-\lambda T_o}. \end{matrix} \quad (6.33)$$

Defining DT as total down time and $UT = t - DT$ as total up time in $(0, t]$, one recognizes that for given t , $\Pr\{DT \text{ in } (0, t] \leq x \mid \text{new at } t = 0\} = \text{WMA}_{S_0}(t - x, x)$ holds for an item described by Fig. 6.2 ($t > 0, 0 < x \leq t$). However, the item can now be up or down at t , and the situation differs thus from that defined by Eq. (6.31), for which the item is up at the given cumulative operating time T_o . $\text{WMA}_{S_0}(t - x, x)$ has been investigated in [A7.29(1957)]; besides a closed analytical expression for constant failure and repair rates (λ, μ) , it is shown that the distribution of DT converges for $t \rightarrow \infty$ to a normal distribution with mean $t \lambda / (\lambda + \mu) \approx t \lambda / \mu$ and variance $t 2 \lambda \mu / (\lambda + \mu)^3 \approx t 2 \lambda / \mu^2$. It can be noted that referred to Eqs. (6.32) and (6.33), mean and variance of the total repair time are given exactly by $T_o \lambda / \mu$ and $T_o 2 \lambda / \mu^2$, respectively (Eq. (A7.220)).

3. *Joint Availability*: The joint availability $\text{JA}_{S_0}(t, t + \theta)$ gives the probability of finding the item operating at the time points t and $t + \theta$, given *item new at* $t = 0$ (t, θ given, see e.g. [6.15(1999), 6.28] for stochastic demand)

$$\text{JA}_{S_0}(t, t + \theta) = \Pr\{\text{up at } t \cap \text{up at } t + \theta \mid \text{new at } t = 0\}. \quad (6.34)$$

For the case of *constant failure rate* $\lambda(x) = \lambda$, Eq. (6.27) yields

$$\text{JA}_{S_0}(t, t + \theta) = \text{PA}_{S_0}(t) \cdot \text{PA}_{S_0}(\theta), \quad \text{for } \lambda(x) = \lambda. \quad (6.35)$$

For arbitrary failure rate, one has to consider that $\{\text{up at } t \cap \text{up at } t + \theta \mid \text{new at } t = 0\}$ occurs with one of the following 2 mutually exclusive events (Appendix A7.3)

$$\{\text{up in } [t, t + \theta] \mid \text{new at } t = 0\}$$

or

$$\{\text{up at } t \cap \text{next failure occurs before } t + \theta \cap \text{up at } t + \theta \mid \text{new at } t = 0\}.$$

The probability for the first event is the interval reliability $\text{IR}_{S_0}(t, t + \theta)$ given by Eq. (6.26). For the second event, it is necessary to consider the distribution function of the *forward recurrence time in the up state* $\tau_{Ru}(t)$. As shown in Fig. 6.3, $\tau_{Ru}(t)$ can only be defined if the item is up at time t , hence

$$\Pr\{\tau_{Ru}(t) > x \mid \text{new at } t = 0\} = \Pr\{\text{up in } (t, t + x) \mid (\text{up at } t \cap \text{new at } t = 0)\}$$

and thus, as for Example A7.2 and considering Eqs. (6.16) and (6.25),

$$\begin{aligned} \Pr\{\tau_{Ru}(t) > x \mid \text{new at } t = 0\} &= \frac{\Pr\{\text{up in } [t, t + x] \mid \text{new at } t = 0\}}{\Pr\{\text{up at } t \mid \text{new at } t = 0\}} = \frac{\text{IR}_{S_0}(t, t + x)}{\text{PA}_{S_0}(t)} \\ &= 1 - F_{\tau_{Ru}}(x). \end{aligned} \quad (6.36)$$

For constant failure rate $\lambda(x) = \lambda$ one has $1 - F_{\tau_{Ru}}(x) = e^{-\lambda x}$, as per Eq. (6.27). Considering Eq. (6.36) it follows that

$$\begin{aligned} JA_{S_0}(t, t+\theta) &= IR_{S_0}(t, t+\theta) + PA_{S_0}(t) \int_0^\theta f_{\tau_{Ru}}(x) PA_{S_1}(\theta-x) dx \\ &= IR_{S_0}(t, t+\theta) - \int_0^\theta \frac{\partial IR_{S_0}(t, t+x)}{\partial x} PA_{S_1}(\theta-x) dx, \end{aligned} \tag{6.37}$$

where $PA_{S_1}(t) = \Pr\{up \text{ at } t \mid \text{a repair begins at } t=0\}$ is given by

$$PA_{S_1}(t) = \int_0^t h_{dud}(x)(1-F(t-x))dx, \tag{6.38}$$

with $h_{dud}(t) = g(t) + g(t)*f(t)*g(t) + g(t)*f(t)*g(t)*f(t)*g(t) + \dots$ (Eq. (A7.50)). $JA_{S_0}(t, t+\theta)$ can also be obtained in a similar way to $PA_{S_0}(t)$ in Eq. (6.17), by considering the alternating renewal process starting up at the time t with $\tau_{Ru}(t)$ distributed according to $F_{\tau_{Ru}}(x)$ as per Eq. (6.36). This leads to

$$JA_{S_0}(t, t+\theta) = IR_{S_0}(t, t+\theta) + \int_0^\theta h'_{duu}(x)(1-F(\theta-x))dx, \tag{6.39}$$

with $h'_{duu}(x) = f'_{\tau_{Ru}}(x) * g(x) + f'_{\tau_{Ru}}(x) * g(x) * f(x) * g(x) + \dots$, see Eq. (A7.50), and $f'_{\tau_{Ru}}(x) = PA_{S_0}(t)f_{\tau_{Ru}}(x) = PA_{S_0}(t)dF_{\tau_{Ru}}(x)/dx = -\partial IR_{S_0}(t, t+x)/\partial x$, see Eqs. (6.36) and (6.37). Similarly as for $\tau_{Ru}(t)$, the distribution function for the forward recurrence time in the down state $\tau_{Rd}(t)$ is given by (Fig. 6.3)

$$\Pr\{\tau_{Rd}(t) \leq x \mid \text{new at } t=0\} = 1 - \int_0^t h_{udu}(y)(1-G(t+x-y))dy / (1-PA_{S_0}(t)), \tag{6.40}$$

with $h_{udu}(t) = f(t) + f(t) * g(t) * f(t) + \dots$ (Eq. (A7.50)). For constant failure rate $\lambda(x) = \lambda$, Eq. (6.37) or (6.39) leads to Eq. (6.35), by considering Eq.(6.19).

Other kinds of availability are possible. For instance, availability by omitting down times for repair shorter than a given fixed or random time Δ has been investigated recently in [6.48], yielding for the case of fixed Δ to $\lim_{t \rightarrow \infty} PA_\Delta(t) = 1 - \frac{\lambda}{\lambda + \mu} (1 + \mu\Delta) e^{-\mu\Delta}$.

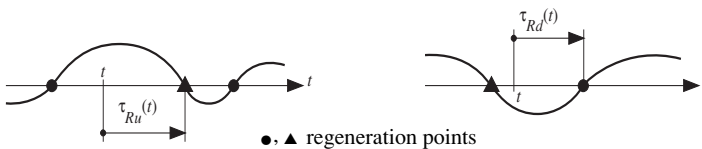


Figure 6.3 Forward recurrence times $\tau_{Ru}(t)$ and $\tau_{Rd}(t)$ in an alternating renewal process

6.2.2 One-Item Structure New at Time $t = 0$ and with Constant Failure Rate λ

In many practical applications, a *constant failure rate* λ can be assumed. In this case, the expressions of Section 6.2.1 can be simplified making use of the *memoryless property* given by the constant failure rate. Table 6.3 summarizes the results for the cases of constant failure rate (λ) and constant or arbitrary repair rate (μ or $\mu(x) = g(x)/(1 - G(x))$). Approximations in Table 6.3 are valid for $\lambda \ll \mu$ and $t > 10/\mu = 10 \text{ MTTR}$. For points 3 in Table 6.3 it can be noted that $AA_{S0}(0) = 1$, as for $PA_{S0}(0)$, and that the convergence of $AA_{S0}(t)$ toward $AA_S = PA_S$ is slower than that of $PA_{S0}(t)$. The product rule for $IR_{S0}(t, t + \theta)$ and $JA_{S0}(t, t + \theta)$ is valid only because of the constant failure rate λ .

Table 6.3 Results for a repairable one-item structure new at $t = 0$ and with constant failure rate λ

	Repair rate		Remarks, Assumptions
	arbitrary ($\mu(x)$)	constant (μ) *	
1. Reliability function $R_{S0}(t)$	$e^{-\lambda t}$	$e^{-\lambda t}$	$R_{S0}(t) = \Pr\{\text{up in } (0, t] \mid \text{new at } t = 0\}$
2. Point availability $PA_{S0}(t)$	$\int_0^t h_{duu}(x) e^{-\lambda(t-x)} dx + e^{-\lambda t}$	$\frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t}$ $\approx \mu / (\lambda + \mu) \approx 1 - \lambda / \mu$ **	$PA_{S0}(t) = \Pr\{\text{up at } t \mid \text{new at } t = 0\}$, $h_{duu} = f * g + f * g * f * g + \dots$
3. Average availability $AA_{S0}(t)$	$\frac{1}{t} \int_0^t PA_{S0}(x) dx$	$\frac{\mu}{\lambda + \mu} + \frac{\lambda(1 - e^{-(\lambda + \mu)t})}{t(\lambda + \mu)^2}$ $\approx 1 - (\lambda / \mu)(1 - 1/t\mu)$ **	$AA_{S0}(t) = E[\text{total up time in } (0, t] \mid \text{new at } t = 0] / t$
4. Interval reliability $IR_{S0}(t, t + \theta)$	$PA_{S0}(t) e^{-\lambda \theta}$	$\frac{\mu e^{-\lambda \theta}}{\lambda + \mu} + \frac{\lambda e^{-(\lambda + \mu)t - \lambda \theta}}{\lambda + \mu}$ $\approx (1 - \lambda / \mu) e^{-\lambda \theta}$ **	$IR_{S0}(t, t + \theta) = \Pr\{\text{up in } [t, t + \theta] \mid \text{new at } t = 0\}$
5. Joint availability $JA_{S0}(t, t + \theta)$	$PA_{S0}(t) PA_{S0}(\theta)$	$PA_{S0}(t) PA_{S0}(\theta)$	$JA_{S0}(t, t + \theta) = \Pr\{\text{up at } t \cap \text{up at } t + \theta \mid \text{new at } t = 0\}$, $PA_{S0}(x)$ as in point 2
6. Mission availability $MA_{S0}(T_o, t_f)$	$e^{-\lambda T_o (1 - G(t_f))}$	$e^{-\lambda T_o} e^{-\mu t_f}$	$MA_{S0}(T_o, t_f) = \Pr\{\text{each failure in a mission with total operating time } T_o \text{ can be repaired in a time } \leq t_f \mid \text{new at } t = 0\}$

see Eq. (6.33) for the *work-mission availability* & Eq. (6.196) for the *overall availability*; up = operating state;

* Markov process; ** approximations valid for $\lambda \ll \mu$ and $t > 10/\mu = 10 \text{ MTTR}$

6.2.3 One-Item Structure with Arbitrary Conditions at $t = 0$

Generalization of the initial conditions at time $t = 0$, i. e., the introduction of p , $F_A(x)$ and $G_A(x)$ as defined by Eqs. (6.12), (6.8), and (6.10), leads to a time behavior of the one-item repairable structure described by Fig. A7.3 and to the following results:

1. Reliability function $R_S(t)$

$$R_S(t) = \Pr\{up \text{ in } (0, t] \mid up \text{ at } t = 0\} = 1 - F_A(t). \quad (6.41)$$

Equation (6.41) follows from $\Pr\{up \text{ in } [0, t]\} = \Pr\{up \text{ at } t = 0 \cap \Pr\{up \text{ in } (0, t]\}\} = \Pr\{up \text{ at } t = 0\} \cdot \Pr\{up \text{ in } (0, t] \mid up \text{ at } t = 0\} = p \cdot (1 - F_A(t)) = p \cdot R_S(t)$.

2. Point availability $PA_S(t)$

$$PA_S(t) = \Pr\{up \text{ at } t\} = p[1 - F_A(t) + \int_0^t h_{duu}(x)(1 - F(t - x))dx] + (1 - p) \int_0^t h_{dud}(x)(1 - F(t - x))dx, \quad (6.42)$$

with $h_{duu}(t) = f_A(t) * g(t) + f_A(t) * g(t) * f(t) * g(t) + \dots$ and $h_{dud}(t) = g_A(t) + g_A(t) * f(t) * g(t) + g_A(t) * f(t) * g(t) * f(t) * g(t) + \dots$ (see also Eq. (A7.50)).

3. Average availability $AA_S(t)$

$$AA_S(t) = \frac{1}{t} E[\text{total up time in } (0, t)] = \frac{1}{t} \int_0^t PA_S(x)dx. \quad (6.43)$$

4. Interval reliability $IR_S(t, t + \theta)$

$$IR_S(t, t + \theta) = \Pr\{up \text{ in } [t, t + \theta]\} = p[1 - F_A(t + \theta) + \int_0^t h_{duu}(x)(1 - F(t + \theta - x))dx] + (1 - p) \int_0^t h_{dud}(x)(1 - F(t + \theta - x))dx. \quad (6.44)$$

5. Joint availability $JA_S(t, t + \theta)$

$$JA_S(t, t + \theta) = \Pr\{up \text{ at } t \cap up \text{ at } t + \theta\} = IR_S(t, t + \theta) - \int_0^\theta \frac{\partial IR_S(t, t + x)}{\partial x} PA_{S1}(\theta - x) dx, \quad (6.45)$$

with $IR_S(t, t + \theta)$ from Eq. (6.44) and $PA_{S1}(t)$ from Eq. (6.38).

6. *Forward recurrence times* ($\tau_{Ru}(t)$ and $\tau_{Rd}(t)$ as in Fig. 6.3)

$$\Pr\{\tau_{Ru}(t) \leq x\} = 1 - \text{IR}_S(t, t+x) / \text{PA}_S(t), \quad (6.46)$$

with $\text{IR}_S(t, t+x)$ according to Eq. (6.44) and $\text{PA}_S(t)$ from Eq. (6.42), and

$$\Pr\{\tau_{Rd}(t) \leq x\} = 1 - \frac{\Pr\{\text{down in } [t, t+x]\}}{1 - \text{PA}_S(t)}, \quad (6.47)$$

where

$$\begin{aligned} \Pr\{\text{down in } [t, t+x]\} &= p \int_0^t h_{udu}(y)(1-G(t+x-y)) dy \\ &\quad + (1-p)[1-G_A(t+x) + \int_0^t h_{udd}(y)(1-G(t+x-y)) dy], \end{aligned}$$

with $h_{udu}(t) = f_A(t) + f_A(t) * g(t) * f(t) + f_A(t) * g(t) * f(t) * g(t) * f(t) + \dots$ and $h_{udd}(t) = g_A(t) * f(t) + g_A(t) * f(t) * g(t) * f(t) + \dots$

Expressions for mission availability and work-mission availability are generally only used for items new at time $t=0$ (see [6.5 (1973)] for a generalization.

6.2.4 Asymptotic Behavior

As $t \rightarrow \infty$ expressions for the point availability, average availability, interval reliability, joint availability, and distribution functions of the forward recurrence time (Eqs. (6.42)-(6.47)) converge to quantities which are independent of t and of the initial conditions at $t=0$. Using the *key renewal theorem* (Eq. (A7.29)) it follows that (see also Example 6.3 and Eqs. (A7.58)-(A7.63))

$$\lim_{t \rightarrow \infty} \text{PA}_S(t) = \text{PA}_S = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}, \quad (6.48)$$

$$\lim_{t \rightarrow \infty} \text{AA}_S(t) = \text{AA}_S = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} = \text{PA}_S, \quad (6.49)$$

$$\lim_{t \rightarrow \infty} \text{IR}_S(t, t+\theta) = \text{IR}_S(\theta) = \frac{1}{\text{MTTF} + \text{MTTR}} \int_{\theta}^{\infty} (1-F(y)) dy, \quad (6.50)$$

$$\lim_{t \rightarrow \infty} \text{JA}_S(t, t+\theta) = \text{JA}_S(\theta) = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \text{PA}_{S0e}(\theta), \quad (6.51)$$

$$\lim_{t \rightarrow \infty} \Pr\{\tau_{Ru}(t) \leq x\} = \frac{1}{\text{MTTF}} \int_0^x (1-F(y)) dy, \quad (6.52)$$

$$\lim_{t \rightarrow \infty} \Pr\{\tau_{Rd}(t) \leq x\} = \frac{1}{\text{MTTR}} \int_0^x (1-G(y)) dy, \quad (6.53)$$

where $MTTF = E[\tau_i]$, $MTTR = E[\tau'_i]$, $i = 1, 2, \dots$ (Fig. 6.2), and $PA_{0e}(\theta)$ is the point availability according to Eq. (6.42) with $p = 1$ and $F_A(t)$ from Eq. (6.57) or (6.52). In practical applications, PA and AA (or PA_S and AA_S for system oriented values) are often referred as *availability* and denoted by A . The use of $PA_S = AA_S = (MTBF - MTTR) / MTBF$ is to avoid, because it implies $MTBF = MTTF + MTTR$.

Example 6.3

Show that for a repairable one-item structure in continuous operation (Point 1, p. 170), the limit

$$\lim_{t \rightarrow \infty} PA_S(t) = PA_S = \frac{MTTF}{MTTF + MTTR}$$

is valid for any distribution function $F(x)$, $F_A(x)$, $G(x)$, $G_A(x)$ satisfying conditions (A7.9)-(A7.11), and for which $f(x)$, $f_A(x)$, $g(x)$, $g_A(x)$ go to 0 as $x \rightarrow \infty$.

Solution

Using the *renewal density theorem* Eq. (A7.31) it follows that

$$\lim_{t \rightarrow \infty} h_{duu}(t) = \lim_{t \rightarrow \infty} h_{duu}(t) = \frac{1}{MTTF + MTTR}.$$

Furthermore, applying the *key renewal theorem* Eq.(A7.29) to $PA_S(t)$ given by Eq.(6.42) yields

$$\begin{aligned} \lim_{t \rightarrow \infty} PA_S(t) &= p \left(1 - 1 + \frac{\int_0^{\infty} (1 - F(x)) dx}{MTTF + MTTR} \right) + (1 - p) \frac{\int_0^{\infty} (1 - F(x)) dx}{MTTF + MTTR} \\ &= p \frac{MTTF}{MTTF + MTTR} + (1 - p) \frac{MTTF}{MTTF + MTTR} = \frac{MTTF}{MTTF + MTTR}. \end{aligned}$$

The limit $MTTF / (MTTF + MTTR)$ can also be obtained from the final value theorem of the Laplace transform (Table A9.7), considering for $s \rightarrow 0$

$$\begin{aligned} \tilde{f}(s) &= 1 - s MTTF + o(s), & \tilde{f}_A(s) &= 1 - s E[\tau_0] + o(s), \\ \tilde{g}(s) &= 1 - s MTTR + o(s), & \tilde{g}_A(s) &= 1 - s E[\tau'_0] + o(s), \end{aligned} \quad (6.54)$$

with $o(s)$ as per Eq. (A7.89) and using Eq. (A7.50). When considering $\tilde{g}(\lambda)$ for availability calculations, the approximation given by Eq. (6.54) often leads to $PA_S = 1$, already by simple redundancy structures. In these cases, Eq. (6.113) has to be used.

In the case of *constant failure & repair rates* ($\lambda(x) = \lambda$, $\mu(x) = \mu$) Eq. (6.42) yields (Eq. (A7.50), Table A9.7)

$$PA_S(t) = \frac{\mu}{\lambda + \mu} + \left(p - \frac{\mu}{\lambda + \mu} \right) e^{-(\lambda + \mu)t} = PA_S + (p - PA_S) e^{-(\lambda + \mu)t}. \quad (6.55)$$

Thus, for this important case, the convergence of $PA_S(t)$ toward $PA_S = \mu / (\lambda + \mu)$ is *exponential* with a time constant $1 / (\lambda + \mu) < 1 / \mu = MTTR$. In particular, for $p = 1$,

i. e. for $PA_S(0) = 1$ and $PA_S(t) \equiv PA_{S0}(t)$, it follows that

$$PA_{S0}(t) - PA_S = \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t} \leq \frac{\lambda}{\mu} e^{-\mu t} = \lambda MTTR e^{-t/MTTR}. \quad (6.56)$$

Generalizing the distribution function $G(x)$ of the repair time and/or $F(x)$ of the failure-free time, $PA_{S0}(t)$ can oscillate damped (as in general for the renewal density $h(t)$ given by Eq. (A7.18)). However, for *constant failure rate* λ and providing $\lambda MTTR$ sufficiently small and some rather weak conditions on the density $g(x)$, lower and upper bounds on $PA_{S0}(t)$ can be found [6.25]

$$PA_{S0}(t) \geq \frac{1}{1 + \lambda MTTR} - c_l \frac{\lambda MTTR}{1 + \lambda MTTR} e^{-(\lambda + 1/MTTR)t}, \quad t \geq 0$$

and

$$PA_{S0}(t) \leq \frac{1}{1 + \lambda MTTR} + c_u \frac{\lambda MTTR}{1 + \lambda MTTR} e^{-(\lambda + 1/MTTR)t}, \quad t \geq 0.$$

$c_l=1$ holds for many practical applications ($\lambda MTTR \ll 0.1$). Sufficient conditions for $c_u=1$ are given in [6.25]. However, conditions on c_u are less important as on c_l , since $PA_{S0}(t) \leq 1$ is always true. The case of a *gamma distribution* with density $g(x) = \alpha^\beta x^{\beta-1} e^{-\alpha x} / \Gamma(\beta)$, mean β/α , and shape parameter $\beta \geq 3$, leads for instance to $|PA_{S0}(t) - PA_S| \leq \lambda MTTR e^{-t/MTTR}$ at least for $t \geq 3 MTTR = 3\beta/\alpha$.

6.2.5 Steady-State Behavior

For

$$p = \frac{MTTF}{MTTF + MTTR}, \quad F_A(x) = \frac{1}{MTTF} \int_0^x (1 - F(y)) dy, \quad G_A(x) = \frac{1}{MTTR} \int_0^x (1 - G(y)) dy \quad (6.57)$$

as *initial conditions/distribution* at $t=0$, the *alternating renewal process* describing the time behavior of a *one-item repairable structure* is *stationary* (in *steady-state*), see Appendix A7.3. With p , $F_A(t)$, and $G_A(t)$ as per Eq. (6.57), the expressions for the point availability (6.42), average availability (6.43), interval reliability (6.44), joint availability (6.45), and the distribution functions of the forward recurrence times (6.46) & (6.47) take the values given by Eqs. (6.48)-(6.53) for all $t \geq 0$, see Example 6.4 for the point availability PA_S . This relationship between asymptotic & steady-state (stationary) behavior is important in practical applications because it allows the following interpretation (see also remarks on pp. 472 & 477):

A one-item repairable structure is in steady-state (stationary behavior) if it began operating at the time $t = -\infty$ and will be considered only for $t \geq 0$, the time $t = 0$ being an arbitrary time point.

Table 6.4 Results for a repairable one-item in asymptotic & steady-state (stationary) behavior

	Failure and repair rates		Remarks, assumptions
	Arbitrary	Constant *	
1. $\Pr\{up \text{ at } t = 0\}$ (p)	$\frac{MTTF}{MTTF + MTTR}$	$\frac{\mu}{\lambda + \mu}$	$MTTF = E[\tau_i], \quad i \geq 1$ $MTTR = E[\tau'_i], \quad i \geq 1$
2. Distribution of τ_0 ($F_A(x) = \Pr\{\tau_0 \leq x\}$)	$\frac{1}{MTTF} \int_0^t (1 - F(x)) dx$	$1 - e^{-\lambda t}$	$F_A(x)$ is also the distribution function of $\tau_{Ru}(t)$ as in Fig. 6.3 ($F_A(x) = \Pr\{\tau_{Ru}(t) \leq x\}$)
3. Distribution of τ'_0 ($G_A(x) = \Pr\{\tau'_0 \leq x\}$)	$\frac{1}{MTTR} \int_0^t (1 - G(x)) dx$	$1 - e^{-\mu t}$	$G_A(x)$ is also the distribution function of $\tau_{Rd}(t)$ as in Fig. 6.3 ($G_A(x) = \Pr\{\tau_{Rd}(t) \leq x\}$)
4. Renewal densities $h_{ud}(t) = h_{du}(t)$, (i. e. failure frequency = repair frequency)	$\frac{1}{MTTF + MTTR}$	$\frac{\lambda \mu}{\lambda + \mu}$	$h_{du}(t) = p h_{duu}(t) + (1-p) h_{dud}(t)$, $h_{ud}(t) = p h_{udu}(t) + (1-p) h_{udd}(t)$, p as in point 1 $\rightarrow h_{du}(t) = h_{ud}(t)$
5. Point availability (PA_S)	$\frac{MTTF}{MTTF + MTTR}$	$\frac{\mu}{\lambda + \mu}$	$PA_S = \Pr\{up \text{ at } t\}, \quad t \geq 0$
6. Average availability (AA_S)	$\frac{MTTF}{MTTF + MTTR}$	$\frac{\mu}{\lambda + \mu}$	$AA_S = \frac{1}{t} E[\text{total up time in } (0, t)],$ $t > 0$
7. Interval reliability ($IR_S(\theta)$)	$\frac{\int_0^\infty (1 - F(x)) dx}{MTTF + MTTR}$	$\frac{\mu}{\lambda + \mu} e^{-\lambda \theta}$	$IR_S(\theta) = \Pr\{up \text{ in } [t, t + \theta]\},$ $t \geq 0$
8. Joint availability ($JA_S(\theta)$)	$\frac{MTTF \cdot PA_{S0e}(\theta)}{MTTF + MTTR}$ $= PA \cdot PA_{S0e}(\theta)$	$\frac{\mu}{\lambda + \mu} \left(\frac{\mu}{\lambda + \mu} + \frac{\lambda e^{-(\lambda + \mu)\theta}}{(\lambda + \mu)} \right)$	$JA_S(\theta) = \Pr\{up \text{ at } t \cap up \text{ at } t + \theta\},$ $PA_{S0e}(\theta) = PA_S(\theta)$ as per Eq. (6.42) with $p = 1$ and $F_A(t)$ as in point 2

λ = failure, μ = repair rate; up = operating state; * Markov process

For constant failure rate λ and repair rate μ , the convergence of $PA_{S0}(t)$ to PA_S is exponential with time constant $\approx 1/\mu = MTTR$ (Eqs. (6.20) & (6.55)). Extrapolating the results of Section 6.2.4, one can assume that for practical applications, the function $PA_{S0}(t)$ is captured at least for some $t > t_0 > 0$ in the band $|PA_{S0}(t) - PA_S| \approx \lambda MTTR e^{-t/MTTR}$ when generalizing the distribution function of repair times. Thus,

for practical purposes one can assume that after a time $t \approx 10 MTTR$, the point availability $PA_{S0}(t)$ has reached its steady-state (stationary) value $PA_S = AA_S$

(this, considering $e^{-10} \approx 5 \cdot 10^{-5}$ and $\lambda MTTR \leq 10^{-2}$, see Tab. 6.3). Important results for the steady-state behavior of a repairable one-item structure are in Table 6.4.

Example 6.4

Show that for a repairable one-item structure in steady-state, i.e. with p , $F_A(x)$, and $G_A(x)$ as per Eq. (6.57), the point availability is $PA_S(t) = PA_S = MTTF / (MTTF + MTTR)$ for all $t \geq 0$.

Solution

Applying the Laplace transform to Eq. (6.42) and using Eqs. (A7.50) and (6.57) yields

$$\begin{aligned} \tilde{P}A_S(s) = & \frac{MTTF}{MTTF + MTTR} \left(\frac{1}{s} - \frac{1 - \tilde{f}(s)}{s^2 MTTF} + \frac{\frac{1 - \tilde{f}(s)}{s} \tilde{g}(s)}{1 - \tilde{f}(s) \tilde{g}(s)} \cdot \frac{1 - \tilde{f}(s)}{s} \right) \\ & + \frac{MTTR}{MTTF + MTTR} \cdot \frac{\frac{1 - \tilde{g}(s)}{s} MTTF}{1 - \tilde{f}(s) \tilde{g}(s)} \cdot \frac{1 - \tilde{f}(s)}{s}, \end{aligned}$$

and finally

$$\tilde{P}A_S(s) = \frac{MTTF}{MTTF + MTTR} \left(\frac{1}{s} - \frac{1 - \tilde{f}(s)}{s^2 MTTF} \right) + \frac{[1 - \tilde{f}(s)][\tilde{g}(s) - \tilde{f}(s) \tilde{g}(s) + 1 - \tilde{g}(s)]}{s^2 (MTTF + MTTR) [1 - \tilde{f}(s) \tilde{g}(s)]},$$

from which

$$\tilde{P}A_S(s) = \frac{MTTF}{MTTF + MTTR} \cdot \frac{1}{s} = \frac{PA_S}{s}.$$

and thus $PA_S(t) = PA_S$ for all $t \geq 0$.

6.3 Systems without Redundancy

The reliability block diagram of a *system without redundancy* (series structure, series model) consists of the series connection of all its elements E_1, \dots, E_n , see Fig. 6.4. Each element E_i in Fig. 6.4 is characterized by the distribution functions $F_i(x)$ for the failure-free time and $G_i(x)$ for the repair time.⁺⁾

6.3.1 Series Structure with Constant Failure and Repair Rates

In this section, *constant* failure and repair rates are assumed, i.e.

$$F_i(x) = 1 - e^{-\lambda_i x}, \quad x > 0, \quad F_i(0) = 0, \quad (6.58)$$

and

$$G_i(x) = 1 - e^{-\mu_i x}, \quad x > 0, \quad G_i(0) = 0, \quad (6.59)$$

⁺⁾ It can be noted that for a series structure, assumption (6.2) of *no further failures at system down* implies also assumption (6.3) of *only one repair crew*.

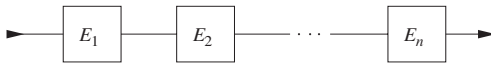


Figure 6.4 Reliability block diagram for a system without redundancy (series structure)

holds for $i = 1, \dots, n$. Because of Eqs. (6.58) and (6.59), the stochastic behavior of the system is described by a time-homogeneous *Markov process*. Let Z_0 be the system up state and Z_i the state in which element E_i is down. Taking assumption (6.2) into account, i. e. of *no further failures at system down*, the corresponding *diagram of transition probabilities* in $(t, t+\delta t]$ (p. 487) is given in Fig. 6.5. Equations of Table 6.2 can be used to obtain the expressions for the reliability function, point availability and interval reliability. With $U = \{Z_0\}$, $\bar{U} = \{Z_1, \dots, Z_n\}$ and the transition rates according to Fig. 6.5, the *reliability function* (see Table 6.2 for notation) follows from

$$R_{S0}(t) = e^{-\lambda_S t}, \quad \text{with} \quad \lambda_S = \sum_{i=1}^n \lambda_i, \quad (6.60)$$

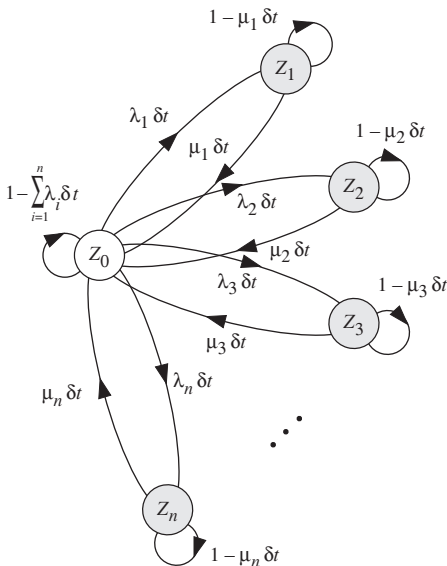


Figure 6.5 Diagram of the transition probabilities in $(t, t+\delta t]$ for a *repairable series structure* with constant failure & repair rates λ_i, μ_i , ideal failure detection & switch, no further failures at system down (Z_1, \dots, Z_n down states (absorbing for reliability calculation), arbitrary $t, \delta t \downarrow 0$, Markov process)

and thus, for the *mean time to failure*,

$$MTTF_{S0} = \frac{1}{\lambda_S}. \quad (6.61)$$

The *point availability* is given by

$$PA_{S0}(t) = P_{00}(t), \quad (6.62)$$

with $P_{00}(t)$ from (Table 6.2)

$$P_{00}(t) = e^{-\lambda_S t} + \sum_{i=1}^n \int_0^t \lambda_i e^{-\lambda_S x} P_{i0}(t-x) dx$$

$$P_{i0}(t) = \int_0^t \mu_i e^{-\mu_i x} P_{00}(t-x) dx, \quad i = 1, \dots, n, \quad (6.63)$$

yielding for the Laplace transform (Table A9.7) of $PA_{S0}(t)$

$$\tilde{P}A_{S0}(s) = \tilde{P}_{00}(s) = \frac{1}{s(1 + \sum_{i=1}^n \frac{\lambda_i}{s + \mu_i})}. \quad (6.64)$$

From Eq. (6.64) there follows the *asymptotic & steady-state* value of the *point and average availability* $PA_S = AA_S = \lim_{s \rightarrow 0} s PA_S(s)$

$$PA_S = AA_S = \frac{1}{1 + \sum_{i=1}^n \frac{\lambda_i}{\mu_i}} \approx 1 - \sum_{i=1}^n \frac{\lambda_i}{\mu_i}. \quad (6.65)$$

Because of the *constant* failure rate of all elements, the *interval reliability* can be directly obtained from Eq. (6.27) by

$$IR_{S0}(t, t+\theta) = PA_{S0}(t) e^{-\lambda_S \theta}, \quad (6.66)$$

with the asymptotic & steady-state value

$$IR_S(\theta) = PA_S e^{-\lambda_S \theta}, \quad (6.67)$$

where (Eq. (6.60))

$$\lambda_S = \sum_{i=1}^n \lambda_i.$$

6.3.2 Series Structure with Constant Failure and Arbitrary Repair Rates

Generalization of the repair time distribution functions $G_i(x)$, with densities $g_i(x)$ and $G_i(0) = 0$, leads to a *semi-Markov process* with state space Z_0, \dots, Z_n , as in Fig. 6.5 (this because of Assumption (6.2) of no further failures at system down). The *reliability function* and the *mean time to failure* are still given by Eqs. (6.60) and (6.61). For the *point availability* let us first calculate the *semi-Markov transition probabilities* $Q_{ij}(x)$ using Table 6.2

$$\begin{aligned} Q_{0i}(x) &= \Pr\{\tau_{0i} \leq x \cap \tau_{0k} > \tau_{0i}, \quad k \neq i\} \\ &= \int_0^x \lambda_i e^{-\lambda_i y} \prod_{k \neq i} e^{-\lambda_k y} dy = \frac{\lambda_i}{\lambda_S} (1 - e^{-\lambda_S x}), \quad i = 1, \dots, n, \\ Q_{i0}(x) &= G_i(x), \quad i = 1, \dots, n. \end{aligned} \quad (6.68)$$

The system of integral Equations for the *transition probabilities* $P_{ij}(t)$ follows then from Table 6.2

$$\begin{aligned} P_{00}(t) &= e^{-\lambda_S t} + \sum_{i=1}^n \int_0^t \lambda_i e^{-\lambda_S x} P_{i0}(t-x) dx, \\ P_{i0}(t) &= \int_0^t g_i(x) P_{00}(t-x) dx, \quad i = 1, \dots, n. \end{aligned} \quad (6.69)$$

For the Laplace transform of the *point availability* $PA_{S0}(t) = P_{00}(t)$ one obtains finally, from Eq. (6.69),

$$\tilde{P}A_{S0}(s) = \tilde{P}_{00}(s) = \frac{1}{s + \lambda_S - \sum_{i=1}^n \lambda_i \tilde{g}_i(s)} = \frac{1}{s + \sum_{i=1}^n \lambda_i (1 - \tilde{g}_i(s))}, \quad (6.70)$$

from which, the *asymptotic & steady-state value* of the *point* and *average availability*

$$PA_S = AA_S = \frac{1}{1 + \sum_{i=1}^n \lambda_i MTTR_i}, \quad (6.71)$$

obtained using $\lim_{s \rightarrow 0} (1 - \tilde{g}(s)) = s \cdot MTTR$, as per Eq. (6.54), and (Eq. (A6.38))

$$MTTR_i = \int_0^{\infty} (1 - G_i(t)) dt. \quad (6.72)$$

The *interval reliability* can be calculated from Eq. (6.66), with $PA_{S0}(t)$ per Eq. (6.70), or Eq. (6.67) with PA_S per Eq. (6.71), see Example 6.5 for an application.

Example 6.5

A system consists of elements E_1 to E_4 which are necessary for the fulfillment of the required function (series structure). Let the failure rates $\lambda_1 = 10^{-3} \text{h}^{-1}$, $\lambda_2 = 0.5 \cdot 10^{-3} \text{h}^{-1}$, $\lambda_3 = 10^{-4} \text{h}^{-1}$, $\lambda_4 = 2 \cdot 10^{-3} \text{h}^{-1}$ be constant and assume that for all elements the repair time is lognormally distributed with parameters $\lambda = 0.5 \text{h}^{-1}$ and $\sigma = 0.6$. Assuming that no further failures can occur at system down (failures during repair are not considered), give the reliability function for a mission of duration $t = 168 \text{h}$, the mean time to failure, the asymptotic & steady-state values of the point and average availability, and the asymptotic & steady-state values of the interval reliability for $\theta = 12 \text{h}$.

Solution

The system failure rate is $\lambda_S = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 36 \cdot 10^{-4} \text{h}^{-1}$, according to Eq. (6.60). The reliability function follows as $R_{S0}(t) = e^{-0.0036t}$, from which $R_{S0}(168 \text{h}) \approx 0.55$. The mean time to failure is $MTTF_{S0} = 1/\lambda_S \approx 278 \text{h}$. The mean time to repair is obtained from Table A6.1 as $E[\tau] = (e^{\sigma^2/2})/\lambda = MTTR \approx 2.4 \text{h}$. For the asymptotic & steady-state values of the point and average availability as well as for the interval reliability for $\theta = 12 \text{h}$ it follows from Eqs. (6.71) and (6.67) that $PA_S = AA_S = 1/(1 + 36 \cdot 10^{-4} \cdot 2.4) \approx 0.991$ and $IR_S(12) \approx 0.991 \cdot e^{-0.0036 \cdot 12} \approx 0.95$.

6.3.3 Series Structure with Arbitrary Failure and Repair Rates

Generalization of repair and failure-free time distribution functions leads to a *nonregenerative stochastic process*. This model can be investigated using supplementary variables, or by approximating the distribution functions of the failure-free time in such a way that the involved stochastic process can be reduced to a regenerative process. Using for the approximation an *Erlang distribution function* leads to a semi-Markov process. As an example, let us consider the case of a two-element series structure (E_1, E_2) and assume that the repair times are arbitrary, with densities $g_1(x)$ and $g_2(x)$, and the failure-free times have densities

$$f_1(x) = \lambda_1^2 x e^{-\lambda_1 x}, \quad x > 0, \quad f_1(0) = 0, \quad (6.73)$$

and

$$f_2(x) = \lambda_2 e^{-\lambda_2 x}, \quad x > 0, \quad f_2(0) = 0. \quad (6.74)$$

Equation (6.73) is the density of the sum of two exponentially distributed random time intervals with density $\lambda_1 e^{-\lambda_1 x}$. Under these assumptions, the two-element series structure corresponds to a *1-out-of-2 standby redundancy* ($E_1, E_{1'}$) with constant failure rate λ_1 and *repair only at the failure of both elements* E_1 and $E_{1'}$, in series with an element (E_2) with constant failure rate λ_2 . Figure 6.6 gives the equivalent reliability block diagram and the corresponding *state transition diagram*. This diagram only *visualizes* the possible transitions. Z_0 and $Z_{1'}$ are the system up states, $Z_{1'}$ and $Z_{2'}$ are *supplementary states* necessary for calculation. For the

semi-Markov transition probabilities $Q_{ij}(x)$ one obtains (Table 6.2, Fig. 6.6)

$$\begin{aligned}
 Q_{01'}(x) = Q_{1'1}(x) &= \int_0^x \lambda_1 e^{-\lambda_1 y} e^{-\lambda_2 y} dy = \frac{\lambda_1}{\lambda_1 + \lambda_2} (1 - e^{-(\lambda_1 + \lambda_2)x}), \\
 Q_{02}(x) = Q_{1'2}(x) &= \frac{\lambda_2}{\lambda_1 + \lambda_2} (1 - e^{-(\lambda_1 + \lambda_2)x}), \\
 Q_{20}(x) = Q_{2'1'}(x) &= \int_0^x g_2(y) dy, \\
 Q_{10}(x) &= \int_0^x g_1(y) dy.
 \end{aligned} \tag{6.75}$$

From Eq. (6.75) it follows that (Tables 6.2 & A9.7, and Eq. (6.54) for $PA_S = AA_S$)

$$R_{S0}(t) = (1 + \lambda_1 t) e^{-\lambda_1 t} e^{-\lambda_2 t} = (1 + \lambda_1 t) e^{-(\lambda_1 + \lambda_2)t}, \tag{6.76}$$

$$MTTF_{S0} = \frac{2\lambda_1 + \lambda_2}{(\lambda_1 + \lambda_2)^2}, \tag{6.77}$$

$$\tilde{P}A_{S0}(s) = \tilde{P}_{00}(s) + \tilde{P}_{01'}(s) = \frac{[s + \lambda_1 + \lambda_2(1 - \tilde{g}_2(s))] + \lambda_1}{[s + \lambda_1 + \lambda_2(1 - \tilde{g}_2(s))]^2 - \lambda_1^2 \tilde{g}_1(s)}, \tag{6.78}$$

$$PA_S = AA_S = \frac{2}{2 + 2\lambda_2 MTTR_2 + \lambda_1 MTTR_1}, \tag{6.79}$$

$$IR_S(\theta) = \frac{(2 + \lambda_1 \theta) e^{-(\lambda_1 + \lambda_2)\theta}}{2 + 2\lambda_2 MTTR_2 + \lambda_1 MTTR_1}. \tag{6.80}$$

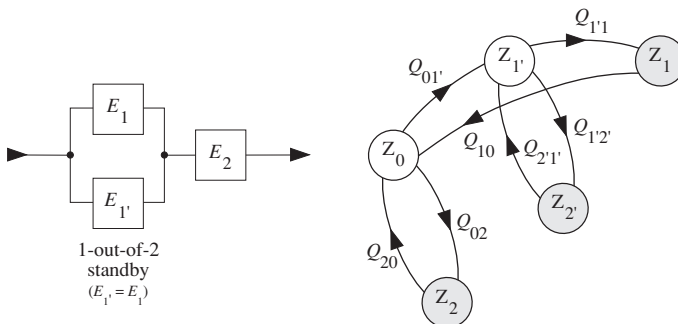


Figure 6.6 Equivalent reliability block diagram and state transition diagram for a two series element system (E_1 and E_2) with arbitrarily distributed repair times, constant failure rate for E_2 , and Erlangian ($n = 2$) distributed failure-free time for E_1 (ideal failure detection & switch, repair of E_1 and $E_{1'}$ only at the failure of both E_1 and $E_{1'}$ (state Z_1), no further failures at system down Z_1, Z_2, Z_2' , down states (absorbing for reliability calculation), semi-Markov process)

The *interval reliability* $IR_{S0}(t, t + \theta)$ can be obtained from

$$IR_{S0}(t, t + \theta) = P_{00}(t)R_{S0}(\theta) + P_{01}(t)R_{S1}(\theta),$$

with $R_{S1}(\theta) = e^{-(\lambda_1 + \lambda_2)\theta}$, and $R_{S0}(\theta)$ per Eq. (6.76) with θ instead of t .

Important results for repairable series structures are summarized in Table 6.5. Asymptotic results for arbitrary failure and repair rates are investigated e.g. in [2.34 (1975)] yielding $AA_S = PA_S = 1 / (1 + \sum_{i=1}^n MTTR_i / MTF_i) \approx 1 - \sum_{i=1}^n MTTR_i / MTF_i$ for the asymptotic & steady-state value of the point and average availability (Point 4 of Table 6.5). $AA_S = PA_S = 1 / (1 + \sum_{i=1}^n MTTR_i / MTF_i)$ follows also in a way similar to the development of Eq. (4.6).

Table 6.5 Results for a *repairable system without redundancy* (elements E_1, \dots, E_n in series), ideal failure detection & switch, *no further failures at system down*

Quantity	Expression	Remarks, assumptions
1. Reliability function ($R_{S0}(t)$)	$\prod_{i=1}^n R_i(t)$	Independent elements (up to system failure), $R_i(0) = 1, i = 1, \dots, n$
2. Mean time to system failure ($MTTF_{S0}$)	$\int_0^\infty R_{S0}(t) dt$	$R_i(t) = e^{-\lambda_i t} \rightarrow R_{S0}(t) = e^{-\lambda_S t}$ and $MTTF_{S0} = 1 / \lambda_S$ with $\lambda_S = \lambda_1 + \dots + \lambda_n$
3. System failure rate up to system failure ($\lambda_S(t)$)	$\sum_{i=1}^n \lambda_i(t)$	Independent elements (up to system failure)
4. Asymptotic & steady-state value of the point availability & average availability ($PA_S = AA_S$)	a) $\frac{1}{1 + \sum_{i=1}^n \frac{\lambda_i}{\mu_i}} \approx 1 - \sum_{i=1}^n \frac{\lambda_i}{\mu_i} *$ b) $\frac{1}{1 + \sum_{i=1}^n \lambda_i MTTR_i} \approx 1 - \sum_{i=1}^n \lambda_i MTTR_i$ c) $\frac{1}{1 + \lambda_2 MTTR_2 + \lambda_1 MTTR_1 / 2}$	At system down, no further failures can occur: a) Constant failure & repair rates λ_i & μ_i for element E_i ($i = 1, \dots, n$) (Fig. 6.5) b) Constant failure rate λ_i and arbitrary repair rate $\mu_i(x)$ with $MTTR_i =$ mean time to repair for element E_i ($i = 1, \dots, n$) c) 2-element series structure with failure rates $\lambda_i^2 x / (1 + \lambda_i x)$ for E_1 and λ_2 for E_2 , arbitrary repair rates (Fig. 6.6)
5. Asymptotic & steady-state value of the interval reliability ($IR_S(\theta)$)	$PA_S e^{-\lambda_S \theta}$	Each element has constant failure rate $\lambda_i, \lambda_S = \lambda_1 + \dots + \lambda_n$

* **Supplementary results:** For *totally independent elements* (n repair crews and possible failures also at system down) it holds that (Table 6.9) $PA_S = \prod_i (1 / (1 + \lambda_i / \mu_i)) \approx 1 - \sum_i \lambda_i / \mu_i$.

6.4 1-out-of-2 Redundancy (Warm, one Repair Crew)

The *1-out-of-2 redundancy*, also known as *1-out-of-2: G*, is the simplest redundant structure arising in practical applications. It consists of two elements E_1 and E_2 , one of which is in the operating state and the other in reserve, when not under repair or waiting for repair. When a failure occurs, one element is repaired while the other continues operation. The system is down when an element fails while the other one is being repaired (assumption (6.2) is thus here automatically satisfied). Assuming ideal *failure detection* and *switching*, the reliability block diagram is a parallel connection of elements E_1 and E_2 , see Fig. 6.7.

Investigations are based on assumptions (6.1)–(6.7). This implies, in particular,, that repair of a redundant element *begins at failure occurrence and is performed without interruption of operation at system level*. Distribution functions of repair and failure-free times are generalized step by step, beginning with exponential, up to the case in which the process involved has only *one regeneration state*. Influence of preventive maintenance, switching, incomplete coverage, common cause failures are considered in Section 6.8, travel time in Example 6.7 (pp. 203-204) and Fig. A7.12.

6.4.1 1-out-of-2 Redundancy with Constant Failure and Repair Rates

Because of the constant failure and repair rates, the time behavior of the 1-out-of-2 redundancy can be described by a time-homogeneous *Markov process*. The number of states is 3 if elements E_1 and E_2 are identical (Figs. 6.8 or A7.4a) and 5 if they are different (Figs. 6.9 or A7.4b, see also the footnote on p. 487); the diagrams of transition probabilities in $(t, t+\delta t]$ are in Figs. 6.8 and 6.9, or A7.4, respectively.

Let us consider the case of identical elements E_1 and E_2 (see Example 6.6 for different elements) and assume as distribution function of the failure-free time

$$F(x) = 1 - e^{-\lambda x}, \quad x > 0, \quad F(0) = 0, \quad (6.81)$$

in the *operating state* and

$$F_r(x) = 1 - e^{-\lambda_r x}, \quad x > 0, \quad F_r(0) = 0, \quad (6.82)$$

in the *reserve state*. This includes *active* (parallel) redundancy for $\lambda_r = \lambda$, *warm* redundancy for $\lambda_r < \lambda$, and *standby* redundancy for $\lambda_r \equiv 0$. Repair times are assumed

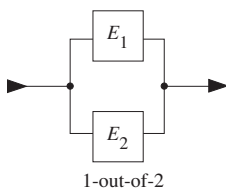


Figure 6.7 1-out-of-2 redundancy reliability block diagram (for ideal failure detection and switch)

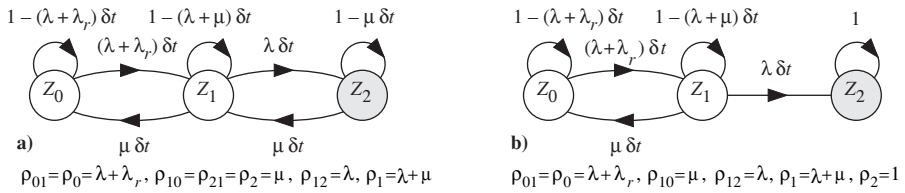


Figure 6.8 Diagrams of the transition probabilities in $(t, t + \delta t]$ for a *repairable 1-out-of-2 warm redundancy with two identical elements, constant failure and repair rates $(\lambda, \lambda_r, \mu)$, ideal failure detection & switch, one repair crew $(Z_2$ down state, arbitrary $t, \delta t \downarrow 0$, Markov process (see footnote on p. 497))* **a)** For the point availability; **b)** For the reliability function (Z_2 absorbing state)

to be independent of failure-free times and distributed according to

$$G(x) = 1 - e^{-\mu x}, \quad x > 0, \quad G(0) = 0. \tag{6.83}$$

Refinements are in Examples 6.6 (different elements) and 6.7 (travel time). For more general situations (particular load sharing, more repair crews, failure and/or repair rates changing at a state transition, etc.), *birth and death processes* (Appendix A7.5.5) can often be used. For all these cases, investigations are generally performed using the *method of differential equations* (Table 6.2 and Appendix A7.5.3.1). Figure 6.8 gives the *diagram of transition probabilities* in $(t, t + \delta t]$ for the point availability (Fig. 6.8a) and the reliability function (Fig. 6.8b), respectively.

Considering the *memoryless property* of exponential distributions (Eq. (A6.87)), the system behavior at times t and $t + \delta t$ can be described by following *difference equations* for the *state probabilities* $P_i(t) \equiv \Pr\{\text{process in } Z_i \text{ at } t\}$, $i = 0, 1, 2$ (Fig. 6.8a)

$$\begin{aligned} P_0(t + \delta t) &= P_0(t)(1 - (\lambda + \lambda_r)\delta t) + P_1(t)\mu\delta t \\ P_1(t + \delta t) &= P_1(t)(1 - (\lambda + \mu)\delta t) + P_0(t)(\lambda + \lambda_r)\delta t + P_2(t)\mu\delta t \\ P_2(t + \delta t) &= P_2(t)(1 - \mu\delta t) + P_1(t)\lambda\delta t. \end{aligned}$$

For $\delta t \downarrow 0$, it follows that

$$\begin{aligned} \dot{P}_0(t) &= -(\lambda + \lambda_r)P_0(t) + \mu P_1(t) \\ \dot{P}_1(t) &= -(\lambda + \mu)P_1(t) + (\lambda + \lambda_r)P_0(t) + \mu P_2(t) \\ \dot{P}_2(t) &= -\mu P_2(t) + \lambda P_1(t). \end{aligned} \tag{6.84}$$

The system of differential equations (6.84) can also be obtained directly from Table 6.2 and Fig. 6.8a. Its solution leads to the state probabilities $P_i(t)$, $i = 0, 1, 2$. Assuming as *initial conditions* at $t = 0$, $P_0(0) = 1$ and $P_1(0) = P_2(0) = 0$, the above state probabilities are identical to the *transition probabilities* $P_{0i}(t)$, $i = 0, 1, 2$, i.e., $P_{00}(t) \equiv P_0(t)$, $P_{01}(t) \equiv P_1(t)$, and $P_{02}(t) \equiv P_2(t)$. The *point availability* $PA_{S0}(t)$ is then given by (see Table 6.2 for notation)

$$PA_{S0}(t) = P_{00}(t) + P_{01}(t). \tag{6.85}$$

$PA_{S1}(t)$ or $PA_{S2}(t)$ could have been determined for suitable initial conditions.

From Eq. (6.85) it follows for the Laplace transform of $PA_{S0}(t)$ that

$$\tilde{P}A_{S0}(s) = \tilde{P}_{00}(s) + \tilde{P}_{01}(s) = \frac{((s + \mu)^2 + s\lambda) + (s + \mu)(\lambda + \lambda_r)}{s[(s + \lambda + \lambda_r)(s + \lambda + \mu) + \mu(s + \mu)]}, \quad (6.86)$$

and thus for $t \rightarrow \infty$ (Table A9.7)

$$\lim_{t \rightarrow \infty} PA_{S0}(t) = PA_S = P_0 + P_1 = \frac{\mu^2 + \mu(\lambda + \lambda_r)}{(\lambda + \lambda_r)(\lambda + \mu) + \mu^2} \approx 1 - \frac{\lambda(\lambda + \lambda_r)}{\mu^2}, \quad (6.87)$$

with $P_i = \lim_{t \rightarrow \infty} P_i(t) = \lim_{t \rightarrow \infty} P_{ji}(t)$, $i, j = 0, 1, 2$ (Eq. (A7.129)). If $PA_{S0}(t) = PA_S$ for $t \geq 0$, then $PA_S = AA_S$ is also the *point & average availability in steady-state*. Obviously, $P_2 = 1 - PA_S$. Investigation of $PA_{S0}(t)$ for $\lambda_r = \lambda$ leads to (Eq. (6.86), Tab. A9.7)

$$PA_{S0}(t) = PA_S + 2\lambda^2 (a_2 e^{a_1 t} - a_1 e^{a_2 t}) / a_1 a_2 (a_2 - a_1),$$

with

$$a_{1,2} = -\mu (1 + 3\lambda / 2\mu) \pm \mu \sqrt{\lambda / \mu + (\lambda / 2\mu)^2} \approx -\mu (1 \mp \sqrt{\lambda / \mu}),$$

and PA_S per Eq.(6.87). Using $a_1 a_2 = \mu^2 + 2\lambda\mu + 2\lambda^2$, it follows that $PA_{S0}(0) = 1$. Furthermore, $dPA_{S0}(t)/dt = 0$ at $t = 0$, yielding $PA_{S0}(t) = 1$ for some t ,⁺ and $a_{1,2} \rightarrow -\mu$ for $\lambda \rightarrow 0$. From these results, and considering $\lambda \ll \mu$, following approximation can be used for practical applications ($e^{a_1 t} \approx e^{a_2 t} \approx e^{-\mu t}$, $a_1 a_2 \approx \mu^2$)

$$PA_{S0}(t) \approx PA_S + (1 - PA_S) e^{-\mu t}, \quad t > 0, \quad PA_{S0}(0) = 1. \quad (6.88)$$

Equation (6.88) is similar to Eq.(6.20); it holds also for $0 \leq \lambda_r \leq \lambda$ and is an important result in developing, with Eq.(6.94), approximate expressions for large series-parallel systems, based on macro-structures (Table 6.10).

To calculate the *reliability function* it is necessary to consider that the 1-out-of-2 redundancy will operate failure free in $(0, t]$ only if in this time interval the *down state at system level* (state Z_2) will *not be visited*. To recognize if Z_2 has been entered before t it is sufficient to make Z_2 *absorbing* (Fig. 6.8b). In this case, if Z_2 is entered the process *remains there indefinitely*. Thus, *the probability of being in Z_2 at t is the probability of having entered Z_2 before the time t* , i. e. the unreliability $1 - R_S(t)$. To avoid ambiguities, the *state probabilities* in Fig. 6.8b are marked by an *apostrophe* (prime). The procedure is similar to that for Eq. (6.84) and leads to

$$\begin{aligned} \dot{P}'_0(t) &= -(\lambda + \lambda_r)P'_0(t) + \mu P'_1(t) \\ \dot{P}'_1(t) &= -(\lambda + \mu)P'_1(t) + (\lambda + \lambda_r)P'_0(t) \\ \dot{P}'_2(t) &= \lambda P'_1(t), \end{aligned} \quad (6.89)$$

and to the corresponding state probabilities $P'_0(t)$, $P'_1(t)$, and $P'_2(t)$. With the *initial*

⁺ More precisely, $PA_{S0}(t) \approx 1 - \lambda^2 t^2$ for $t \downarrow 0$, using $e^x \approx 1 + x + x^2/2$ (further approximations are possible for particular values of λ, μ ; however, Eqs.(6.88)&(6.94) better agree for macro-structures).

conditions at $t=0$, $P_0'(0)=1$ and $P_1'(0)=P_2'(0)=0$, the state probabilities $P_0'(t)$, $P_1'(t)$ and $P_2'(t)$ are identical to the transition probabilities $P_{00}'(t) \equiv P_0'(t)$, $P_{01}'(t) \equiv P_1'(t)$ and $P_{02}'(t) \equiv P_2'(t)$. The reliability function is then given by (Table 6.2 for notation)

$$R_{S0}(t) = P_{00}'(t) + P_{01}'(t). \tag{6.90}$$

Equations (6.89) & (6.90) yield following Laplace transform for $R_{S0}(t)$

$$\tilde{R}_{S0}(s) = \frac{(s + \lambda + \mu) + (\lambda + \lambda_r)}{(s + \lambda + \lambda_r)(s + \lambda) + s\mu}, \tag{6.91}$$

from which the mean time to failure ($MTTF_{S0} = \tilde{R}_{S0}(0)$, Eq. (2.61)) follows as

$$MTTF_{S0} = \frac{2\lambda + \lambda_r + \mu}{\lambda(\lambda + \lambda_r)} \approx \frac{\mu}{\lambda(\lambda + \lambda_r)}. \tag{6.92}$$

Investigation of $R_{S0}(t)$ for $\lambda_r = \lambda$ leads to (Eq. (6.91), Table A9.7)

$$R_{S0}(t) = (r_2 e^{r_1 t} - r_1 e^{r_2 t}) / (r_2 - r_1),$$

with

$$r_{1,2} = -[(3\lambda + \mu)/2] \pm \sqrt{((3\lambda + \mu)/2)^2 - 2\lambda^2}.$$

For $\lambda \ll \mu$, it follows that $r_1 \approx -\mu$ and $r_2 \approx 0$, yielding

$$R_{S0}(t) \approx e^{\mu t}. \tag{6.93}$$

Using $\sqrt{1-\epsilon} \approx 1-\epsilon/2$ for $r_2 = -(3\lambda + \mu)(1 - \sqrt{1-8\lambda^2/(3\lambda + \mu)^2})$ leads to $r_2 \approx -2\lambda^2/(3\lambda + \mu)$. $R_{S0}(t)$ can thus be approximated by a decreasing exponential function with time constant $MTTF_{S0} \approx (3\lambda + \mu)/2\lambda^2$.⁺⁾ Considering $\lambda \ll \mu$, extension to a warm redundancy $0 \leq \lambda_r \leq \lambda$ leads to

$$R_{S0}(t) \approx e^{-\lambda_S t}, \quad t > 0, \quad R_{S0}(0) = 1, \quad \lambda_S = \frac{1}{MTTF_{S0}} = \frac{\lambda(\lambda + \lambda_r)}{2\lambda + \lambda_r + \mu} \approx \frac{\lambda(\lambda + \lambda_r)}{\mu}. \tag{6.94}$$

Similarly as for $PA_{S0}(t)$, $dR_{S0}(t)/dt = 0$ at $t=0$, and thus $R_{S0}(t) = 1$ for some t .⁺⁾

Concluding the above investigations, results of Eqs. (6.88) & (6.94) show that:

For $\lambda, \lambda_r \ll \mu$, a repairable 1-out-of-2 warm redundancy with constant failure & repair rates λ, λ_r, μ , and one repair crew, behaves approximately like a one-item structure with constant failure rate $\lambda_S \approx \lambda(\lambda + \lambda_r)/\mu$ and repair rate $\mu_S \approx \mu$; result on which the macro structures method (Tab. 6.10) can be based ($\mu_S \approx 2\mu$ for two repair crews (Tab. 6.9)).

⁺⁾ More precisely, $R_{S0}(t) \approx 1 - r_1 r_2 t^2 / 2 \approx 1 - \lambda^2 t^2 \approx PA_{S0}(t)$ for $t \downarrow 0$, using $e^x \approx 1 + x + x^2/2$.

⁺⁺⁾ This result can be extended to an arbitrary repair rate, using $MTTF_{S0}$ per Eq. (6.108).

Using Eq. (6.291), the *system mean up time* MUT_S follows as (Example 6.29)

$$MUT_S = \frac{PA_S}{f_{uds}} = \frac{P_0 + P_1}{\lambda P_1} = \frac{\mu^2 + \mu(\lambda + \lambda_r)}{\lambda\mu(\lambda + \lambda_r)} = \frac{\mu + \lambda + \lambda_r}{\lambda(\lambda + \lambda_r)} \leq MTTFS_0. \quad (6.95)$$

Considering that the return from the down state Z_2 is to the up state Z_1 (Fig. 6.8 a), it holds $MUT_S = MTTFS_1$ (Example 6.29, p. 279); furthermore, only one repair crew leads to $MDT_S = 1/\mu = MTTR$, yielding $PA_S = MUT_S / (MUT_S + MDT_S)$ as for Eq. (6.87).

Because of the *memoryless property* of the time-homogeneous Markov process, the *interval reliability* follows directly from the *transition probabilities* $P_{ij}(t)$ and the reliability functions $R_{Si}(t)$ (Table 6.2). In particular, $P_0(0) = 1$ yields

$$R_{S0}(t, t + \theta) = P_{00}(t)R_{S0}(\theta) + P_{01}(t)R_{S1}(\theta), \quad (6.96)$$

with $P_{00}(t)$, $P_{01}(t)$ as in Eq. (6.85). The asymptotic & steady-state value follows as

$$R_S(\theta) = P_0R_{S0}(\theta) + P_1R_{S1}(\theta) = \frac{\mu^2 R_{S0}(\theta) + \mu(\lambda + \lambda_r)R_{S1}(\theta)}{(\lambda + \lambda_r)(\lambda + \mu) + \mu^2} \approx R_{S0}(\theta).$$

Further results for a 1-out-of-2 redundancy are in Sections 6.8.3 (imperfect switching), 6.8.4 (incomplete coverage), and 6.8.7 (common cause failures).

To compare the effectiveness of calculation methods, let us now express the reliability function, point availability, and interval reliability using the *method of integral equations* (Appendix A7.5.3.2). Equation (A7.102) and Fig. 6.8a yield

$$\begin{aligned} Q_{01}(x) &= \Pr\{\tau_{01} \leq x\} = 1 - \Pr\{\tau_{01} > x\} = 1 - e^{-\lambda x} e^{-\lambda_r x} = 1 - e^{-(\lambda + \lambda_r)x}, \\ Q_{10}(x) &= \Pr\{\tau_{10} \leq x \cap \tau_{12} > \tau_{10}\} = \int_0^x \mu e^{-\mu y} e^{-\lambda y} dy = \frac{\mu}{\lambda + \mu} (1 - e^{-(\lambda + \mu)x}), \\ Q_{12}(x) &= \Pr\{\tau_{12} \leq x \cap \tau_{10} > \tau_{12}\} = \int_0^x \lambda e^{-\lambda y} e^{-\mu y} dy = \frac{\lambda}{\lambda + \mu} (1 - e^{-(\lambda + \mu)x}), \\ Q_{21}(x) &= \Pr\{\tau_{21} \leq x\} = 1 - e^{-\mu x}. \end{aligned}$$

From Table 6.2 it follows then that

$$\begin{aligned} R_{S0}(t) &= e^{-(\lambda + \lambda_r)t} + \int_0^t (\lambda + \lambda_r) e^{-(\lambda + \lambda_r)x} R_{S1}(t - x) dx, \\ R_{S1}(t) &= e^{-(\lambda + \mu)t} + \int_0^t \mu e^{-(\lambda + \mu)x} R_{S0}(t - x) dx, \end{aligned} \quad (6.97)$$

for the *reliability functions* $R_{S0}(t)$ and $R_{S1}(t)$, as well as

$$\begin{aligned} P_{00}(t) &= e^{-(\lambda + \lambda_r)t} + \int_0^t (\lambda + \lambda_r) e^{-(\lambda + \lambda_r)x} P_{10}(t - x) dx, & P_{20}(t) &= \int_0^t \mu e^{-\mu x} P_{10}(t - x) dx, \\ P_{10}(t) &= \int_0^t \mu e^{-(\lambda + \mu)x} P_{00}(t - x) dx + \int_0^t \lambda e^{-(\lambda + \mu)x} P_{20}(t - x) dx, \end{aligned}$$

Table 6.6 Reliability function $R_{S0}(t)$, point availability $PA_{S0}(t)$, mean time to failure $MTTF_{S0}$, and steady-state point & average availability $PA_S=AA_S$ & interval reliability $IR_S(\theta)$ for a *repairable 1-out-of-2 redundancy with two identical elements, constant failure & repair rates λ, λ_r, μ , ideal failure detection & switch, one repair crew* (Markov process, approximations valid for $(\lambda + \lambda_r) \ll \mu$)

	Standby ($\lambda_r \equiv 0$)	Warm ($\lambda_r < \lambda$)	Active ($\lambda_r = \lambda$)
$R_{S0}(t)^*$	$\approx e^{-\frac{\lambda^2 t}{2\lambda + \mu}}$	$\approx e^{-\frac{\lambda(\lambda + \lambda_r)t}{2\lambda + \lambda_r + \mu}}$	$\approx e^{-\frac{2\lambda^2 t}{3\lambda + \mu}}$
$PA_{S0}(t)^*$	$\approx PA_S + (1 - PA_S)e^{-\mu t}$	$\approx PA_S + (1 - PA_S)e^{-\mu t}$	$\approx PA_S + (1 - PA_S)e^{-\mu t}$
$MTTF_{S0}^*$	$\frac{2\lambda + \mu}{\lambda^2} \approx \frac{\mu}{\lambda^2}$	$\frac{2\lambda + \lambda_r + \mu}{\lambda(\lambda + \lambda_r)} \approx \frac{\mu}{\lambda(\lambda + \lambda_r)}$	$\frac{3\lambda + \mu}{2\lambda^2} \approx \frac{\mu}{2\lambda^2}$
$PA_S = AA_S^{**}$	$\frac{\mu(\lambda + \mu)}{\lambda(\lambda + \mu) + \mu^2}$ $\approx 1 - (\lambda/\mu)^2$	$\frac{\mu(\lambda + \lambda_r + \mu)}{(\lambda + \lambda_r)(\lambda + \mu) + \mu^2}$ $\approx 1 - \lambda(\lambda + \lambda_r)/\mu^2$	$\frac{\mu(2\lambda + \mu)}{2\lambda(\lambda + \mu) + \mu^2}$ $\approx 1 - 2(\lambda/\mu)^2$
$IR_S(\theta)^{**}$	$\approx R_{S0}(\theta)$	$\approx R_{S0}(\theta)$	$\approx R_{S0}(\theta)$

* new at $t = 0$; ** asymptotic & steady-state value (for practical applications, convergence of $PA_{S0}(t)$ to PA_S and of $IR_{S0}(t, t + \theta)$ to $IR_S(\theta)$ is good after $t \approx 10/\mu = 10$ *MTTR*, see also p. 198)

Supplementary results: See Example 6.6 for two different elements and Table 6.9 for two different elements and two repair crews (active redundancy); assuming in Fig. 6.8a $Z_2 \rightarrow Z_0$ with μ_g instead of $Z_2 \rightarrow Z_1$ with μ yields $PA_S = AA_S \approx 1 - 2\lambda^2/\mu\mu_g$ (active redundancy).

and

$$\begin{aligned}
 P_{01}(t) &= \int_0^t (\lambda + \lambda_r) e^{-(\lambda + \lambda_r)x} P_{11}(t - x) dx, & P_{21}(t) &= \int_0^t \mu e^{-\mu x} P_{11}(t - x) dx, \\
 P_{11}(t) &= e^{-(\lambda + \mu)t} + \int_0^t \mu e^{-(\lambda + \mu)x} P_{01}(t - x) dx + \int_0^t \lambda e^{-(\lambda + \mu)x} P_{21}(t - x) dx, & (6.98)
 \end{aligned}$$

for the transition probabilities. The solution of the system of integral equations (6.97) yields, in particular, Eq. (6.91) and the solution of the systems of integral equations (6.98) yields, in particular, Eq. (6.86). Equations (6.97) and (6.98) show how the use of integral equations leads to a quicker solution than differential equations, for the case of arbitrary initial conditions at $t = 0$.

Table 6.6 summarizes the main results of Section 6.4.1. It gives *approximate expressions* valid for $\lambda \ll \mu$ and distinguishes between the cases of active ($\lambda_r = \lambda$), warm ($\lambda_r < \lambda$), and standby redundancy ($\lambda_r \equiv 0$).

From Table 6.6 and Eqs. (6.15) & (6.20), the improvement in $MTTF_{S_0}$ brought by a repairable redundancy 1-out-of-2 (with ideal failure detection & switch, and *repair on line* of a redundant element) is given by

$$\frac{MTTF_{S_0 \text{ 1-out-of-2}}}{MTTF_{S_0 \text{ one item}}} \approx \begin{array}{cc} \text{active} & \text{standby} \\ \frac{\mu / 2\lambda^2}{1/\lambda} = \frac{\mu}{2\lambda} & \frac{\mu / \lambda^2}{1/\lambda} = \frac{\mu}{\lambda} \end{array}$$

(for the nonrepairable case, the gain were 1.5 & 2, respectively, Table 6.6 with $\mu=0$). Investigation of the *unavailability* in steady-state $1 - PA_S$ leads to

$$\frac{1 - PA_S \text{ 1-out-of-2}}{1 - PA_S \text{ one item}} \approx \begin{array}{cc} \text{active} & \text{standby} \\ \frac{2(\lambda / \mu)^2}{\lambda / \mu} = 2 \frac{\lambda}{\mu} & \frac{(\lambda / \mu)^2}{\lambda / \mu} = \frac{\lambda}{\mu} \end{array}$$

Above results can be extended to cover situations in which failure or repair rates are modified at *state changes*, e. g. because of *load sharing*, *differences within elements*, *repair priority*, or other. Such requirements can be introduced in the diagram of transition probabilities in $(t, t + \delta t]$, see for instance Figs.2.12, A7.4- A7.6.

Example 6.6

Give the mean time to failure $MTTF_{S_0}$ and the asymptotic & steady-state value of the point availability PA_S for a 1-out-of-2 active redundancy with two *different elements* E_1 & E_2 , constant failure and repair rates $\lambda_1, \lambda_2, \mu_1, \mu_2$ (one repair crew, ideal failure detection & switch).

Solution

Figure 6.9 gives the reliability block diagram and the diagram of transition probabilities in $(t, t + \delta t]$. $MTTF_{S_0}$ and PA_S can be calculated from appropriate systems of algebraic equations. According to Table 6.2 and considering Fig. 6.9 it follows for the *mean time to failure* that

$$MTTF_{S_0} = (1 + \lambda_1 MTTF_{S_1} + \lambda_2 MTTF_{S_2}) / (\lambda_1 + \lambda_2)$$

$$MTTF_{S_1} = (1 + \mu_1 MTTF_{S_0}) / (\lambda_2 + \mu_1), \quad MTTF_{S_2} = (1 + \mu_2 MTTF_{S_0}) / (\lambda_1 + \mu_2),$$

which leads to

$$MTTF_{S_0} = \frac{(\lambda_1 + \mu_2)(\lambda_2 + \mu_1) + \lambda_1(\lambda_1 + \mu_2) + \lambda_2(\lambda_2 + \mu_1)}{\lambda_1 \lambda_2 (\lambda_1 + \lambda_2 + \mu_1 + \mu_2)}, \quad (6.99)$$

and in particular for $\lambda_1 \ll \mu_1$ and $\lambda_2 \ll \mu_2$,

$$MTTF_{S_0} \approx \mu_1 \mu_2 / (\lambda_1 \lambda_2 (\mu_1 + \mu_2)). \quad (6.100)$$

As for Eq. (6.93), the *reliability function* can be expressed by

$$R_{S_0}(t) = e^{-\lambda_S t} \quad \text{with} \quad \lambda_S = \frac{1}{MTTF_{S_0}} \approx \frac{\lambda_1 \lambda_2 (\mu_1 + \mu_2)}{\mu_1 \mu_2} = \lambda_1 \lambda_2 \left(\frac{1}{\mu_1} + \frac{1}{\mu_2} \right). \quad (6.101)$$

$\lambda_1 = \lambda_2 = \lambda$ & $\mu_1 = \mu_2 = \mu$ yield results as per Table 6.6 (for active redundancy). For the asymptotic & steady-state value of the point availability and average availability, $PA_S = AA_S = P_0 + P_1 + P_2$ holds with $P_0, P_1,$ and P_2 as solution of (Table 6.2)

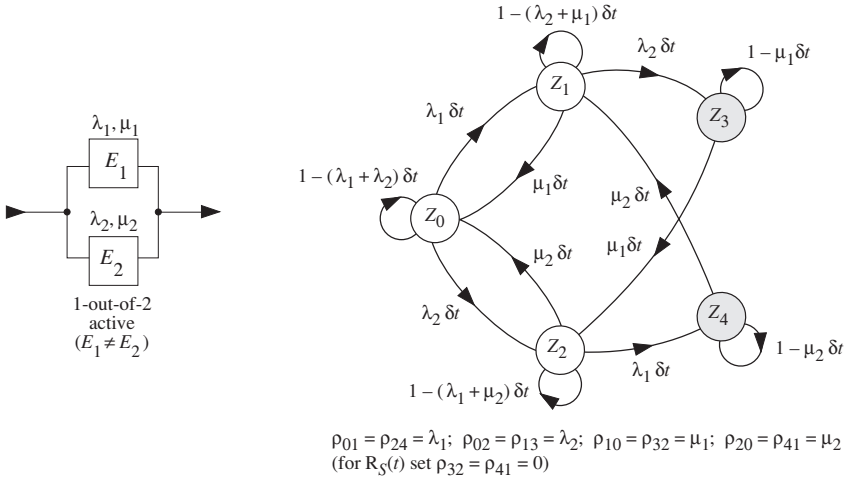


Figure 6.9 Reliability block diagram and diagram of transition probabilities in $(t, t + \delta t]$ for a repairable 1-out-of-2 active redundancy with two different elements, const. failure & repair rates $(\lambda_1, \lambda_2, \mu_1, \mu_2)$, ideal failure detection & switch, one repair crew (Z_3 & Z_4 down states (absorbing for reliability calculation), arbitrary $t, \delta t \downarrow 0$, Markov process)

$$\begin{aligned}
 (\lambda_1 + \lambda_2)P_0 &= \mu_1 P_1 + \mu_2 P_2, & (\lambda_2 + \mu_1)P_1 &= \lambda_1 P_0 + \mu_2 P_4, \\
 (\lambda_1 + \mu_2)P_2 &= \lambda_2 P_0 + \mu_1 P_3, & \mu_1 P_3 &= \lambda_2 P_1, & \mu_2 P_4 &= \lambda_1 P_2.
 \end{aligned}$$

One (arbitrarily chosen) of the five equations must be dropped and replaced by $P_0 + P_1 + P_2 + P_3 + P_4 = 1$. The solution yields P_0 through P_4 , from which

$$PA_S = AA_S = P_0 + P_1 + P_2 = \frac{1}{1 + \frac{\lambda_1 \lambda_2 [\mu_1^2 + \mu_2^2 + (\lambda_1 + \lambda_2)(\mu_1 + \mu_2)]}{\mu_1 \mu_2 [\mu_1 \mu_2 + (\lambda_1 + \lambda_2)(\lambda_1 + \lambda_2 + \mu_1 + \mu_2)]}}, \tag{6.102}$$

yielding, for $\lambda_1 \ll \mu_1$ and $\lambda_2 \ll \mu_2$,

$$PA_S = AA_S \approx 1 - \frac{\lambda_1 \lambda_2}{\mu_1^2 \mu_2^2} (\mu_1^2 + \mu_2^2) = 1 - \frac{\lambda_1}{\mu_1} \cdot \frac{\lambda_2}{\mu_2} \cdot \left(\frac{\mu_1}{\mu_2} + \frac{\mu_2}{\mu_1} \right). \tag{6.103}$$

$\lambda_1 = \lambda_2 = \lambda$ & $\mu_1 = \mu_2 = \mu$ yield results as per Table 6.6 (for active redundancy).

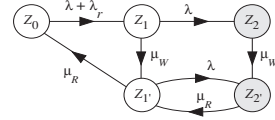
Example 6.7

As a refinement of the case investigated with Fig. 6.8 assume that to the repair time, distributed according to $G(x) = 1 - e^{-\mu_R x}$, a wait time for travel distributed according to $W(x) = 1 - e^{-\mu_W x}$ has to be added to the repair time for a failure occurred when both units are up (one operating, the other in reserve state). Repairs for failures occurred during the travel time or a repair do not need to wait for a further travel time. As before, the system has only one repair crew. Investigate the mean time to failure $MTTF_{S0}$ and the steady state availability $PA_S = AA_S$.

Solution

The system behavior can be described by a 5 states Markov process (graph). $MTTF_{S0}$ follows as solution of (Table 6.2, $M_i = MTTF_{S_i}$): $M_0 = M_1 + 1 / (\lambda + \lambda_r)$; $M_1 = (1 + \mu_w M_1) / (\lambda + \mu_w)$, $M_1 = (1 + \mu_R M_0) / (\lambda + \mu_R)$, yielding

$$MTTF_{S0} = \frac{1}{\lambda} + \frac{(\lambda + \mu_R)(\lambda + \mu_w)}{\lambda(\lambda + \lambda_r)(\lambda + \mu_R + \mu_w)} \approx \frac{1/(1/\mu_R + 1/\mu_w)}{\lambda(\lambda + \lambda_r)} \tag{6.103}$$



$PA_S = AA_S$ follows as solution of (Table 6.2): $\mu_w P_2 = \lambda P_1$, $(\lambda + \lambda_r)P_0 = \mu_R P_1$, $(\lambda + \mu_w)P_1 = (\lambda + \lambda_r)P_0$, $(\lambda + \mu_R)P_1 = \mu_w P_1 + \mu_R P_2$, $P_0 + P_1 + P_1' + P_2 + P_2' = 1$, yielding

$$PA_S = AA_S = P_0 + P_1 + P_1' = \frac{1}{1 + \frac{\lambda(\lambda + \lambda_r)[\lambda + \mu_R + \mu_w + \mu_R^2/\mu_w]}{\mu_R[(\lambda + \lambda_r)(\lambda + \mu_w + \mu_R) + (\lambda + \mu_w)\mu_R]}} \approx 1 - \frac{\lambda(\lambda + \lambda_r)}{\mu_R^2} \left(1 + \frac{\mu_R}{\mu_w} + \frac{\mu_R^2}{\mu_w^2}\right) \tag{6.104}$$

For $\mu_w = \infty$ and $\mu_R = \mu$, Eqs. (6.103) & (6.104) yield Eqs. (6.92) & (6.87); $\mu_w = 0$ yields results for the nonrepairable case; $\mu_w = \mu_R = \mu$ yields $MTTF_{S0} = \mu / 2\lambda(\lambda + \lambda_r)$, $PA_S \approx 1 - 3\lambda(\lambda + \lambda_r) / \mu^2$.

Supplementary results: Addition of a travel time to each repair has no practical significance. Generalization of distribution functions for repair and travel time lead to a 4 states semi-regenerative process with 3 reg. states (Fig. A.7.12).

6.4.2 1-out-of-2 Redundancy with Constant Failure and Arbitrary Repair Rates

Consider now a 1-out-of-2 *warm redundancy* with 2 identical elements $E_1 = E_2 = E$, failure-free times distributed according to Eqs. (6.81) & (6.82), and repair time with mean $MTTR < \infty$, distributed according to an arbitrary distribution function $G(x)$ with $G(0) = 0$ and density $g(x)$. The time behavior of this system can be described by a process with states Z_0 , Z_1 , and Z_2 . Because of the arbitrary repair rate, only states Z_0 and Z_1 are *regeneration states*. These states constitute a semi-Markov process *embedded* in the original *semi-regenerative process* (Fig. A.7.11). The *semi-Markov transition probabilities* $Q_{ij}(x)$ are given by Eq. (A7.182). Setting these quantities in the equations of Table 6.2 (SMP), by considering $Q_0(x) = Q_{01}(x)$ and $Q_1(x) = Q_{10}(x) + Q'_{12}(x)$ as per Eq. (A7.183), it follows for the *reliability functions* $R_{S_i}(t)$

$$R_{S0}(t) = e^{-(\lambda + \lambda_r)t} + \int_0^t (\lambda + \lambda_r) e^{-(\lambda + \lambda_r)x} R_{S1}(t - x) dx,$$

$$R_{S1}(t) = e^{-\lambda t} (1 - G(t)) + \int_0^t g(x) e^{-\lambda x} R_{S0}(t - x) dx, \tag{6.105}$$

and for the *transition probabilities* $P_{ij}(t)$ of the embedded semi-Markov process

$$\begin{aligned} P_{00}(t) &= e^{-(\lambda+\lambda_r)t} + \int_0^t (\lambda + \lambda_r) e^{-(\lambda+\lambda_r)x} P_{10}(t-x) dx, \\ P_{10}(t) &= \int_0^t g(x) e^{-\lambda x} P_{00}(t-x) dx + \int_0^t g(x) (1-e^{-\lambda x}) P_{10}(t-x) dx, \\ P_{11}(t) &= (1-G(t)) e^{-\lambda t} + \int_0^t g(x) e^{-\lambda x} P_{01}(t-x) dx + \int_0^t g(x) (1-e^{-\lambda x}) P_{11}(t-x) dx, \\ P_{01}(t) &= \int_0^t (\lambda + \lambda_r) e^{-(\lambda+\lambda_r)x} P_{11}(t-x) dx. \end{aligned} \quad (6.106)$$

The solution of Eqs. (6.105) leads to

$$\tilde{R}_{S0}(s) = \frac{s + \lambda + (\lambda + \lambda_r)(1 - \tilde{g}(s + \lambda))}{(s + \lambda)[(s + (\lambda + \lambda_r)(1 - \tilde{g}(s + \lambda)))]}, \quad (6.107)$$

and, considering $MTTF_{S0} = \tilde{R}_{S0}(0)$ (Eq. (2.61)),

$$MTTF_{S0} = \frac{\lambda + (\lambda + \lambda_r)(1 - \tilde{g}(\lambda))}{\lambda(\lambda + \lambda_r)(1 - \tilde{g}(\lambda))} \approx \frac{1}{(\lambda + \lambda_r)(1 - \tilde{g}(\lambda))}. \quad (6.108)$$

The Laplace transform of the *point availability* $PA_{S0}(t) = P_{00}(t) + P_{01}(t)$ follows as solution of Eqs. (6.106)

$$\tilde{P}_{AS0}(s) = \tilde{P}_{00}(s) + \tilde{P}_{01}(s) = \frac{(s + \lambda)[1 - \tilde{g}(s) + \tilde{g}(s + \lambda)] + (\lambda + \lambda_r)(1 - \tilde{g}(s + \lambda))}{(s + \lambda)[(s + (\lambda + \lambda_r)(1 - \tilde{g}(s))) + s \tilde{g}(s + \lambda)]}, \quad (6.109)$$

and leads to the *asymptotic & steady-state point and average availability* $PA_S = AA_S$ (considering $\lim_{s \rightarrow 0} (1 - \tilde{g}(s)) = s \cdot MTTR$ as per Eq. (6.54))

$$PA_S = AA_S = \frac{\lambda \tilde{g}(\lambda) + (\lambda + \lambda_r)(1 - \tilde{g}(\lambda))}{\lambda(\lambda + \lambda_r)MTTR + \lambda \tilde{g}(\lambda)} = \frac{\lambda + \lambda_r(1 - \tilde{g}(\lambda))}{\lambda(\lambda + \lambda_r)MTTR + \lambda \tilde{g}(\lambda)}. \quad (6.110)$$

where

$$MTTR = \int_0^\infty x g(x) dx = \int_0^\infty (1 - G(x)) dx, \quad (6.111)$$

and $\tilde{g}(\lambda)$ is the Laplace transform of the density $g(x)$ for $s = \lambda$, see Examples 6.8 & 6.9 for the approximation of $\tilde{g}(\lambda)$. Calculation of the *interval reliability* is difficult because state Z_1 is regenerative only at its occurrence point (Fig. A7.11). However, for $\lambda MTTR \ll 1$, $\tilde{g}(\lambda) \rightarrow 1$ and the asymptotic value of the state probability for Z_1 ($P_1 = \lim_{t \rightarrow \infty} P_{01}(t)$) becomes very small with respect to that for Z_0 ($P_0 = \lim_{t \rightarrow \infty} P_{00}(t)$). For the asymptotic & steady-state value of the *interval reliability* it holds then that

$$IR_S(\theta) \approx P_0 R_{S0}(\theta) = \lambda \tilde{g}(\lambda) R_{S0}(\theta) / (\lambda(\lambda + \lambda_r)MTTR + \lambda \tilde{g}(\lambda)). \quad (6.112)$$

In practical applications, $\lambda MTTR < 0.01$ and Eq. (6.112) yields $IR_S(\theta) \approx R_{S0}(\theta)$.

Example 6.8

Let the density $g(x)$ of the repair time τ' of a system with constant failure rate $\lambda > 0$ be continuous and assume furthermore that $\lambda E[\tau'] = \lambda MTTR \ll 1$ and $\lambda \text{Var}[\tau'] < MTTR$. Investigate the quantity $\tilde{g}(\lambda)$ for $\lambda \rightarrow 0$.

Solution

For $\lambda \rightarrow 0$, $\lambda MTTR \ll 1$ & $\lambda \text{Var}[\tau'] < MTTR$, the 3 first terms of the series expansion of $e^{-\lambda t}$ lead to

$$\tilde{g}(\lambda) = \int_0^\infty g(t)e^{-\lambda t} dt \approx \int_0^\infty g(t)(1 - \lambda t + \frac{(\lambda t)^2}{2}) dt = 1 - \lambda E[\tau'] + E[\tau'^2] \lambda^2 / 2.$$

From this, follows the *approximate expression* (Eq. (A6.45))

$$\tilde{g}(\lambda) \approx 1 - \lambda MTTR + \lambda^2 (MTTR^2 + \text{Var}[\tau']) / 2. \tag{6.113}$$

In many practical applications,

$$\tilde{g}(\lambda) \approx 1 - \lambda MTTR \tag{6.114}$$

is a sufficiently good approximation, however not in calculating steady-state availability (Eq. (6.114) would give for Eq. (6.110) $PA_S = 1$, thus Eq. (6.113) has to be used).

Supplementary results: $g(x) = \mu e^{-\mu x}$ leads to $\tilde{g}(\lambda) = \mu / (\lambda + \mu) \approx 1 - \lambda / \mu + (\lambda / \mu)^2$ which agree with Eq. (6.113), considering $MTTR = 1 / \mu$ and $\text{Var}[\tau'] = 1 / \mu^2$.

Example 6.9

In a 1-out-of-2 warm redundancy with identical elements E_1 and E_2 let the failure rates λ in the operating state and λ_r in the reserve state be constant. For the repair time let us assume that it is distributed according to $G(x) = 1 - e^{-\mu(x-\psi)}$ for $x > \psi$ and $G(t) = 0$ for $x \leq \psi$, with $MTTR \equiv 1 / \mu > \psi$. Assuming $\lambda \psi \ll 1$, investigate the influence of ψ on the mean time to failure $MTTF_{S0}$ and on the asymptotic & steady-state value of the point availability PA_S .

Solution

With

$$\tilde{g}(\lambda) = \int_\psi^\infty \mu' e^{-\mu'(t-\psi) - \lambda t} dt = \frac{\mu'}{\lambda + \mu'} e^{-\lambda \psi} \approx \frac{\mu'}{\lambda + \mu'} (1 - \lambda \psi)$$

and considering $MTTR = \int_0^\infty t g(t) dt = \int_\psi^\infty t \mu' e^{-\mu'(t-\psi)} dt = \psi + \frac{1}{\mu'} \equiv \frac{1}{\mu}$, i.e., $\mu' = \mu / (1 - \mu \psi)$ and thus $\tilde{g}(\lambda) \approx \mu(1 - \lambda \psi) / (\lambda + \mu(1 - \lambda \psi))$, Eq. (6.108) (left-hand equality) and Eq. (6.110) lead to the *approximate expressions*

$$MTTF_{S0, \psi > 0} \approx \frac{2\lambda + \lambda_r + \mu(1 - \lambda \psi)}{\lambda(\lambda + \lambda_r)}$$

and

$$PA_{S, \psi > 0} \approx \frac{\mu(\lambda + \lambda_r + \mu(1 - \lambda \psi))}{(\lambda + \lambda_r)(\lambda + \mu(1 - \lambda \psi)) + \mu^2(1 - \lambda \psi)} \approx 1 - \frac{\lambda(\lambda + \lambda_r)(1 - \mu \psi)}{\mu(\lambda + \lambda_r + \mu(1 - \lambda \psi))}.$$

On the other hand, $\psi = 0$ leads to $1 - \tilde{g}(\lambda) = \lambda / (\lambda + \mu)$ and thus (Eqs. (6.92) and (6.87))

$$MTTF_{S0, \psi = 0} = \frac{2\lambda + \lambda_r + \mu}{\lambda(\lambda + \lambda_r)} \quad \text{and} \quad PA_{S, \psi = 0} = \frac{\mu(\lambda + \lambda_r + \mu)}{(\lambda + \mu)(\lambda + \lambda_r) + \mu^2}.$$

Assuming $\mu \gg \lambda$, λ_r yields (considering $\lambda \psi < \lambda / \mu \ll 1$)

$$\frac{MTTF_{S0, \psi > 0}}{MTTF_{S0, \psi = 0}} \approx 1 - \lambda \psi \quad \text{and} \quad \frac{PA_{S, \psi > 0}}{PA_{S, \psi = 0}} \approx 1 + \lambda \psi \frac{\lambda + \lambda_r}{\mu} \approx 1. \tag{6.115}$$

Equation (6.115) allows the conclusion to be made that:

For $\lambda MTTR \ll 1$, the shape of the distribution function of the repair time has (as long as $MTTR$ is unchanged) a small influence on results at system level, in particular on the mean time to failure $MTTF_{S0}$ and on the asymptotic & steady-state value of the point availability PA_S of a 1-out-of-2 redundancy.

Above conclusion can often be extended to more complex structures. Example 6.10 shows a numerical comparison for the case of a 1-out-of-2 parallel redundancy.

Example 6.10

A 1-out-of-2 parallel redundancy with identical elements E_1 and E_2 has failure rate $\lambda = 10^{-2} \text{h}^{-1}$ and lognormally distributed repair times with mean $MTTR = 2.4 \text{h}$ and variance 0.6h^2 (Eqs. (A6.112), (A6.113) with $\lambda = 0.438 \text{h}^{-1}$, $\sigma = 0.315$). Compute the mean time to failure $MTTF_{S0}$ and the asymptotic & steady-state point and average availability PA_S with approximate expressions: (i) $\tilde{g}(\lambda)$ from Eq. (6.114); (ii) $\tilde{g}(\lambda)$ from Eq. (6.113); (iii) $g(t) = \mu' e^{-\mu'(t-\psi)}$, $t \geq \psi$, $\psi = 1.3 \text{h}$, $1/\mu' = 1.1 \text{h}$, $1/\mu = 2.4 \text{h}$ (Eq. (4.2)); (iv) $g(t) = \mu e^{-\mu t}$ and $1/\mu = 2.4 \text{h}$.

Solution

(i) With $\tilde{g}(\lambda) = 0.976$ it follows (Eq. (6.108)) that $MTTF_{S0} \approx 2183 \text{h}$ and (Eq. (6.110)) $PA_S = 1$. (ii) With $\tilde{g}(\lambda) \approx 0.9763$ it follows (Eq. (6.108)) that $MTTF_{S0} \approx 2211 \text{h}$ and (Eq. (6.110)) $PA_S \approx 0.9994$. (iii) Example 6.9 yields $MTTF_{S0, \psi=1.3 \text{h}} \approx 2206 \text{h}$ and $PA_{S, \psi=1.3 \text{h}} \approx 0.9995$. (iv) From Eqs. (6.92) and (6.87) it follows that $MTTF_{S0} \approx 2233 \text{h}$ and $PA_S \approx 0.9989$.

Supplementary results: Numerical computation with the lognormal distribution ($MTTR = 2.4 \text{h}$, $\text{Var}[\tau] = 0.6 \text{h}^2$) yields $MTTF_{S0} \approx 2186 \text{h}$ and $PA_S \approx 0.9995$. For a failure rate $\lambda = 10^{-3} \text{h}^{-1}$, results were: 209'333h, 1; 209'611h, 0.999997; 209'563h, 0.999995; 209'833, 0.999989; 209'513h, 0.999994.

6.4.3 1-out-of-2 Redundancy with Constant Failure Rate only in the Reserve State, Arbitrary Repair Rates

Generalization of repair and failure rates for a 1-out-of-2 redundancy leads to a *nonregenerative stochastic process*. However, in many practical applications it can be assumed that *the failure rate in reserve state is constant*. If this holds, and the 1-out-of-2 redundancy has *only one repair crew*, then the process involved is regenerative with exactly *one regeneration state* [6.5 (1975)].

To see this, consider a 1-out-of-2 warm redundancy, satisfying assumptions (6.1) - (6.7), with failure-free times distributed according to $F(x)$ in operating state and $V(x) = 1 - e^{-\lambda_r x}$ in reserve state, and repair times distributed according to $G(x)$ for repair of failures in operating state and $W(x)$ for repair of failures in reserve state ($F(0) = V(0) = G(0) = W(0) = 0$, densities $f(x), v(x), g(x), w(x) \rightarrow 0$ for $x \rightarrow \infty$, means and variances $< \infty$). Figure 6.10a shows a possible time schedule and Fig. 6.10b gives the *state transition diagram* of the involved stochastic process.

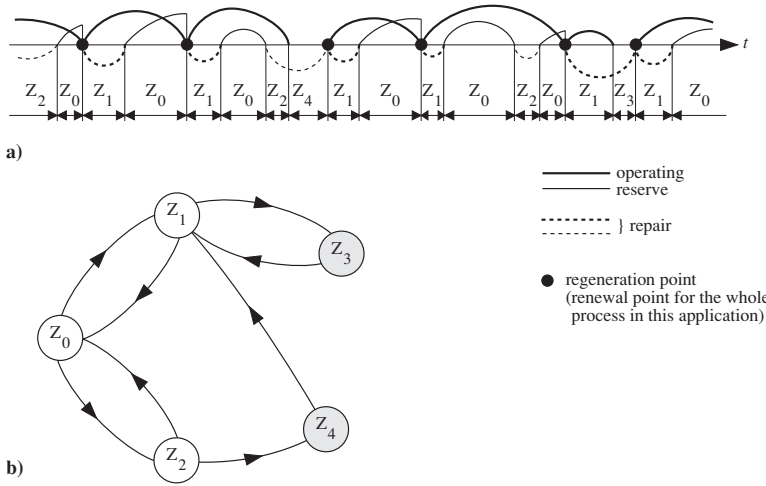


Figure 6.10 Repairable 1-out-of-2 warm redundancy with constant failure rate λ_r in reserve state, arbitrary failure rate in operating state, arbitrary repair rates, ideal failure detection & switch, one repair crew (Z_3 & Z_4 down states, absorbing for rel. calculation): a) Possible time schedule (repair times exaggerated); b) State transition diagram to visualize state transitions (Z_1 regeneration state)

States Z_0, Z_1, Z_2 are up states. Z_1 is the only *regeneration state* (Z_0, Z_2, Z_3, Z_4 are not regeneration states). At its occurrence, a failure-free time of the operating element and a repair time for a failure in the operating state are started (Fig. 6.10a). The occurrence of Z_1 is a *regeneration point* with respect to Z_1 and in this application a renewal point for the whole process. It brings the process to a situation of *total independence from the previous development* (the process restarts anew). From this, it is sufficient to investigate the behavior between *two consecutive regeneration points*, and from $t=0$ up to the first regeneration point (Appendix A7.4).

Let us consider first the case in which the regeneration state Z_1 is entered at $t=0$ (S_{RP0}), and let S_{RP1} be the first regeneration point after $t=0$. The *reliability function* $R_{S1}(t) = \Pr\{\text{up in } (0, t] \mid Z_1 \text{ entered at } t=0\}$ is given by

$$R_{S1}(t) = 1 - F(t) + \int_0^t u_1(x) R_{S1}(t-x) dx, \tag{6.116}$$

with

$$1 - F(t) = \Pr\{\text{failure-free time of the operating element} > t \mid Z_1 \text{ entered at } t=0\}^+)$$

and

$$\int_0^t u_1(x) R_{S1}(t-x) dx = \Pr\{(S_{RP1} \leq t \cap \text{system not failed in } (0, S_{RP1}]) \cap \text{up in } (S_{RP1}, t]) \mid Z_1 \text{ entered at } t=0\}.$$

^{+) Z_1 entered at $t=0$ implies operating element new at $t=0$, see Figs. 6.10a and 6.11.}

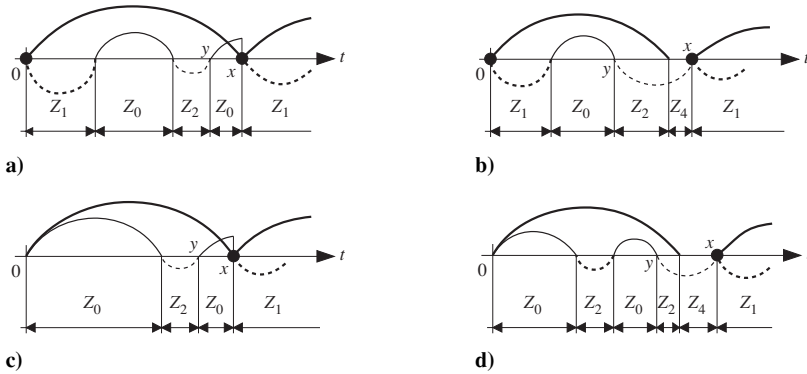


Figure 6.11 Possible time schedules for the 1-out-of-2 redundancy according to Fig. 6.10 for the cases in which state Z_1 (a, b) or state Z_0 with both elements new (c, d) is entered at $t = 0$

The first regeneration point S_{RP1} occurs at the time x (within the interval $(x, x+dx]$) only if at this time the operating element fails (for the first time) and the reserve element is ready to enter the operating state. $u_1(x)$, defined as (Example A7.2)

$$u_1(x) = \lim_{\delta x \downarrow 0} \frac{1}{\delta x} \Pr\{x < S_{RP1} \leq x + \delta x \cap \text{system not failed in } (0, x] \mid Z_1 \text{ entered at } t=0\},$$

follows from (Fig. 6.11a)

$$u_1(x) = f(x)PA_d(x), \tag{6.117}$$

with

$$\begin{aligned} PA_d(x) &= \Pr\{\text{reserve element up at time } x \mid Z_1 \text{ entered at } t=0\} \\ &= \int_0^x h'_{dud}(y)e^{-\lambda_r(x-y)}dy \end{aligned} \tag{6.118}$$

and (with $*$ as convolution (Eq.(A6.75)))

$$h'_{dud}(y) = g(y) + g(y) * v(y) * w(y) + g(y) * v(y) * w(y) * v(y) * w(y) + \dots \tag{6.119}$$

The point availability $PA_{S1}(t) = \Pr\{\text{up at } t \mid Z_1 \text{ entered at } t=0\}$ is given by

$$PA_{S1}(t) = 1 - F(t) + \int_0^t u_1(x)PA_{S1}(t-x)dx + \int_0^t u_2(x)PA_{S1}(t-x)dx, \tag{6.120}$$

with $1 - F(t)$ as for Eq. (6.116),

$$\int_0^t u_1(x) PA_{S_1}(t-x) dx = \Pr\{(S_{RP1} \leq t \cap \text{system not failed in } (0, S_{RP1}] \cap \text{up at } t) \mid Z_1 \text{ entered at } t=0\},$$

and

$$\int_0^t u_2(x) PA_{S_1}(t-x) dx = \Pr\{(S_{RP1} \leq t \cap \text{system failed in } (0, S_{RP1}] \cap \text{up at } t) \mid Z_1 \text{ entered at } t=0\}.$$

$u_2(x)$, defined as (Example A7.2)

$$u_2(x) = \lim_{\delta x \downarrow 0} \frac{1}{\delta x} \Pr\{(x < S_{RP1} \leq x + \delta x \cap \text{system failed in } (0, x] \mid Z_1 \text{ entered at } t=0\},$$

follows from (Fig. 6.11b)

$$u_2(x) = g(x)F(x) + \int_0^x h'_{udd}(y) w(x-y) (F(x) - F(y)) dy \quad (6.121)$$

with

$$h'_{udd}(y) = g(y) * v(y) + g(y) * v(y) * w(y) * v(y) + \dots \quad (6.122)$$

One recognizes that $u_1(x) + u_2(x)$ is the density of the *interval times* $S_{RP_{i+1}} - S_{RP_i}$ separating consecutive regeneration points S_{RP_i} ($i=0, 1, \dots, S_{RP_0} \equiv 0$), i. e. separating consecutive renewal points of the embedded renewal process.

Consider now the case in which at $t=0$ the state Z_0 with both elements new is entered. The reliability function $R_{S_0}(t) = \Pr\{\text{up in } (0, t] \mid Z_0 \text{ with both elements new is entered at } t=0\}$ is given by

$$R_{S_0}(t) = 1 - F(t) + \int_0^t u_3(x) R_{S_1}(t-x) dx, \quad (6.123)$$

with (Fig. 6.11c)

$$u_3(x) = \lim_{\delta x \downarrow 0} \frac{1}{\delta x} \Pr\{(x < S_{RP1} \leq x + \delta x \cap \text{system not failed in } (0, x] \mid Z_0 \text{ with both elements new is entered at } t=0\} = f(x) PA_0(x), \quad (6.124)$$

where

$$\begin{aligned} PA_0(x) &= \Pr\{\text{reserve element up at time } x \mid Z_0 \text{ with both elem. new is entered at } t=0\} \\ &= e^{-\lambda_r x} + \int_0^x h'_{duu}(y) e^{-\lambda_r(x-y)} dy, \end{aligned} \quad (6.125)$$

with

$$h'_{duu}(y) = v(y) * w(y) + v(y) * w(y) * v(y) * w(y) + \dots \quad (6.126)$$

The *point availability* $PA_{S_0}(t) = \Pr\{\text{up at } t \mid Z_0 \text{ with both elements new is entered at } t=0\}$ is given by

$$PA_{S_0}(t) = 1 - F(t) + \int_0^t u_3(x) PA_{S_1}(t-x) dx + \int_0^t u_4(x) PA_{S_1}(t-x) dx, \quad (6.127)$$

with (Fig. 6.11d)

$$u_4(x) = \lim_{\delta x \downarrow 0} \frac{1}{\delta x} \Pr\{(x < S_{RP1} \leq x + \delta x \cap \text{system failed in } (0, x]) \mid Z_0 \text{ with both elements new is entered at } t=0\} = \int_0^x h'_{udu}(y) w(x-y)(F(x) - F(y)) dy \quad (6.128)$$

and

$$h'_{udu}(y) = v(y) + v(y) * w(y) * v(y) + v(y) * w(y) * v(y) * w(y) * v(y) + \dots \quad (6.129)$$

One recognizes that $u_3(x) + u_4(x)$ is the density of the time from $t=0$, when the state Z_0 is entered with both elements new, to the first regeneration point S_{RP1} , i.e. to the first renewal point of the embedded renewal process with density $u_1(x) + u_2(x)$ for the time intervals separating consecutive renewal points.

Equations (6.116), (6.120), (6.123), (6.127) can be solved using Laplace transforms (LT). However, analytical difficulties can arise when calculating LT for $F(x)$, $G(x)$, $W(x)$, $u_1(x)$, $u_2(x)$, $u_3(x)$, $u_4(x)$ or at the inversion of final equations. Easier is the calculation of the *mean time to failure* $MTTF_{S_0} = \tilde{R}_{S_0}(0)$ (Eqs. (2.59), (2.61)) and of the *asymptotic & steady-state point and average availability* $PA_S = AA_S = \lim_{s \rightarrow 0} s \tilde{PA}_{S_0}(s) = \lim_{s \rightarrow 0} s \tilde{PA}_{S_1}(s)$, for which the following expressions can be found using LT (see Eqs. (6.123) & (6.116) for $MTTF_{S_0}$ and Eqs. (6.120) or (6.127) for PA_S , and consider (Eq. (6.54)) $\lim_{s \rightarrow 0} (1 - \tilde{f}(s)) / s = MTTF$)

$$MTTF_{S_0} = MTTF \left[1 + \frac{\int_0^\infty u_3(x) dx}{1 - \int_0^\infty u_1(x) dx} \right], \quad (6.130)$$

and

$$\lim_{t \rightarrow \infty} PA_{S_0}(t) = \lim_{t \rightarrow \infty} PA_{S_1}(t) = PA_S = AA_S = \frac{MTTF}{\int_0^\infty x(u_1(x) + u_2(x)) dx}, \quad (6.131)$$

with

$$MTTF = \int_0^\infty (1 - F(x)) dx. \quad (6.132)$$

Eq. (6.131) considers that PA_S exists (p. 478-79) and that $u_1(x) + u_2(x)$ is the density of a random variable with finite mean (and thus $\int_0^\infty (u_1(x) + u_2(x)) dx = 1$); same for $u_3(x) + u_4(x)$.

It must be pointed out that $R_{S_0}(t)$ and $PA_{S_0}(t)$ apply only to the case in which at $t=0$ both elements are new (Fig. 6.11 c & d). Situations with arbitrary initial conditions at $t=0$ (e. g. entering state Z_0 with the operating element not new or entering state Z_2) are not considered here because their computation requires the knowledge of the time spent in the operating state before $t=0$.

The model investigated in this section has as special cases that of Section 6.4.2 ($F(x) = 1 - e^{-\lambda x}$, $W(x) = G(x)$) and the 1-out-of-2 standby redundancy with identical elements and arbitrarily distributed failure-free and repair times (Example 6.11).

Table 6.7 summarizes the results for the 1-out-of-2 redundancy with arbitrary repair rates, and failure rates as general as possible within a regenerative process.

Example 6.11

Using the results of Section 6.4.3, give the expressions for the reliability function $R_{S_0}(t)$ and the point availability $PA_{S_0}(t)$ for a 1-out-of-2 standby redundancy with 2 identical elements, failure-free time distributed according to $F(x)$, with density $f(x)$, and repair time distributed according to $G(x)$ with density $g(x)$.

Solution

For a standby redundancy, $u_1(x) = f(x)G(x)$, $u_2(x) = g(x)F(x)$, $u_3(x) = f(x)$, and $u_4(x) \equiv 0$ (Eqs. (6.117), (6.121), (6.124), and (6.128)). From this, the expressions for $R_{S_0}(t)$, $R_{S_1}(t)$, $PA_{S_0}(t)$, and $PA_{S_1}(t)$ can be given. The Laplace transforms of $R_{S_0}(t)$ and $PA_{S_0}(t)$ are

$$\tilde{R}_{S_0}(s) = \frac{1 - \tilde{f}(s)}{s} + \frac{\tilde{f}(s)(1 - \tilde{f}(s))}{s(1 - \tilde{u}_1(s))}, \quad (6.133)$$

$$\tilde{PA}_{S_0}(s) = \frac{1 - \tilde{f}(s)}{s} + \frac{\tilde{f}(s)(1 - \tilde{f}(s))}{s[1 - (\tilde{u}_1(s) + \tilde{u}_2(s))]}, \quad (6.134)$$

with

$$\tilde{u}_1(s) = \int_0^{\infty} f(t)G(t)e^{-st} dt \quad \text{and} \quad \tilde{u}_2(s) = \int_0^{\infty} g(t)F(t)e^{-st} dt .$$

The mean time to failure $MTTF_{S_0}$ follows from Eq. (6.133) as $MTTF_{S_0} = \tilde{R}_{S_0}(0)$, or directly from Eq. (6.130),

$$MTTF_{S_0} = MTF + \frac{MTF}{1 - \int_0^{\infty} f(x)G(x)dx} . \quad (6.135)$$

The asymptotic & steady-state value of the point and average availability $PA_S = AA_S$ follows from Eq. (6.134) as $PA_S = AA_S = \lim_{s \rightarrow 0} s \tilde{PA}_{S_0}(s)$ or directly from Eq. (6.131),

$$PA_S = AA_S = \frac{MTF}{\int_0^{\infty} x d(F(x)G(x))} . \quad (6.136)$$

Table 6.7 Mean time to failure $MTTF_{S0}$, steady-state point & average availability $PA_S = AA_S$, and steady-state interval reliability $IR_S(\theta)$ for a repairable 1-out-of-2 redundancy with two identical elements, arbitrary repair rates, failure rates as general as possible within a regenerative process, ideal failure detection & switch, one repair crew (regenerative process as per Fig. 6.10)

		Standby ($\lambda_r = 0$)	Warm ($\lambda_r < \lambda$)		Active ($\lambda_r = \lambda$)	
Element E_1 and E_2	Distribution of the failure-free times	OS	$F(x)$	$1 - e^{-\lambda x}$	$F(x)$	$1 - e^{-\lambda x}$
		RS	-	$1 - e^{-\lambda_r x}$	$1 - e^{-\lambda_r x}$	$1 - e^{-\lambda x}$
	Distribution of the repair times	OS	$G(x)$	$G(x)$	$G(x)$	$G(x)$
		RS	-	$G(x)$	$W(x)$	$G(x)$
Mean of the failure-free times		$MTTF = \int_0^\infty (1 - F(x)) dx$	$\frac{1}{\lambda}$ or $\frac{1}{\lambda_r}$	$MTTF$ or $\frac{1}{\lambda_r}$	$\frac{1}{\lambda}$	
Mean of the repair times		$MTTR = \int_0^\infty (1 - G(x)) dx$	$MTTR$	$MTTR$ or $MTTR_W$	$MTTR$	
1-out-of-2 redundancy	Mean time to failure ($MTTF_{S0}$)	$MTTF + \frac{\int_0^\infty f(x)G(x) dx}{1 - \int_0^\infty f(x)G(x) dx}$	$\frac{1}{\lambda} + \frac{1}{(\lambda + \lambda_r)(1 - \tilde{g}(\lambda))}$ $\approx \frac{1}{\lambda} (1 + \frac{1}{(\lambda + \lambda_r)MTTR})$	$MTTF + \frac{MTTF \int_0^\infty u_3(x) dx}{1 - \int_0^\infty u_1(x) dx}$	$\frac{1}{\lambda} + \frac{1}{2\lambda(1 - \tilde{g}(\lambda))}$ $\approx \frac{1}{\lambda} + \frac{1}{2\lambda^2 MTTR}$	
	Point & average availability ($PA_S = AA_S$) *	$\frac{MTTF}{\int_0^\infty x d(F(x)G(x))}$	$\frac{\lambda + \lambda_r (1 - \tilde{g}(\lambda))}{\lambda(\lambda + \lambda_r)MTTR + \lambda \tilde{g}(\lambda)}$	$\frac{MTTF}{\int_0^\infty x(u_1(x) + u_2(x)) dx}$	$\frac{2 - \tilde{g}(\lambda)}{2\lambda MTTR + \tilde{g}(\lambda)}$	
	Interval reliability ($IR_S(\theta)$) *	$\approx R_{S0}(\theta)$	$\approx R_{S0}(\theta)$	$\approx R_{S0}(\theta)$	$\approx R_{S0}(\theta)$	

$u_1(x), u_2(x), u_3(x)$ as per Eqs. (6.117), (6.121), (6.124); OS = operating state; RS = reserve state

* asymptotic & steady-state value

6.5 *k*-out-of-*n* Redundancy (Warm, Identical Elements, one Repair Crew)

A *k*-out-of-*n* redundancy, also known as *k*-out-of-*n*: *G*, consists of *n* often identical elements, of which *k* are necessary for the required function and *n* - *k* are in reserve state, when not under repair or waiting for repair.. Assuming ideal failure detection and switching, the reliability block diagram is as given in Fig. 6.12. Investigations

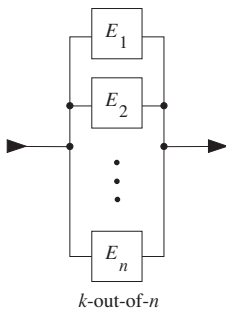


Figure 6.12 k -out-of- n redundancy reliability block diagram (ideal failure detection & switch)

in this Section assume identical elements E_1, \dots, E_n , *only one repair crew*, and *no further failures at system down* (failures during repair at system level are not considered, as per assumption (6.2)). Section 6.5.1 considers the case of *warm redundancy* with constant failure rate λ in the operation state and $\lambda_r < \lambda$ in the *reserve state* as well as constant repair rate μ . This case includes *active redundancy* ($\lambda_r = \lambda$) and *standby redundancy* ($\lambda_r = 0$). An extension to cover other situations in which the failure rate is modified at state changes (e. g. for *load sharing*) is possible using equations for the *birth and death process* developed in Appendix A7.5.5 (see also pp. 61-64). Section 6.5.2 investigates a k -out-of- n active redundancy with constant failure rate and arbitrary repair rate. The influence of series elements (including *switching elements*) is considered in Sections 6.6 - 6.7. Imperfect switching, incomplete coverage, and common cause failures are investigated in Section 6.8.

6.5.1 k -out-of- n Redundancy with Const. Failure & Repair Rates

Assuming constant failure and repair rates, the time behavior of the k -out-of- n redundancy with identical elements can be investigated using a *birth and death process* (Appendix A7.5.5). Figure 6.13 gives the corresponding diagram of transition probabilities in $(t, t + \delta t]$. From Fig. 6.13 and Table 6.2, the following system of differential equations can be established for the state probabilities $P_j(t) = \Pr\{\text{in state } Z_j \text{ at } t\}$ of a k -out-of- n warm redundancy with one repair crew and no further failures at system down (constant failure rates λ & λ_r and repair rate μ)

$$\begin{aligned} \dot{P}_0(t) &= -v_0 P_0(t) + \mu P_1(t) \\ \dot{P}_j(t) &= v_{j-1} P_{j-1}(t) - (v_j + \mu) P_j(t) + \mu P_{j+1}(t), \quad j = 1, \dots, n-k, \\ \dot{P}_{n-k+1}(t) &= v_{n-k} P_{n-k}(t) - \mu P_{n-k+1}(t), \end{aligned} \quad (6.137)$$

with

$$v_j = k\lambda + (n-k-j)\lambda_r, \quad j = 0, \dots, n-k. \quad (6.138)$$

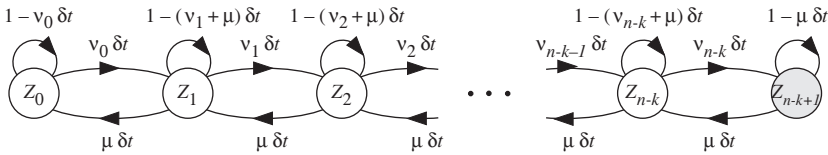


Figure 6.13 Diagram of transition probabilities in $(t, t + \delta t]$ for a repairable k -out-of- n warm redundancy with n identical elements, constant failure and repair rates $(\lambda, \lambda_r, \mu)$, ideal failure detection & switch, one repair crew, no further failures at system down (Z_{n-k+1} down state (absorbing for reliability calculation), arbitrary $t, \delta t \downarrow 0$, Markov process (birth and death))

For the investigation of more general situations (arbitrary load sharing, more than one repair crew, or other cases in which failure and/or repair rates change at a state transition) one can use the *birth and death process* introduced in Appendix A7.5.5. The solution of the system (6.137) - (6.138) with the *initial conditions* at $t = 0, P_i(0) = 1$ and $P_j(0) = 0$ for $j \neq i$, yields the *point availability* (see Table 6.2 for notations)

$$PA_{S_i}(t) = \sum_{j=0}^{n-k} P_{ij}(t), \tag{6.139}$$

with $P_{ij}(t) \equiv P_j(t)$ from Eq. (6.137) with $P_i(0) = 1$. In many practical applications, only the *asymptotic & steady-state* value of the point availability PA_S is required. This can be obtained by setting $\dot{P}_j(t) = 0$ and $P_j(t) = P_j$ ($j = 0, \dots, n - k + 1$) in Eq. (6.137). The solution yields (Eqs. (A7.134) & (A7.151))

$$PA_S = \sum_{j=0}^{n-k} P_j = 1 - P_{n-k+1}, \quad \text{with } P_j = P_0 \pi_j = \frac{\pi_j}{\sum_{i=0}^{n-k+1} \pi_i}, \quad \pi_i = \frac{v_0 \dots v_{i-1}}{\mu^i}, \quad \pi_0 = 1,$$

i.e.,

$$PA_S = \frac{\mu^{n-k+1} + v_0 \mu^{n-k} + v_0 v_1 \mu^{n-k-1} + \dots + v_0 \dots v_{n-k-1} \mu}{\mu^{n-k+1} + v_0 \mu^{n-k} + v_0 v_1 \mu^{n-k-1} + \dots + v_0 \dots v_{n-k-1} \mu + v_0 \dots v_{n-k}} \approx 1 - \frac{v_0 \dots v_{n-k}}{\mu^{n-k+1}}. \tag{6.140}$$

PA_S is also the asymptotic & steady-state value of the *average availability* AA_S . As shown in Example A7.11 (Eq. (A7.157), for $2v_j < \mu$ it holds that

$$P_j > \sum_{i=j+1}^{n-k+1} P_i, \quad j = 0, \dots, n - k.$$

From this, the following *bounds on PA_S* can be used in many practical applications (assuming $2v_j < \mu, j = 0, \dots, n - k$) to obtain an *approximate expression* for PA_S

$$\sum_{j=0}^i P_j \leq PA_S < P_i + \sum_{j=0}^i P_j, \quad i = 0, \dots, n - k. \tag{6.141}$$

The *reliability function* follows from Table 6.2 and Fig. 6.13

$$\begin{aligned}
 R_{S_0}(t) &= e^{-v_0 t} + \int_0^t v_0 e^{-v_0 x} R_{S_1}(t-x) dx \\
 R_{S_j}(t) &= e^{-(v_j+\mu)t} + \int_0^t [v_j R_{S_{j+1}}(t-x) + \mu R_{S_{j-1}}(t-x)] e^{-(v_j+\mu)x} dx, \\
 & \qquad \qquad \qquad j=1, \dots, n-k-1, \\
 R_{S_{n-k}}(t) &= e^{-(v_{n-k}+\mu)t} + \int_0^t \mu R_{S_{n-k-1}}(t-x) e^{-(v_{n-k}+\mu)x} dx,
 \end{aligned} \tag{6.142}$$

with v_j as in Eq. (6.138). Similar results hold for the *mean time to failure*

$$\begin{aligned}
 MTTFS_0 &= MTTFS_1 + 1/v_0 \\
 MTTFS_j &= (1+v_j MTTFS_{j+1} + \mu MTTFS_{j-1}) / (v_j + \mu), \quad j = 1, \dots, n-k-1, \\
 MTTFS_{n-k} &= (1 + \mu MTTFS_{n-k-1}) / (v_{n-k} + \mu).
 \end{aligned} \tag{6.143}$$

The solution of Eqs. (6.142) and (6.143), shows that $R_{S_i}(t)$ and $MTTFS_i$ depend on $n-k$ only. This leads for $n-k=1$ to

$$\tilde{R}_{S_0_1}(s) = \frac{s + v_0 + v_1 + \mu}{(s + v_0)(s + v_1) + s\mu}, \quad MTTFS_{0_1} = \frac{v_0 + v_1 + \mu}{v_0 v_1} \approx \frac{\mu}{v_0 v_1}, \tag{6.144}$$

and for $n-k=2$ to

$$\begin{aligned}
 \tilde{R}_{S_0_2}(s) &= \frac{(s + v_0 + v_1 + \mu)(s + v_2 + \mu) + v_1(v_0 - \mu)}{s(s + v_0 + v_1 + \mu)(s + v_2 + \mu) + v_0 v_1 v_2 + s v_1(v_0 - \mu)}, \\
 MTTFS_{0_2} &= \frac{v_2(v_0 + v_1 + \mu) + \mu(v_0 + \mu) + v_0 v_1}{v_0 v_1 v_2} \approx \frac{\mu^2}{v_0 v_1 v_2}.
 \end{aligned} \tag{6.145}$$

This property holds for the *point availability* PA_S as well, see Table 6.8 for results.

Because of the constant failure rate, the *interval reliability* follows directly from

$$IR_{S_i}(t, t+\theta) = \sum_{j=0}^{n-k} P_{ij}(t) R_{S_j}(\theta), \quad i = 0, \dots, n-k, \tag{6.146}$$

with $P_{ij}(t)$ as in Eq. (6.139) and $R_{S_i}(\theta)$ from Eq. (6.142) with $t = \theta$. The asymptotic & steady-state value is then given by

$$IR_S(\theta) = \sum_{j=0}^{n-k} P_j R_{S_j}(\theta), \tag{6.147}$$

with P_j from Eq. (6.140). Table 6.8 summarizes the main results for the k -out-of- n warm redundancy with identical elements, constant failure & repair rates, one repair crew, and no further failures at system down.

Table 6.8 Mean time to failure $MTTF_{S0}$, steady-state point & average availability $PA_S = AA_S$, and steady-state interval reliability $IR_S(\theta)$ for a *repairable k-out-of-n warm redundancy* with *n* identical elements, constant failure & repair rates λ, λ_r, μ ($\lambda_r < \lambda$ for reserve state, $\lambda_r \equiv 0$ for standby), ideal failure detection and switch, *one repair crew*, and *no further failures at system down* (Markov process (birth and death) as per Fig. 6.13)

		Mean time to failure ($MTTF_{S0}$)	Asymptotic & steady-state point and average availability ($PA_S = AA_S$)	Interval reliability ($IR_S(\theta)$)
$n-k=1$	gen. case	$\frac{v_0 + v_1 + \mu}{v_0 v_1} \approx \frac{\mu}{v_0 v_1}$	$\frac{v_0 \mu + \mu^2}{v_0 v_1 + v_0 \mu + \mu^2} \approx 1 - \frac{v_0 v_1}{\mu^2}$	$\approx R_{S0}(\theta)$
	$n=2$ $k=1$	$\frac{2\lambda + \lambda_r + \mu}{\lambda(\lambda + \lambda_r)} \approx \frac{\mu}{\lambda(\lambda + \lambda_r)}$	$\frac{\mu(\lambda + \lambda_r + \mu)}{(\lambda + \lambda_r)(\lambda + \mu) + \mu^2} \approx 1 - \frac{\lambda(\lambda + \lambda_r)}{\mu^2}$	$\approx R_{S0}(\theta)$
	$n=3$ $k=2$	$\frac{4\lambda + \lambda_r + \mu}{2\lambda(2\lambda + \lambda_r)} \approx \frac{\mu}{2\lambda(2\lambda + \lambda_r)}$	$\frac{\mu(2\lambda + \lambda_r + \mu)}{(2\lambda + \lambda_r)(2\lambda + \mu) + \mu^2} \approx 1 - \frac{2\lambda(2\lambda + \lambda_r)}{\mu^2}$	$\approx R_{S0}(\theta)$
$n-k=2$	gen. case	$\frac{v_2(v_0 + v_1 + \mu)}{v_0 v_1 v_2} + \frac{\mu(v_0 + \mu) + v_0 v_1}{v_0 v_1 v_2} \approx \frac{\mu^2}{v_0 v_1 v_2}$	$\frac{v_0 v_1 \mu + v_0 \mu^2 + \mu^3}{v_0 v_1 v_2 + v_0 v_1 \mu + v_0 \mu^2 + \mu^3} \approx 1 - \frac{v_0 v_1 v_2}{\mu^3}$	$\approx R_{S0}(\theta)$
	$n=3$ $k=1$	$\approx \frac{\mu^2}{\lambda(\lambda + \lambda_r)(\lambda + 2\lambda_r)}$	$\approx 1 - \frac{\lambda(\lambda + \lambda_r)(\lambda + 2\lambda_r)}{\mu^3}$	$\approx R_{S0}(\theta)$
	$n=5$ $k=3$	$\approx \frac{\mu^2}{3\lambda(3\lambda + \lambda_r)(3\lambda + 2\lambda_r)}$	$\approx 1 - \frac{3\lambda(3\lambda + \lambda_r)(3\lambda + 2\lambda_r)}{\mu^3}$	$\approx R_{S0}(\theta)$
$n-k$ arbitrary	$\approx \frac{\mu^{n-k}}{v_0 \dots v_{n-k}}$	$\approx 1 - \frac{v_0 \dots v_{n-k}}{\mu^{n-k+1}} \approx 1 - \frac{1/\mu}{MTTF_{S0}} = 1 - \frac{MTTR_S}{MTTF_{S0}}$	$\approx R_{S0}(\theta)$	

$v_i = k\lambda + (n-k-i)\lambda_r, i=0, \dots, n-k; \lambda, \lambda_r =$ failure rates ($\lambda_r = \lambda \rightarrow$ active red. $\Rightarrow v_0 \dots v_{n-k} = \lambda^{n-k+1} n! / (k-1)!$; $\lambda_r \equiv 0 \rightarrow$ standby redundancy $\Rightarrow v_0 \dots v_{n-k} = (k\lambda)^{n-k+1}$); $\mu =$ repair rate ($MTTR_S = 1/\mu$ because of only one repair crew, see the discussion to Eqs. (6.148) & (6.149) for *n* repair crews); $R_{S0}(\theta)$ from Eq. (6.142), see [6.5 (1985)] for exact solutions

Assuming for comparative investigations with Table 6.8, *totally independent elements* (i.e. *n* repair crews) and using PA_S for $PA_S = AA_S$, following approximate expressions can be found for *active redundancy* (see Table 6.9 or e.g. [6.27, 6.43])

$$MTTF_{S0} \approx \frac{1}{k \lambda \binom{n}{k}} (\mu/\lambda)^{n-k} \quad n \text{ repair crews, active redundancy, } \lambda/\mu \ll 1 \quad (6.148)$$

$$PA_S \approx 1 - \frac{k}{n-k+1} \binom{n}{k} (\lambda/\mu)^{n-k+1},$$

and for *standby redundancy* (see e. g. [6.43])

$$\begin{aligned}
 MTTF_{S0} &\approx \frac{(n-k)! \mu^{n-k}}{(k\lambda)^{n-k+1}} \\
 PA_S &\approx 1 - \frac{(k\lambda/\mu)^{n-k+1}}{(n-k+1)!}
 \end{aligned}
 \quad n \text{ repair crews, standby, redundancy, } \lambda/\mu \ll 1 \quad (6.149)$$

As for Eq. (A7.189), PA_S in Eq. (6.148) and Eq. (6.149) can be expressed as $PA_S \approx 1 - MTTR_S / MTTF_S$ with $MTTR_S = 1 / (n-k+1)\mu$ and $MTTF_S = MTTF_{S0}$; the same holds for the results of Tables 6.6 & 6.8, considering $MTTR_S = 1/\mu$ because of only one repair crew. Comparing results of Eq.(6.148) with those of Table 6.8 for $\lambda_r = \lambda$, one recognizes that $MTTF_{S0IE} / MTTF_{S0MS} \approx (n-k)!$ and $\overline{PA}_{SIE} / \overline{PA}_{SMS} \approx 1 / (n-k+1)!$, with $\overline{PA}_S = 1 - PA_S$; where *IE* stands for independent elements (Eq. (6.148) or Table 6.9) and *MS* for macro-structure (Tables 6.8 or 6.10).

6.5.2 *k*-out-of-*n* Redundancy with Constant Failure and Arbitrary Repair Rates

Generalization of the repair rate, by conserving *constant failure rates* (λ, λ_r) , *only one repair crew*, and *no further failure at system down*, leads to stochastic processes with $2(n-k)+1$ states, of which $n-k+1$ *regeneration* & $n-k$ *not regeneration states* (Z_0, Z_1 & Z_2 in Fig.A7.11 for $n-k=1$, Z_0, Z_1, Z_2 , & Z_2, Z_3 in Fig.A7.13 for $n-k=2$).

As an example let us consider a 2-out-of-3 *active* redundancy, i. e. a *majority redundancy*, with 3 identical elements, failure rate λ and repair time distributed according to $G(x)$ with $G(0) = 0$ and density $g(x)$. Because of the assumption of *no further failure at system down*, results of Section 6.4.2 for the 1-out-of-2 warm redundancy can be used for $n-k=1$ by setting $k\lambda$ instead of λ (see Example A7.12 and also Tab. 6.8 row $n-k=1$). For the 2-out-of-3 *active* redundancy one has to set 2λ instead of λ ($k=2$) and λ instead of λ_r (active redundancy) in Eqs. (6.108) & (6.110) to obtain Eqs. (6.152) & (6.155). However, in order to show the utility of time schedules, an alternative derivation is given below.

Using Fig. 6.14a, the following integral equation can be established for the *reliability function* $R_{S0}(t)$ (see Table 6.2 for notations)

$$\begin{aligned}
 R_{S0}(t) &= e^{-3\lambda t} + \int_0^t 3\lambda e^{-3\lambda x} e^{-2\lambda(t-x)}(1-G(t-x))dx \\
 &\quad + \int_0^t \int_0^y 3\lambda e^{-3\lambda x} g(y-x)e^{-2\lambda(y-x)} R_{S0}(t-y) dx dy. \quad (6.150)
 \end{aligned}$$

The Laplace transform of $R_{S0}(t)$ follows as

$$\tilde{R}_{S0}(s) = \frac{s + 5\lambda - 3\lambda\tilde{g}(s + 2\lambda)}{(s + 2\lambda)(s + 3\lambda) - 3\lambda(s + 2\lambda)\tilde{g}(s + 2\lambda)}, \tag{6.151}$$

and (considering $MTTF_{S0} = \tilde{R}_{S0}(0)$) the *mean time to failure* as

$$MTTF_{S0} = \frac{5 - 3\tilde{g}(2\lambda)}{6\lambda(1 - \tilde{g}(2\lambda))}. \tag{6.152}$$

For the *point availability*, Fig. 6.14b yields

$$\begin{aligned} PA_{S0}(t) &= e^{-3\lambda t} + \int_0^t 3\lambda e^{-3\lambda x} PA_{S1}(t-x) dx \\ PA_{S1}(t) &= e^{-2\lambda t}(1-G(t)) + \int_0^t g(x)e^{-2\lambda x} PA_{S0}(t-x) dx + \int_0^t g(x)(1-e^{-2\lambda x}) PA_{S1}(t-x) dx, \end{aligned} \tag{6.153}$$

from which,

$$\tilde{P\ddot{A}}_{S0}(s) = \frac{(s + 2\lambda)[1 + \tilde{g}(s + 2\lambda) - \tilde{g}(s)] + 3\lambda(1 - \tilde{g}(s + 2\lambda))}{s(s + 2\lambda)[1 + \tilde{g}(s + 2\lambda) - \tilde{g}(s)] + 3\lambda(s + 2\lambda)(1 - \tilde{g}(s))}. \tag{6.154}$$

Asymptotic & steady-state value of the point and average availability follows from

$$PA_S = AA_S = \lim_{s \rightarrow 0} s\tilde{P\ddot{A}}_{S0}(s) = \frac{3 - \tilde{g}(2\lambda)}{2\tilde{g}(2\lambda) + 6\lambda MTTR}, \tag{6.155}$$

by considering $\lim_{s \rightarrow 0} (1 - \tilde{g}(s)) = s \cdot MTTR$ as per Eq. (6.54). For the approximation of $\tilde{g}(2\lambda)$, Eq. (6.113) must be used. For the asymptotic & steady-state value of the *interval reliability*, Eq. (6.112) can be used in most applications. Generalization of failure and repair rates leads to *nonregenerative stochastic processes*.

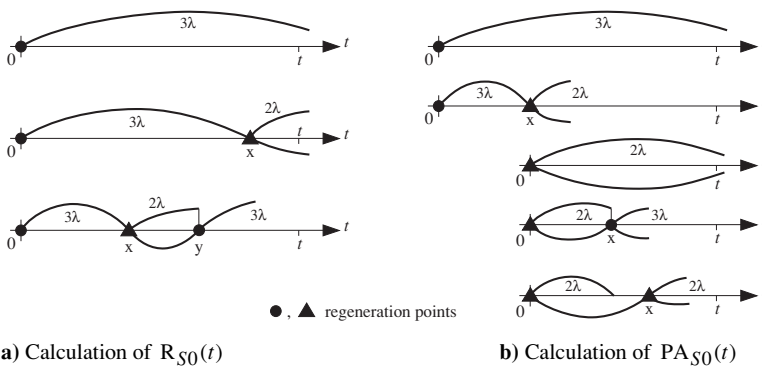


Figure 6.14 Possible time schedule for a repairable 2-out-of-3 active redundancy with 3 identical elements, constant failure rate, arbitrary repair rate, ideal failure detection & switch, one repair crew, no further failures at system down (repair times exaggerated)

6.6 Simple Series - Parallel Structures (one Repair Crew)

A *series-parallel structure* is an arbitrary combination of series and parallel models, see Table 2.1 (rows 2- 6) for some examples. Such a structure is generally investigated on a case-by-case basis using the methods of Sections 6.3– 6.5. If the time behavior can be described by a Markov or semi-Markov process, Table 6.2 can be used to establish equations for the reliability function, point availability, and interval reliability (inclusive mean time to failure and asymptotic & steady-state values).

As a first example, let us consider a repairable *1-out-of-2 active redundancy* with elements $E_1 = E_2 = E$ in series with a *switching element* E_v (see Table 6.11a on p. 248 for the case of a warm redundancy). The failure rates λ and λ_v as well as the repair rates μ and μ_v are constant (time independent). The system has only one repair crew, *repair priority* on E_v (a repair on E_1 or E_2 is stopped as soon as a failure of E_v occurs, see Example 6.12 for the case of no priority), and *no further failures at system down* (failures during a repair at system level are not considered). Figure 6.15 gives the reliability block diagram and the diagram of transition probabilities in $(t, t + \delta t]$. The *reliability function* can be calculated using Table 6.2, or directly by considering that for a series structure the reliability at system level is still the product of the reliability of the elements

$$R_{S0}(t) = R_{S0\ 1\text{-out-of-}2}(t) e^{-\lambda_v t}. \quad (6.156)$$

Because of the term $e^{-\lambda_v t}$, the Laplace transform of $R_{S0}(t)$ follows directly from the Laplace transform of the reliability function for the 1-out-of-2 parallel redundancy $R_{S0\ 1\text{-out-of-}2}$ (Eq. (6.91) with $\lambda_r = \lambda$), by replacing s with $s + \lambda_v$ (Table A9.7)

$$\tilde{R}_{S0}(s) = \frac{s + 3\lambda + \lambda_v + \mu}{(s + 2\lambda + \lambda_v)(s + \lambda + \lambda_v) + (s + \lambda_v)\mu}.$$

The *mean time to failure* $MTTF_{S0}$ follows from $MTTF_{S0} = \tilde{R}_{S0}(0)$

$$MTTF_{S0} = \frac{3\lambda + \lambda_v + \mu}{(2\lambda + \lambda_v)(\lambda + \lambda_v) + \mu\lambda_v} = \frac{1}{\lambda_v + 2\lambda^2 / (3\lambda + \lambda_v + \mu)} \approx \frac{1}{\lambda_v + 2\lambda^2 / \mu}. \quad (6.157)$$

The last part of Eq. (6.157) clearly shows the effect of the series element E_v (see Eq. (6.160) for a discussion). The *asymptotic & steady-state* value of the *point and average availability* $PA_S = AA_S$ is obtained as solution of following system of algebraic equations (Fig. 6.15 and Table 6.2)

$$\begin{aligned} P_0 &= \frac{(\mu_v P_1 + \mu P_2)}{2\lambda + \lambda_v}, & P_1 &= \frac{\lambda_v}{\mu_v} P_0, & P_3 &= \frac{\lambda_v}{\mu_v} P_2, \\ P_2 &= \frac{1}{\lambda + \lambda_v + \mu} (\mu_v P_3 + \mu P_4 + 2\lambda P_0), & P_4 &= \frac{\lambda}{\mu} P_2. \end{aligned} \quad (6.158)$$

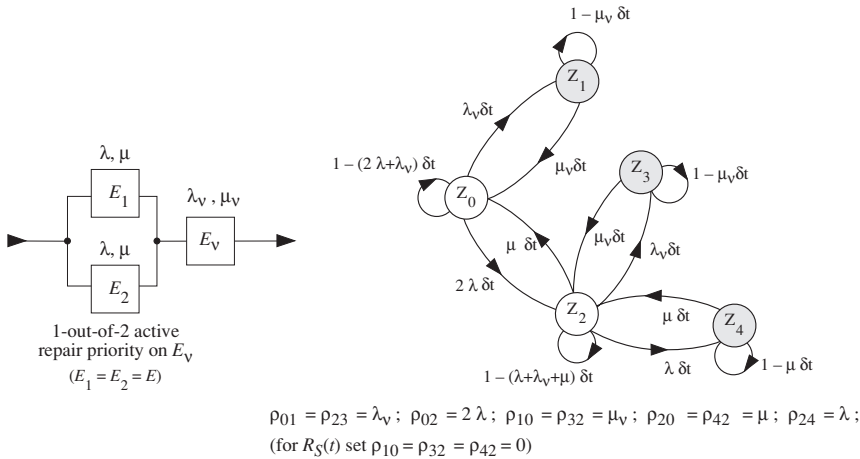


Figure 6.15 Reliability block diagram and diagram of transition probabilities in $(t, t + \delta t)$ for a repairable 1-out-of-2 active redundancy with a series (switch) element E_v , $E_1 = E_2 = E$, constant failure and repair rates $(\lambda, \lambda_v, \mu, \mu_v)$, ideal failure detection & switch, one repair crew, repair priority on E_v , no further failures at system down (Z_1, Z_3, Z_4 down states (absorbing for reliability calculation), arbitrary $t, \delta t \downarrow 0$, Markov process)

Note: The diagram of transition probabilities would have 8 states (2^3) for the case of totally independent elements ($E_1 \neq E_2$, 3 repair crews), 9 states for the case as in Fig. A7.6c, and 16 states (p. 226) for $E_1 \neq E_2$, one repair crew and repair as per *first-in first-out* (see footnote on p. 487).

For the solution of the system given by Eq. (6.158), one (arbitrarily chosen) equation must be dropped and replaced by $P_0 + P_1 + P_2 + P_3 + P_4 = 1$. The solution yields P_0 through P_4 , from which (considering $\lambda_i \ll \mu_i$ for the approximation)

$$\begin{aligned}
 PA_S = AA_S = P_0 + P_2 &= \frac{\mu^2 \mu_v + 2\lambda \mu \mu_v}{\mu^2 \mu_v + 2\lambda \mu \mu_v + 2\lambda(\lambda \mu_v + \lambda_v \mu) + \mu^2 \lambda_v} \\
 &= \frac{1}{1 + \lambda_v / \mu_v + 2(\lambda / \mu)^2 / (1 + 2\lambda / \mu)} \approx 1 - \frac{\lambda_v}{\mu_v} - \frac{2(\lambda / \mu)^2}{1 + 2\lambda / \mu}. \tag{6.159}
 \end{aligned}$$

As for the mean time to failure (Eq. (6.157)), the last part of Eq. (6.159) shows the influence of the series element E_v . This influence becomes negligible for

$$\lambda_v \ll 2\lambda^2 / \mu \quad (\lambda_v \ll (\mu_v / \mu)(2\lambda^2 / \mu) \text{ for } PA_S = AA_S). \tag{6.160}$$

For the asymptotic & steady-state value of the interval reliability it follows (Tab. 6.2)

$$IR_S(\theta) = P_0 R_{S0}(\theta) + P_2 R_{S2}(\theta) \approx PA_S \cdot R_{S0}(\theta), \tag{6.161}$$

Example 6.12

Give the reliability function and the asymptotic & steady-state value of the point and average availability for a 1-out-of-2 active redundancy in series with a switching element, as in Fig. 6.15, but *without repair priority* on the switching element.

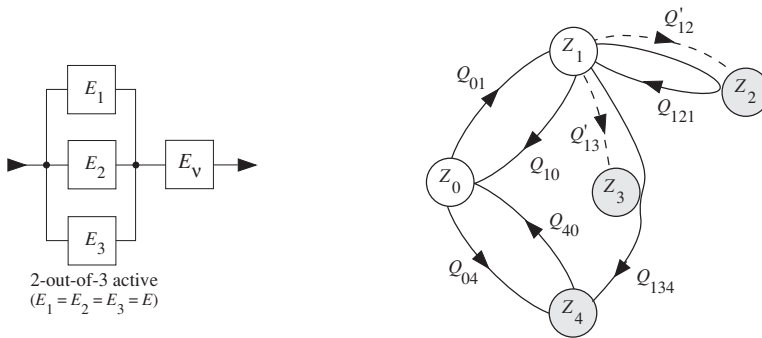


Figure 6.16 Reliability block diagram and state transition diagram for a *repairable 2-out-of-3 majority redundancy* with *constant failure rates* λ for E and λ_v for E_v , *arbitrary distributed repair times*, *ideal failure detection & switch*, *one repair crew*, *no repair priority*, *no further failures at system down* (Z_2, Z_3, Z_4 down states (absorbing for reliability calculation), Z_0, Z_1, Z_4 constitute an embedded semi-Markov process)

Solution

The diagram of transition probabilities in $(t, t + \delta t]$ of Fig. 6.15 can be used by changing the transition from state Z_3 to state Z_2 to one from Z_3 to Z_1 and μ_v in μ . The reliability function is still given by Eq. (6.156), since states Z_1, Z_3 , and Z_4 are absorbing states for reliability calculations. For the asymptotic & steady-state value of the point and average availability $PA_S = AA_S$, the system of algebraic equations (6.158) is modified to

$$P_0 = \frac{(\mu_v P_1 + \mu P_2)}{2\lambda + \lambda_v}, \quad P_1 = \frac{\lambda_v}{\mu_v} P_0 + \frac{\mu}{\mu_v} P_3, \quad P_3 = \frac{\lambda_v}{\mu} P_2, \quad P_2 = \frac{\mu P_4 + 2\lambda P_0}{\lambda + \lambda_v + \mu}, \quad P_4 = \frac{\lambda}{\mu} P_2,$$

and the solution yields (considering $P_1 + \dots + P_4 = 1$ and $\lambda_i \ll \mu_i$ for the approximation)

$$PA_S = AA_S = \frac{1}{1 + \frac{\lambda_v}{\mu_v} + \frac{2\lambda(\lambda + \lambda_v)/\mu^2}{1 + (2\lambda + \lambda_v)/\mu}} \approx 1 - \frac{\lambda_v}{\mu_v} - \frac{2\lambda(\lambda + \lambda_v)/\mu^2}{1 + (2\lambda + \lambda_v)/\mu} \approx 1 - \frac{\lambda_v}{\mu_v} - \frac{2\lambda^2}{\mu^2} \left(1 - \frac{2\lambda}{\mu}\right) - \frac{2\lambda\lambda_v}{\mu^2} \left(1 - \frac{3\lambda + \lambda_v}{\mu}\right). \tag{6.162}$$

Comparison of Eq. (6.159) with Eq. (6.162) shows the advantage ($\approx 2\lambda\lambda_v/\mu^2$) of the repair priority on E_v on the availability $PA_S = AA_S$ (no change for $MTTF_{S0}$).

As a second example let us consider a 2-out-of-3 majority redundancy (2-out-of-3 active redundancy in series with a voter E_v) with arbitrary repair rate. Assumptions (6.1) - (6.7) also hold here, in particular (6.2), i.e. *no further failures at system down*. The system has constant failure rates, λ for the three redundant elements and λ_v for the series element E_v , and repair time distributed according to $G(x)$ with $G(0) = 0$ and density $g(x)$. Figure 6.16 shows the corresponding

reliability diagram and the *state transition diagram*. Z_0 and Z_1 are up states. Z_0 , Z_1 and Z_4 are *regeneration states* and constitute a *semi-Markov process embedded* in the original process. This property will be used for the investigations. From Fig. 6.16 and Table 6.2 there follows for the *semi-Markov transition probabilities* $Q_{01}(x)$, $Q_{10}(x)$, $Q_{04}(x)$, $Q_{40}(x)$, $Q_{121}(x)$, $Q_{134}(x)$ (similar as for Figs. A7.11 - A7.13)

$$\begin{aligned}
 Q_{01}(x) &= \Pr\{\tau_{01} \leq x \cap \tau_{04} > \tau_{01}\} = \int_0^x 3\lambda e^{-3\lambda y} e^{-\lambda_v y} dy = \frac{3\lambda(1 - e^{-(3\lambda + \lambda_v)x})}{3\lambda + \lambda_v}, \\
 Q_{10}(x) &= \Pr\{\tau_{10} \leq x \cap (\tau_{12} > \tau_{10} \cap \tau_{13} > \tau_{10})\} = \int_0^x g(y) e^{-(2\lambda + \lambda_v)y} dy \\
 &= G(x) e^{-(2\lambda + \lambda_v)x} + \int_0^x (2\lambda + \lambda_v) e^{-(2\lambda + \lambda_v)y} G(y) dy, \\
 Q_{121}(x) &= \Pr\{\tau_{121} \leq x\} \\
 &= \int_0^x g(y) \int_0^y 2\lambda e^{-(2\lambda + \lambda_v)z} dz dy = \int_0^x g(y) \frac{2\lambda}{2\lambda + \lambda_v} (1 - e^{-(2\lambda + \lambda_v)y}) dy, \\
 Q_{134}(x) &= \Pr\{\tau_{134} \leq x = \int_0^x g(y) \int_0^y \lambda_v e^{-(2\lambda + \lambda_v)z} dz dy = \frac{\lambda_v}{2\lambda} Q_{121}(x), \\
 Q_{04}(x) &= \Pr\{\tau_{04} \leq x \cap \tau_{01} > \tau_{04}\} = \int_0^x \lambda_v e^{-(\lambda_v + 3\lambda)y} dy = \frac{\lambda_v}{3\lambda} Q_{01}(x), \\
 Q_{40}(x) &= \Pr\{\tau_{40} \leq x\} = G(x). \tag{6.163}
 \end{aligned}$$

$Q_{121}(x)$ is used to calculate the *point availability*. It accounts for the process returning from state Z_2 to state Z_1 and that Z_2 is *not a regeneration state* (probability for the transition $Z_1 \rightarrow Z_2 \rightarrow Z_1$, see also Fig. A7.11a), similarly for $Q_{134}(x)$. $Q'_{12}(x)$ and $Q'_{13}(x)$ as given in Fig 6.16 are *not semi-Markov transition probabilities* (Z_2 and Z_3 are *not regeneration states*). However,

$$\begin{aligned}
 Q'_{12}(x) &= \Pr\{\tau_{12} \leq x \cap (\tau_{13} > \tau_{12} \cap \tau_{10} > \tau_{12})\} = \int_0^x 2\lambda e^{-2\lambda y} e^{-\lambda_v y} (1 - G(y)) dy, \\
 Q'_{13}(x) &= \Pr\{\tau_{13} \leq x \cap (\tau_{12} > \tau_{13} \cap \tau_{10} > \tau_{13})\} = Q'_{12}(x) \lambda_v / 2\lambda,
 \end{aligned}$$

yields an equivalent $Q_1(x) = Q_{10}(x) + Q'_{12}(x) + Q'_{13}(x)$ useful for the calculation of the *reliability function*. Considering that Z_0 and Z_1 are up states and *regeneration states*, as well as the above expressions, the following system of integral equations can be established for the *reliability functions* $R_{S0}(t)$ & $R_{S1}(t)$, as per Eq. (A7.172),

$$\begin{aligned}
 R_{S0}(t) &= e^{-(3\lambda + \lambda_v)t} + \int_0^t 3\lambda e^{-(3\lambda + \lambda_v)x} R_{S1}(t - x) dx, \\
 R_{S1}(t) &= e^{-(2\lambda + \lambda_v)t} (1 - G(t)) + \int_0^t g(x) e^{-(2\lambda + \lambda_v)x} R_{S0}(t - x) dx. \tag{6.164}
 \end{aligned}$$

The system of equations (6.164) for $R_{S0}(t)$ & $R_{S1}(t)$ has a great intuitive appeal and could have been written without the use of $Q_{ij}(x)$. Its solution yields, in particular,

$$\tilde{R}_{S0}(s) = \frac{s + 5\lambda + \lambda_v - 3\lambda\tilde{g}(s + 2\lambda + \lambda_v)}{(s + 2\lambda + \lambda_v)[s + \lambda_v + 3\lambda(1 - \tilde{g}(s + 2\lambda + \lambda_v))]}, \quad (6.165)$$

and (considering $MTTF_{S0} = \tilde{R}_{S0}(0)$)

$$MTTF_{S0} = \frac{5\lambda + \lambda_v - 3\lambda\tilde{g}(2\lambda + \lambda_v)}{(2\lambda + \lambda_v)[\lambda_v + 3\lambda(1 - \tilde{g}(2\lambda + \lambda_v))]} . \quad (6.166)$$

$\tilde{R}_{S0}(s)$ and $MTTF_{S0}$ could have been obtained as for Eq. (6.157) by setting $s = s + \lambda_v$ in Eq (6.151). For the *point availability*, calculation of the transition probabilities $P_{ij}(t)$ with Table 6.2 (or Eq. (A7.169)) and Eq. (6.163) leads to

$$P_{00}(t) = e^{-(3\lambda + \lambda_v)t} + \int_0^t 3\lambda e^{-(3\lambda + \lambda_v)x} P_{10}(t-x) dx + \int_0^t \lambda_v e^{-(3\lambda + \lambda_v)x} P_{40}(t-x) dx ,$$

$$P_{10}(t) = \int_0^t g(x) e^{-(2\lambda + \lambda_v)x} P_{00}(t-x) dx \\ + \int_0^t \frac{2\lambda}{2\lambda + \lambda_v} (1 - e^{-(2\lambda + \lambda_v)x}) g(x) P_{10}(t-x) dx \\ + \int_0^t \frac{\lambda_v}{2\lambda + \lambda_v} (1 - e^{-(2\lambda + \lambda_v)x}) g(x) P_{40}(t-x) dx ,$$

$$P_{40}(t) = \int_0^t g(x) P_{00}(t-x) dx$$

$$P_{01}(t) = \int_0^t 3\lambda e^{-(3\lambda + \lambda_v)x} P_{11}(t-x) dx + \int_0^t \lambda_v e^{-(3\lambda + \lambda_v)x} P_{41}(t-x) dx ,$$

$$P_{11}(t) = e^{-(2\lambda + \lambda_v)t} (1 - G(t)) + \int_0^t g(x) e^{-(2\lambda + \lambda_v)x} P_{01}(t-x) dx \\ + \int_0^t \frac{1}{2\lambda + \lambda_v} (1 - e^{-(2\lambda + \lambda_v)x}) g(x) [2\lambda P_{11}(t-x) + \lambda_v P_{41}(t-x)] dx ,$$

$$P_{41}(t) = \int_0^t g(x) P_{01}(t-x) dx . \quad (6.167)$$

From the two systems of integral equations (6.167) it follows the *point availability* $PA_{S0}(t) = P_{00}(t) + P_{01}(t)$ and (using Laplace transform) the asymptotic & steady-state *value*

$$PA_S = AA_S = \frac{(2\lambda + \lambda_v - 2\lambda(1 - \tilde{g}(2\lambda + \lambda_v))) + 3\lambda(1 - \tilde{g}(2\lambda + \lambda_v))}{(2\lambda + \lambda_v)[1 + (3\lambda + \lambda_v)MTTR] + \lambda(\lambda_v MTTR - 2)(1 - \tilde{g}(2\lambda + \lambda_v))}, \quad (6.168)$$

with $MTTR$ as per Eq. (6.111). For $\lambda_v = 0$, Eqs. (6.166) & (6.168) yield Eqs. (6.152) & (6.155). For the asymptotic & steady-state value of the *interval reliability*, the following *approximate expression* can often be used for practical applications

$$IR_S(\theta) \approx PA_S \cdot R_{S0}(\theta), \quad (6.169)$$

with $PA_S = AA_S$ per Eq. (6.168), see Example 6.13.

Example 6.13

(i) Give using Eqs. (6.166) and (6.168) the mean time to failure $MTTF_{S0}$ and the asymptotic & steady-state point and average availability $PA_S = AA_S$ for the case of a constant repair rate $\mu \gg \lambda, \lambda_v$. (ii) Compare for the case of constant repair rate the true value of the interval reliability $IR_S(\theta)$ with the approximate expression given by Eq. (6.169).

Solution

(i) With $G(x) = 1 - e^{-\mu x}$ it follows that $\tilde{g}(2\lambda + \lambda_v) = \mu / (2\lambda + \lambda_v + \mu)$ and thus from Eq. (6.166)

$$MTTF_{S0} = \frac{5\lambda + \lambda_v + \mu}{(3\lambda + \lambda_v)(2\lambda + \lambda_v) + \mu\lambda_v} = \frac{1}{\lambda_v + 6\lambda^2 / (5\lambda + \lambda_v + \mu)} \approx \frac{1}{\lambda_v + 6\lambda^2 / \mu}, \quad (6.170)$$

and from Eq. (6.168)

$$\begin{aligned} PA_S = AA_S &= \frac{\mu(\lambda_v + \mu) + 3\lambda\mu}{(3\lambda + \lambda_v + \mu)(\lambda_v + \mu) + 3\lambda(2\lambda + \lambda_v)} = \frac{1}{1 + \frac{\lambda_v}{\mu} + \frac{3\lambda(2\lambda + \lambda_v)}{\mu(\mu + 3\lambda + \lambda_v)}} \\ &\approx 1 - \frac{\lambda_v}{\mu} - \frac{3\lambda(2\lambda + \lambda_v) / \mu^2}{1 + (3\lambda + \lambda_v) / \mu} \approx 1 - \frac{\lambda_v}{\mu} - \frac{6(\lambda / \mu)^2}{1 + 3\lambda / \mu}, \end{aligned} \quad (6.171)$$

(Eq. (6.171) follows also from Eq. (6.162) by replacing 2λ with 3λ , $1 \cdot \lambda$ with 2λ , and μ_v with μ). It can be noted that the influence of the series element E_v becomes negligible for

$$\lambda_v \ll 6\lambda^2 / \mu. \quad (6.172)$$

(ii) With $P_{00}(t)$ and $P_{01}(t)$ from Eq. (6.167) it follows for the asymptotic & steady-state value of the interval reliability (Table 6.2) that

$$IR_S(\theta) = \frac{\mu(\lambda_v + \mu)R_{S0}(\theta) + 3\lambda\mu R_{S1}(\theta)}{(3\lambda + \lambda_v + \mu)(\lambda_v + \mu) + 3\lambda(2\lambda + \lambda_v)}. \quad (6.173)$$

The *approximate expression* according to Eq. (6.169) yields

$$IR_S(\theta) \approx \frac{(\mu(\lambda_v + \mu) + 3\lambda\mu)R_{S0}(\theta)}{(3\lambda + \lambda_v + \mu)(\lambda_v + \mu) + 3\lambda(2\lambda + \lambda_v)} \approx (1 - \lambda_v / \mu)R_{S0}(\theta),$$

i.e., practically the same result as per Eq. (6.173), considering $R_{S1}(\theta) \lesssim R_{S0}(\theta)$.

To give a better feeling for the mutual influence of the different parameters involved, Figs. 6.17 and 6.18 compare the mean time to failure $MTTF_{S0}$ and the asymptotic & steady-state unavailability $1 - PA_S$ of some basic *series - parallel structures*. The equations are taken from Table 6.10 which summarizes results of Sections 6.2-6.6 for constant failure & repair rates. Comparison with Figs. 2.8 & 2.9 (nonrepairable case) confirms that the most important gain is obtained by the first step (structure b), and shows that the influence of series elements is much greater in the repairable than in the nonrepairable case (p. 46). Referring to the structures a), b), and c) of Figs. 6.17 and 6.18 the following *design rule* can be formulated:

To approach the $\mu/2\lambda_1$ MTTF gain given by the redundancy (p. 202), the failure rate of the series element in a repairable 1-out-of-2 active redundancy should not be greater than 1% (0.2% for $\mu/\lambda_1 > 500$) of the failure rate of the redundant elements; i.e.,

$$\lambda_2 < 0.01\lambda_1 \text{ in general, and } \lambda_2 < 0.002\lambda_1 \text{ for } \mu/\lambda_1 > 500. \quad (6.174)$$

6.7 Approximate Expressions for Large Series - Parallel Structures ^{*)}

6.7.1 Introduction

Reliability and availability calculation of *large series - parallel structures* rapidly becomes time-consuming, even if *constant failure rate* λ_i and *repair rate* μ_i is assumed for each element E_i of the reliability block diagram and only mean time to failure $MTTF_{S0}$ or steady-state availability $PA_S = AA_S$ is required. This is because of the large number of states involved, which for a reliability block diagram with n elements can reach $1 + \sum_{i=1}^n \prod_{k=n-i+1}^n k = n! \sum_{i=0}^n 1/i! \approx e \cdot n!$ by n different elements and repair as per first-in first-out (see e. g. Notes to Figs. 6.15 & 6.20). 2^n states holds for nonrepairable systems or for repairable system with totally independent elements (Point 1 below). Use of *approximate expressions* becomes thus important. Besides the assumption of *one repair crew and no further failure at system down* (Sections 6.2 - 6.6, partly 6.7 - 6.10), given below as Point 3, further assumptions yielding reliability & availability approximate expressions are possible for constant failure rate λ_i and constant repair rate $\mu_i \gg \lambda_i$ for each element E_i . Here some examples:

1. *Totally independent elements* (IE): If each element of the reliability block diagram operates and is repaired independently from each other (active redundancy, independent elements, one repair crew per element), series-parallel structures

^{*)} A broad literature deals with approximate expressions, mainly on limiting values for the reliability function or for the steady-state availability, see e. g. [2.34, 6.3, 6.19, 6.43, A7.10, A7.26, A7.27].

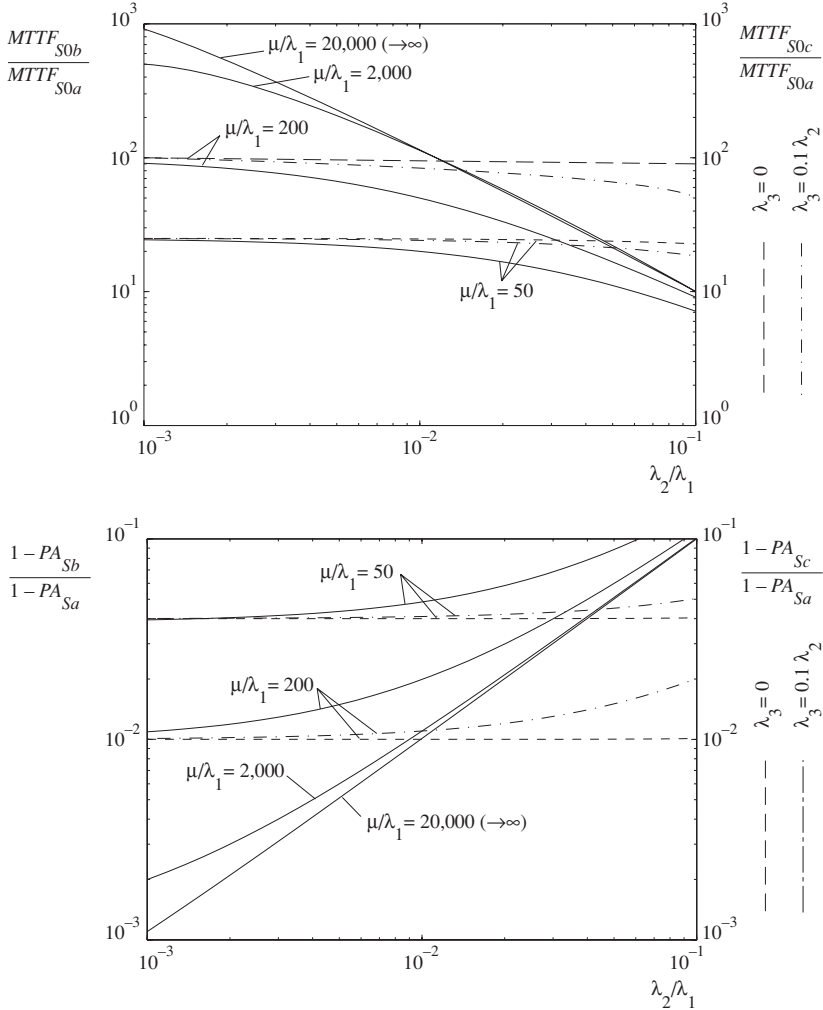
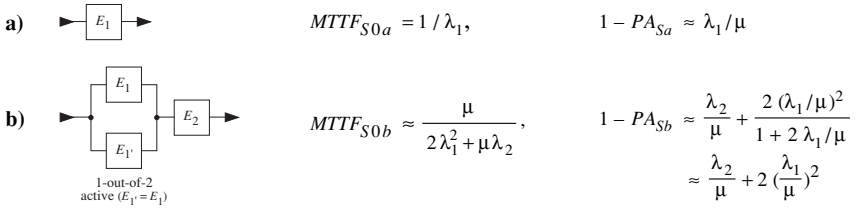


Figure 6.17 Comparison between the one-item structure and a 1-out-of-2 active redundancy with a series element: repairable, constant failure & repair rates ($\lambda_1, \lambda_2, \mu$), ideal failure detection & switch, one repair crew, repair priority on E_2 , no further failure at system down (Markov processes, λ_1 remains the same in both structures, Eqs. from Table 6.10; on the right, $MTTF_{S0c}/MTTF_{S0a}$ and $(1 - PA_{Sc})/(1 - PA_{Sa})$ with $MTTF_{S0c}$ and $1 - PA_{Sc}$ from Fig. 6.18; see Fig. 2.8 for nonrepairable)

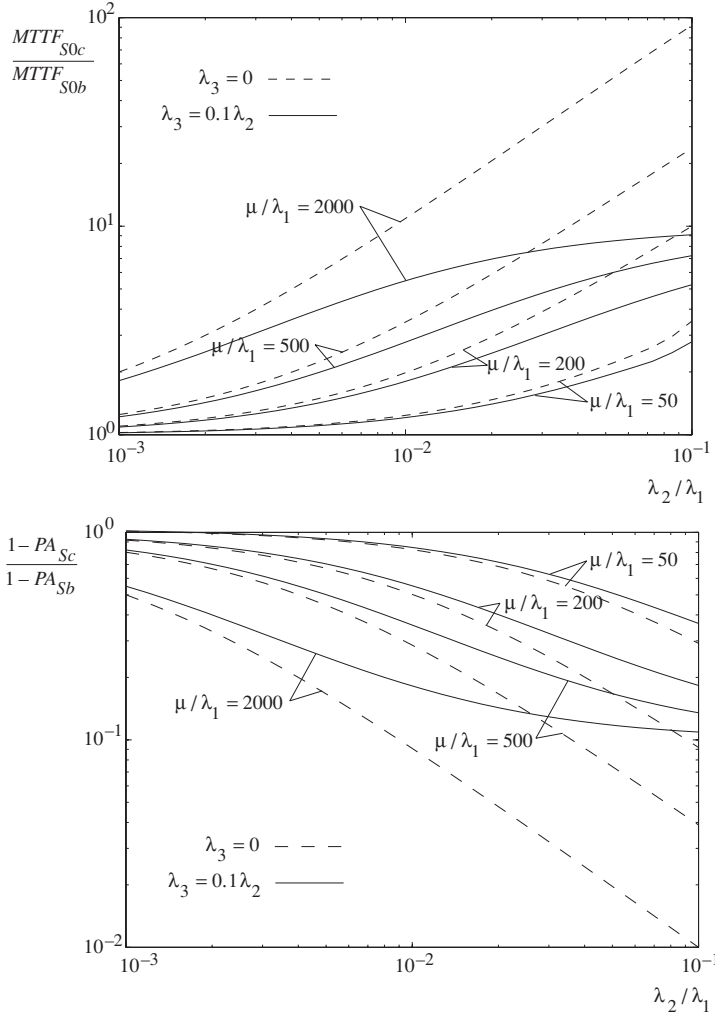
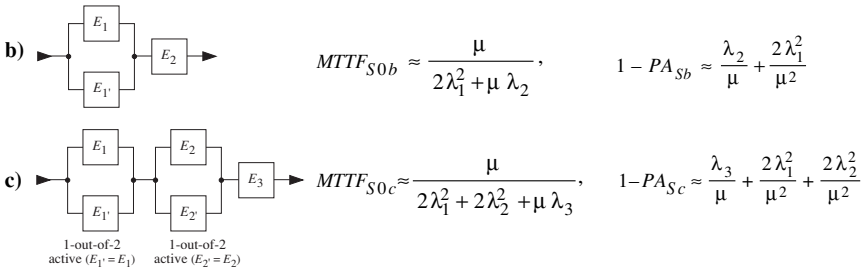


Figure 6.18 Comparison between basic series-parallel structures: repairable, active redundancy, constant failure & repair rates ($\lambda_1, \lambda_2, \lambda_3, \mu$), ideal failure detection & switch, one repair crew, repair priority on E_3 , no further failure at system down (Markov processes, λ_1 and λ_2 remain the same in both structures; equations from Table 6.10; see Fig. 2.9 for the nonrepairable case)

can be reduced to one-item structures, which are themselves successively integrated into further series - parallel structures up to the system level. To each of the one-item structure obtained, the mean time to failure $MTTF_{S0}$ and steady-state availability PA_S , calculated for the underlying series - parallel structure, are used to compute an equivalent $MTTR_S$ from $PA_S = MTTF_S / (MTTF_S + MTTR_S)$ using $MTTF_S = MTTF_{S0}$. To simplify calculations, and considering comments to Eq. (6.94), *constant failure rate* $\lambda_S = 1/MTTF_{S0}$ and *constant repair rate* $\mu_S = 1/MTTR_S$ are assumed for each of the one-item structures obtained. Table 6.9 (p.232) summarizes basic series - parallel structures based on totally independent elements (see Section 6.7.2 for a selected example).⁺⁾

2. *Macro-structures (MS)*: A macro-structure is a series, parallel, or simple series - parallel structure which is considered as a one-item structure for calculations at higher levels, integrated into further macro-structures up to system level [6.5 (1991)]. It satisfies Assumptions (6.1) - (6.7), in particular *one repair crew* for each macro-structure and *no further failures during a repair at the macro-structure level*. The procedure is similar to that of point 1 above (see also the remarks to Eqs. (4.37) and (6.94)). Table 6.10 (p. 233) summarizes basic macro-structures useful for practical applications (see Section 6.7.2 for a selected example).⁺⁾
3. *One repair crew and no further failures at system down (no FF)*: Assumptions (6.3) & (6.2), valid for all models of Sections 6.2 - 6.7 (except Eqs. (6.148), (6.149)) apply in many practical situations. No further failures at system down means that failures during a repair at system level are not considered. This assumption has *no influence on the reliability function* at system level and its *influence on the availability is limited* if $\lambda \ll \mu$ holds for each element.
4. *Cutting states*: Removing the states with more than k failures from the diagram of transition probabilities in $(t, t + \delta t]$ (or the state transition diagram) produces in general an important reduction of the state diagram. The choice of k (often $k = 2$) is based on the required precision. An upper bound on the error for the asymptotic & steady-state availability $PA_S = AA_S$ (based on the mapping of states with k failures at system level in state Z_k of a birth & death process and using Eq. (A7.157) ($P_k > \sum_{i=k+1}^n P_i$)) has been introduced in [2.50 (1992)].
5. *Clustering of states*: Grouping of elements in the reliability block diagram or of states in the diagram of transition probabilities in $(t, t + \delta t]$ produces in general an important reduction of the number of states in the state diagram.

Combination of the above methods is possible, see also Sections 6.8.9 & 6.9.7 and the footnote on p. 226 for further considerations. However, as a basic rule,

series elements must be grouped before any analysis (2nd row of Table 6.10).

⁺⁾ Methods 1 & 2 apply for constant failure & repair rates for each element, yielding approximately *constant failure & repair rates* (λ_S, μ_S) for the reduced structure (Eqs. (6.88), (6.94), (6.48)).

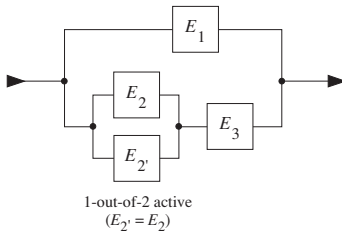


Figure 6.19 Basic reliability block diagram for a repairable uninterruptible electrical power supply

Considering that the steady-state probability for states with more than one failure decreases rapidly as the number of failures increases ($\sim \lambda/\mu$ for each failure, see e. g. pp. 237 and 269 and the corresponding Figs. 6.20 and 6.34), all methods given above yield good *approximate expressions* for $MTTF_{S0}$ and PA_S in practical applications. However, referring to the *unavailability* $1 - PA_S$, method 1 above can deliver lower values, for instance a factor 2 with an order of magnitude $(\lambda/\mu)^2$ for a 1-out-of-2 active redundancy (compare Tables 6.9 & 6.10). Analytical comparison of the above methods is difficult, in general. Numerical investigations show a close convergence of the results given by the different methods, as illustrated for instance in Section 6.7.2 (p. 237) for a practical example with low values for μ/λ .

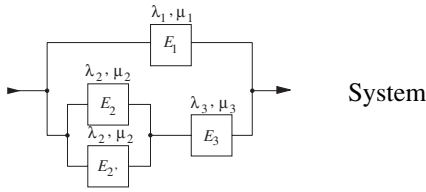
6.7.2 Application to a Practical Example

To illustrate how methods 1 to 3 of Section 6.7.1 work, let us consider the system with a reliability block diagram as in Fig. 6.19, and assume system new at $t = 0$, active redundancy, constant failure rates $\lambda_1 - \lambda_3$, constant repair rates $\mu_1 - \mu_3$, $\lambda_i \ll \mu_i$, repair priority E_1, E_3, E_2 [6.5 (1988)]. Except for some series elements (to be considered separately in a final step), the reliability block diagram of Fig. 6.19 describes an uninterruptible power supply (UPS) used for instance to buffer electrical power network failures in computer systems (E_1 being the power network).⁺⁾

Although limited to 4 elements, the stochastic process describing the system of Fig. 6.19 would contain up to 65 states if the assumption of *no further failure at system down* were dropped (pp. 226, 235). Assuming no further failure at system down, the state space is reduced to 12 states (Fig. 6.20). In the following, the mean time to failure ($MTTF_{S0}$) and the asymptotic & steady-state point and average availability ($PA_S = AA_S$) of the system given by Fig. 6.19 is investigated using method 1 (Table 6.9), method 2 (Table 6.10), and method 3 (Table 6.2) of Section 6.7.1. For a numerical comparison, results are given on p. 237 (also for method 4 and for the exact solution obtained by dropping the assumption of no further failure at system down), showing that all methods used deliver good approximate expressions.

⁺⁾ A refinement to include the battery discharge has been investigated in [6.47 (2002)].

Method 1 of Section 6.7.1 yields, using Table 6.9,



System

$$\lambda_5 \approx \frac{2\lambda_2^2}{\mu_2}, \quad \mu_5 = 2\mu_2, \quad (6.175)$$

$$\lambda_6 \approx \lambda_3 + \lambda_5, \quad \mu_6 \approx \frac{\lambda_5 + \lambda_3}{\lambda_5/\mu_5 + \lambda_3/\mu_3}, \quad (6.176)$$

$$\lambda_S \approx \frac{\lambda_1 \lambda_6 (\mu_1 + \mu_6)}{\mu_1 \mu_6}, \quad \mu_S \approx \mu_1 + \mu_6. \quad (6.177)$$

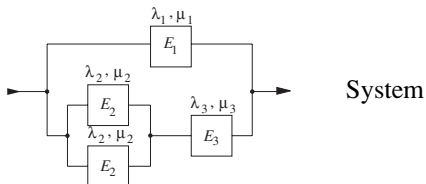
From Eqs. (6.175) – (6.177) it follows that

$$1 / MTTF_{S0} \equiv \lambda_S \approx \lambda_1 \left[\frac{\lambda_3}{\mu_1} + \frac{2\lambda_2^2}{\mu_1 \mu_2} + \frac{\lambda_3}{\mu_3} + \left(\frac{\lambda_2}{\mu_2}\right)^2 \right], \quad (6.178)$$

and

$$PA_S \approx 1 - \frac{\lambda_S}{\mu_S} \approx 1 - \frac{\lambda_1}{\mu_1} \left[\frac{\lambda_3}{\mu_3} + \left(\frac{\lambda_2}{\mu_2}\right)^2 \right]. \quad (6.179)$$

Method 2 of Section 6.7.1 yields, using Table 6.10,



System

Table 6.9 Basic structures to investigate *large series-parallel systems* by assuming *totally independent elements* (each element operates and is repaired independently from every other element): *active redundancy, constant failure & repair rates* ($\lambda_i \ll \mu_i$), *ideal failure detection & switch*, *n repair crews* (one for each element), Markov processes (for rows 1 to 5 see Table 6.4, Eqs. (6.60) & (2.48), (6.99) & (2.48), (6.170) with $\lambda_v=0$ & (2.48), and (6.148), respectively; $\lambda_S \equiv 1/MTTF_{S0}$ and $\mu_S \equiv 1/MTTR_S = \lambda_S / (1 - PA_S)$ used to simplify the notation; $PA_S = AA_S$)

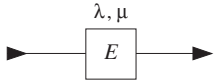
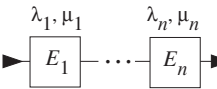
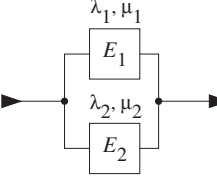
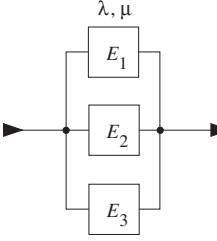
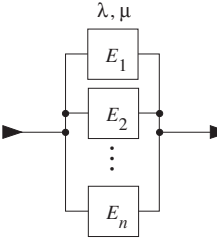
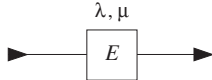
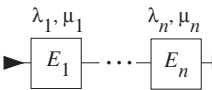
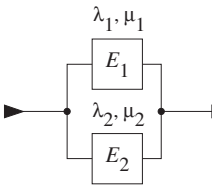
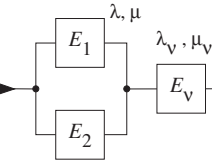
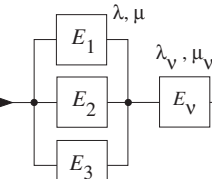
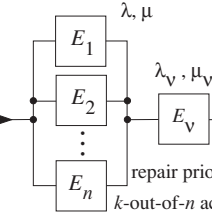
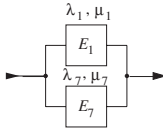
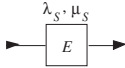
	$\lambda_S \equiv 1/MTTF_{S0} = \lambda, \quad \mu_S = \mu, \quad PA_S = \mu / (\mu + \lambda) = \mu_S / (\mu_S + \lambda_S) \approx 1 - \lambda_S / \mu_S$ $\Rightarrow \mu_S \equiv 1/MTTR_S = \frac{\lambda_S PA_S}{1 - PA_S} \approx \frac{\lambda_S}{1 - PA_S}$
	$\lambda_S \equiv 1/MTTF_{S0} = \lambda_1 + \dots + \lambda_n, \quad \Rightarrow \mu_S \approx \frac{\lambda_S}{1 - PA_S} \approx \frac{\lambda_1 + \dots + \lambda_n}{\lambda_1 / \mu_1 + \dots + \lambda_n / \mu_n}$ $PA_S = PA_1 \dots PA_n = \frac{\mu_1}{\mu_1 + \lambda_1} \dots \frac{\mu_n}{\mu_n + \lambda_n} \approx 1 - \left(\frac{\lambda_1}{\mu_1} + \dots + \frac{\lambda_n}{\mu_n} \right)$
 <p>1-out-of-2 (active)</p>	$\frac{1}{\lambda_S} \equiv MTTF_{S0} = \frac{(\lambda_1 + \lambda_2 + \mu_1)(\lambda_1 + \lambda_2 + \mu_2) - \lambda_1 \lambda_2}{\lambda_1 \lambda_2 (\lambda_1 + \lambda_2 + \mu_1 + \mu_2)} \approx \frac{\mu_1 \mu_2}{\lambda_1 \lambda_2 (\mu_1 + \mu_2)}$ $PA_S = PA_1 + PA_2 - PA_1 PA_2 = \frac{\mu_1 \mu_2 + \mu_1 \lambda_2 + \mu_2 \lambda_1}{(\mu_1 + \lambda_1)(\mu_2 + \lambda_2)} \approx 1 - \frac{\lambda_1 \lambda_2}{\mu_1 \mu_2}$ $\Rightarrow \mu_S \approx \frac{\lambda_S}{1 - PA_S} \approx \mu_1 + \mu_2$
 <p>2-out-of-3 active ($E_1 = E_2 = E_3 = E$)</p>	$1 / \lambda_S \equiv MTTF_{S0} = \frac{5 \lambda + \mu}{6 \lambda^2} \approx \frac{\mu}{6 \lambda^2}$ $PA_S = 3 PA^2 - 2 PA^3 \approx 1 - \frac{3 (\lambda / \mu)^2}{1 + 3 \lambda / \mu} \approx 1 - 3 \left(\frac{\lambda}{\mu} \right)^2$ $\Rightarrow \mu_S \approx \frac{\lambda_S}{1 - PA_S} \approx 2 \mu$
 <p>k-out-of-n active ($E_1 = \dots = E_n = E$)</p>	$1 / \lambda_S \equiv MTTF_{S0} \approx \frac{1}{k \lambda} \binom{n}{k} \left(\frac{\mu}{\lambda} \right)^{n-k}$ $PA_S \approx 1 - \frac{k}{n-k+1} \binom{n}{k} \left(\frac{\lambda}{\mu} \right)^{n-k+1}$ $\Rightarrow \mu_S \approx \frac{\lambda_S}{1 - PA_S} \approx (n-k+1) \mu$

Table 6.10 Basic macro-structures to investigate large series-parallel systems by successive building of macro-structures bottom up to system level, independent elem., active redundancy, const. failure & repair rates ($\lambda_i \ll \mu_i$), ideal failure detection & switch, one repair crew per macro-structure, repair priority on E_v , no further failure at macro-structure down, Markov proc. (for rows 1-6 see Table 6.4, Eqs. (6.60) & (6.65), (6.100) & (6.103), (6.157) & (6.159), (6.170) & (6.171), and (6.60), (6.65) & Tab. 6.8, resp.; $\lambda_S \equiv 1/MTTF_{S0}$, $\mu_S \equiv 1/MTTR_S \approx \lambda_S/(1-PA_S)$ used to simplify the notation; $PA_S = AA_S$)

	$\lambda_S \equiv 1/MTTF_{S0} = \lambda, \mu_S = \mu, PA_S = \mu/(\mu + \lambda) = \mu_S/(\mu_S + \lambda_S) \approx 1 - \lambda_S/\mu_S$ $\Rightarrow \mu_S \equiv 1/MTTR_S = \frac{\lambda_S PA_S}{1 - PA_S} \approx \frac{\lambda_S}{1 - PA_S}$
	$\lambda_S \equiv 1/MTTF_{S0} = \lambda_1 + \dots + \lambda_n, PA_S \approx 1 - (\lambda_1/\mu_1 + \dots + \lambda_n/\mu_n)$ $\Rightarrow \mu_S \approx \frac{\lambda_S}{1 - PA_S} \approx \frac{\lambda_1 + \dots + \lambda_n}{\lambda_1/\mu_1 + \dots + \lambda_n/\mu_n} \quad (\approx \mu \text{ for } \mu_1 = \dots = \mu_n = \mu)$
 <p>1-out-of-2 (active)</p>	$1/\lambda_S \equiv MTTF_{S0} \approx \mu_1 \mu_2 / (\lambda_1 \lambda_2 (\mu_1 + \mu_2))$ $PA_S \approx 1 - \frac{\lambda_1 \lambda_2}{\mu_1^2 \mu_2^2} (\mu_1^2 + \mu_2^2)$ $\Rightarrow \mu_S \approx \frac{\lambda_S}{1 - PA_S} \approx \mu_1 \mu_2 \frac{\mu_1 + \mu_2}{\mu_1^2 + \mu_2^2} \quad (\approx \mu \text{ for } \mu_1 = \mu_2)$
 <p>1-out-of-2 active ($E_1 = E_2 = E$) repair priority on E_v</p>	$1/\lambda_S \equiv MTTF_{S0} = 1/(\lambda_v + 2\lambda^2/(\mu + 3\lambda + \lambda_v)) \approx 1/(\lambda_v + 2\lambda^2/\mu)$ $PA_S \approx 1 - \frac{\lambda_v}{\mu_v} - \frac{2(\lambda/\mu)^2}{1 + 2\lambda/\mu}$ $\Rightarrow \mu_S \approx \frac{\lambda_S}{1 - PA_S} \quad (\approx \mu_v \text{ for } \mu_v = \mu)$
 <p>2-out-of-3 active ($E_1 = E_2 = E_3 = E$) repair priority on E_v</p>	$1/\lambda_S \equiv MTTF_{S0} \approx 1/(\lambda_v + 6\lambda^2/\mu)$ $PA_S \approx 1 - \frac{\lambda_v}{\mu_v} - \frac{6(\lambda/\mu)^2}{1 + 3\lambda/\mu}$ $\Rightarrow \mu_S \approx \frac{\lambda_S}{1 - PA_S} \approx \mu_v \frac{\lambda_v + 6\lambda^2/\mu}{\lambda_v + \frac{6\lambda^2/\mu}{1 + 3\lambda/\mu} \cdot \frac{\mu_v}{\mu}}$ $(\approx \mu_v \text{ for } \mu_v = \mu)$
 <p>k-out-of-n active ($E_1 = \dots = E_n = E$) repair priority E_v</p>	$1/\lambda_S \equiv MTTF_{S0} \approx 1/(\lambda_v + \lambda \frac{n!}{(k-1)!} (\frac{\lambda}{\mu})^{n-k})$ $PA_S \approx 1 - \frac{\lambda_v}{\mu_v} - \frac{n!}{(k-1)!} (\frac{\lambda}{\mu})^{n-k+1}$ $\Rightarrow \mu_S \approx \frac{\lambda_S}{1 - PA_S} \quad (\approx \mu_v \text{ for } \mu_v = \mu)$



$$\lambda_7 \approx \lambda_3 + 2\lambda_2^2 / \mu_2, \quad \mu_7 \approx \frac{\mu_3 (2\lambda_2^2 + \mu_2 \lambda_3) (1 + 2\lambda_2 / \mu_2)}{\mu_2 \lambda_3 + 2\lambda_2 \lambda_3 + 2\lambda_2^2 \mu_3 / \mu_2}, \quad (6.180)$$



$$\lambda_s \approx \frac{\lambda_1 \lambda_7 (\mu_1 + \mu_7)}{\mu_1 \mu_7}, \quad \mu_s \approx \mu_1 \mu_7 \frac{\mu_1 + \mu_7}{\mu_1^2 + \mu_7^2}. \quad (6.181)$$

From Eqs. (6.180) and (6.181) it follows that

$$\frac{1}{MTTF_{S0}} \equiv \lambda_s \approx \lambda_1 \left(\frac{2\lambda_2^2 + \mu_2 \lambda_3}{\mu_1 \mu_2} + \frac{\mu_2 \lambda_3 + 2\lambda_2 \lambda_3 + 2\mu_3 \lambda_2^2 / \mu_2}{\mu_2 \mu_3 (1 + 2\lambda_2 / \mu_2)} \right) \approx \lambda_1 \left(\frac{\lambda_3}{\mu_1} + \frac{\lambda_3}{\mu_3} \right), \quad (6.182)$$

and

$$\begin{aligned} PA_S &\approx 1 - \frac{\lambda_s}{\mu_s} \approx 1 - \frac{2\lambda_2^2 + \mu_2 \lambda_3}{\mu_2} \left(\frac{\lambda_1}{\mu_1^2} + \frac{\lambda_1 (\mu_2 \lambda_3 + 2\lambda_2 \lambda_3 + 2\mu_3 \lambda_2^2 / \mu_2)^2}{(2\lambda_2^2 + \mu_2 \lambda_3)^2 (1 + 2\lambda_2 / \mu_2)^2 \mu_3^2} \right) \\ &\approx 1 - \frac{\lambda_1 \lambda_2 \lambda_3}{\mu_1 \mu_2 \mu_3} \left(\frac{\mu_2}{\lambda_2} + 2 \frac{\lambda_2}{\lambda_3} \right) \left(\frac{\mu_3}{\mu_1} + \frac{(\mu_2 \lambda_3 + 2\lambda_2 \lambda_3 + 2\mu_3 \lambda_2^2 / \mu_2)^2 \mu_1 / \mu_3}{(2\lambda_2^2 + \mu_2 \lambda_3)^2 (1 + 2\lambda_2 / \mu_2)^2} \right) \\ &\approx 1 - \frac{\lambda_1 \lambda_3}{\mu_3^2} \left(1 + \frac{\mu_3}{\mu_1} \right). \end{aligned} \quad (6.183)$$

Method 3 of Section 6.7.1 yields, using Table 6.2 and Fig. 6.20, the following system of algebraic equations for the mean time to failure ($M_i = MTTF_{Si}$)

$$\begin{aligned} \rho_0 M_0 &= 1 + \lambda_1 M_1 + 2\lambda_2 M_2 + \lambda_3 M_3, & \rho_1 M_1 &= 1 + \mu_1 M_0 + 2\lambda_2 M_7, \\ \rho_2 M_2 &= 1 + \mu_2 M_0 + \lambda_3 M_4 + \lambda_2 M_6 + \lambda_1 M_7, & \rho_3 M_3 &= 1 + \mu_3 M_0 + 2\lambda_2 M_4, \\ \rho_4 M_4 &= 1 + \mu_3 M_2 + \lambda_2 M_5, & \rho_5 M_5 &= 1 + \mu_3 M_6, \\ \rho_6 M_6 &= 1 + \mu_2 M_2 + \lambda_3 M_5, & \rho_7 M_7 &= 1 + \mu_1 M_2, \end{aligned} \quad (6.184)$$

where

$$\begin{aligned} \rho_0 &= \lambda_1 + 2\lambda_2 + \lambda_3, & \rho_1 &= \mu_1 + 2\lambda_2 + \lambda_3, & \rho_2 &= \mu_2 + \lambda_1 + \lambda_2 + \lambda_3, \\ \rho_3 &= \mu_3 + 2\lambda_2 + \lambda_1, & \rho_4 &= \mu_3 + \lambda_2 + \lambda_1, & \rho_5 &= \mu_3 + \lambda_1, \\ \rho_6 &= \mu_2 + \lambda_3 + \lambda_1, & \rho_7 &= \mu_1 + \lambda_3 + \lambda_2, & \rho_8 &= \mu_1, \\ \rho_9 &= \mu_1, & \rho_{10} &= \mu_1, & \rho_{11} &= \mu_1. \end{aligned} \quad (6.185)$$

From Eqs. (6.184) and (6.185) it follows that

$$1 / \lambda_s \equiv MTTF_{S0} = \frac{a_5 + a_6 (a_8 + a_9 a_{10}) + a_7 a_{10}}{1 - a_6 a_{12} - a_{11} (a_7 + a_6 a_9)}, \quad (6.186)$$

with

$$\begin{aligned}
 a_1 &= \frac{1}{\rho_4} + \frac{\lambda_2}{\rho_4 \rho_5} (1 + \mu_3 \frac{\lambda_3 + \rho_5}{\rho_5 \rho_6 - \lambda_3 \mu_3}), & a_2 &= \frac{\lambda_2 \mu_2 \mu_3}{\rho_4 (\rho_5 \rho_6 - \lambda_3 \mu_3)} + \frac{\mu_3}{\rho_4}, \\
 a_3 &= \frac{1}{\rho_3} (1 + 2\lambda_2 a_1), & a_4 &= \frac{2\lambda_2}{\rho_3} a_2, & a_5 &= \frac{1 + \lambda_3 a_3}{\rho_0 - \lambda_3 \mu_3 / \rho_3}, \\
 a_6 &= \frac{\lambda_1}{\rho_0 - \lambda_3 \mu_3 / \rho_3}, & a_7 &= \frac{2\lambda_2 + \lambda_3 a_4}{\rho_0 - \lambda_3 \mu_3 / \rho_3}, & a_8 &= \frac{1 + 2\lambda_2 / \rho_7}{\rho_1}, \\
 a_9 &= \frac{2\lambda_2 \mu_1}{\rho_1 \rho_7}, & a_{10} &= \frac{1 + \lambda_3 a_1 + (\lambda_2 \lambda_3 + \lambda_2 \rho_3) / (\rho_5 \rho_6 - \lambda_3 \mu_3) + \lambda_1 / \rho_7}{\rho_2 - \lambda_3 a_2 - \lambda_2 \mu_2 \rho_5 / (\rho_5 \rho_6 - \lambda_3 \mu_3) - \lambda_1 \mu_1 / \rho_7}, \\
 a_{11} &= \frac{\mu_2}{\rho_2 - \lambda_3 a_2 - \lambda_2 \mu_2 \rho_5 / (\rho_5 \rho_6 - \lambda_3 \mu_3) - \lambda_1 \mu_1 / \rho_7}, & a_{12} &= \frac{\mu_1}{\rho_1}. \quad (6.187)
 \end{aligned}$$

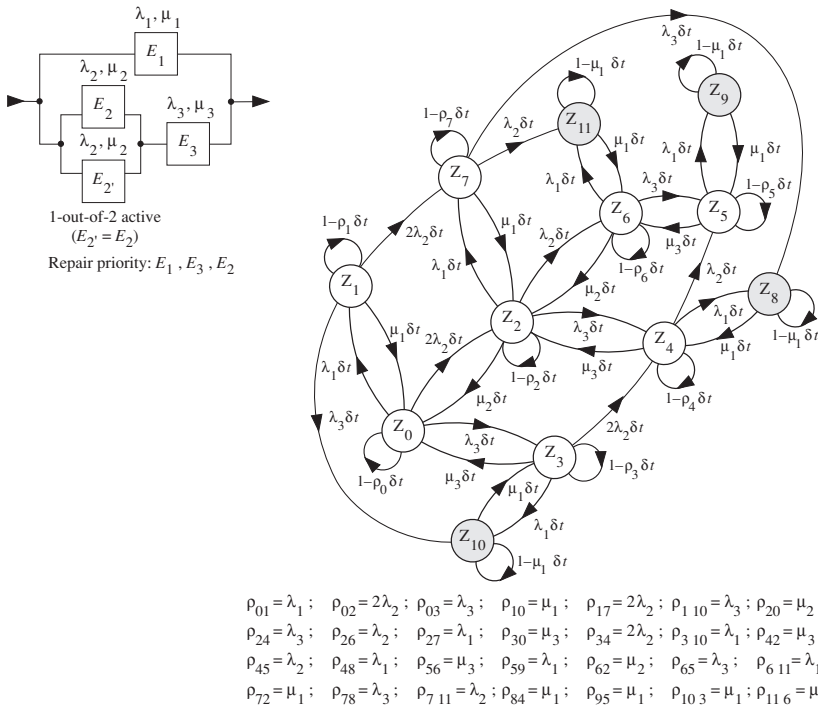


Figure 6.20 Reliability block diagram and diagram of transition probabilities in $(t, t + \delta t]$ for the system described by Fig. 6.19 with active redundancy, const. failure & repair rates (λ_i, μ_i) , ideal failure detection & switch, one repair crew, repair priority in the sequence E_1, E_2, E_3 , no further failures at system down (Z_8, Z_9, Z_{10}, Z_{11} down states (absorbing for reliability calculation), arbitrary $t, \delta t \downarrow 0$, Markov process, $\rho_i = \sum_j \rho_{ij}$; $1+3+4+3+1=12$ states (4 with 2 failed elements))
Note: The diagram of transition probabilities would have $1+4+6+3+1=15$ states for $E_2 \neq E_2'$, $2^4=16$ states for totally independent elements (4 repair crews and possible failures at system down), and 65 states for $E_2 \neq E_2'$, one repair crew & repair as per first-in-first-out.

Similarly, for the *asymptotic & steady-state* value of the point and average availability $PA_S = AA_S$ the following system of algebraic equations, can be obtained using Table 6.2 and Fig. 6.20

$$\begin{aligned}
 \rho_0 P_0 &= \mu_1 P_1 + \mu_2 P_2 + \mu_3 P_3, & \rho_1 P_1 &= \lambda_1 P_0, \\
 \rho_2 P_2 &= 2\lambda_2 P_0 + \mu_3 P_4 + \mu_2 P_6 + \mu_1 P_7, & \rho_3 P_3 &= \lambda_3 P_0 + \mu_1 P_{10}, \\
 \rho_4 P_4 &= \lambda_3 P_2 + 2\lambda_2 P_3 + \mu_1 P_8, & \rho_5 P_5 &= \lambda_2 P_4 + \lambda_3 P_6 + \mu_1 P_9, \\
 \rho_6 P_6 &= \lambda_2 P_2 + \mu_3 P_5 + \mu_1 P_{11}, & \rho_7 P_7 &= 2\lambda_2 P_1 + \lambda_1 P_2, \\
 \rho_8 P_8 &= \lambda_1 P_4 + \lambda_3 P_7, & \rho_9 P_9 &= \lambda_1 P_5, \\
 \rho_{10} P_{10} &= \lambda_3 P_1 + \lambda_1 P_3, & \rho_{11} P_{11} &= \lambda_1 P_6 + \lambda_2 P_7.
 \end{aligned} \tag{6.188}$$

with ρ_i as in Eq. (6.185). One (arbitrarily chosen) of the Eqs. (6.188) must be dropped and replaced by $P_0 + P_1 + \dots + P_{11} = 1$. The solution yields P_0 to P_{11} , from which

$$PA_S = P_0 + \dots + P_7 = P_0(1 + b_1 + b_2 + b_3 + b_4 + b_5 + b_6 + b_7), \tag{6.189}$$

with

$$P_0 = 1 / (1 + \sum_{i=1}^{11} b_i) \tag{6.190}$$

and

$$\begin{aligned}
 b_1 &= \frac{\lambda_1}{\rho_1}, & b_2 &= \frac{\rho_0 - \lambda_1 \mu_1 / \rho_1}{\mu_2} - \frac{\mu_3 \lambda_3 (1 + \lambda_1 / \rho_1)}{(\mu_3 + 2\lambda_2) \mu_2}, \\
 b_3 &= \frac{\lambda_3 (1 + \lambda_1 / \rho_1)}{\mu_3 + 2\lambda_2}, & b_4 &= \frac{\lambda_3 b_2 (1 + \lambda_1 / \rho_7) + 2\lambda_2 b_3 + 2\lambda_1 \lambda_2 \lambda_3 / \rho_7 \rho_1}{\rho_4 - \lambda_1}, \\
 b_5 &= \frac{\lambda_2 b_4 + \frac{\lambda_2 \lambda_3}{\rho_7 (\mu_2 + \lambda_3)} (b_2 (\rho_7 + \lambda_1) + 2\lambda_1 \lambda_2 / \rho_1)}{\rho_5 - \lambda_1 - \mu_3 \lambda_3 / (\mu_2 + \lambda_3)}, & b_7 &= \frac{2\lambda_1 \lambda_2}{\rho_1 \rho_7} + \frac{\lambda_1}{\rho_7} b_2, \\
 b_6 &= \frac{\lambda_2}{\mu_2 + \lambda_3} (b_2 + \frac{2\lambda_1 \lambda_2}{\rho_1 \rho_7} + \frac{\lambda_1}{\rho_7} b_2 + \frac{\mu_3}{\lambda_2} b_5), & b_8 &= \frac{\lambda_1}{\mu_1} b_4 + \frac{\lambda_3}{\mu_1} b_7, \\
 b_9 &= \frac{\lambda_1}{\mu_1} b_5, & b_{10} &= \frac{\lambda_3 \lambda_1}{\mu_1 \rho_1} + \frac{\lambda_1}{\mu_1} b_3, & b_{11} &= \frac{\lambda_1}{\mu_1} b_6 + \frac{\lambda_2}{\mu_1} b_7.
 \end{aligned} \tag{6.191}$$

An analytical comparison of Eqs. (6.186) with Eqs. (6.178) and (6.182) or of Eq. (6.189) with Eqs. (6.179) and (6.183) is time consuming. Numerical evaluation yields (λ and μ in h^{-1} , *MTTF* in h)

λ_1	1/100	1/100	1/1,000	1/1,000
λ_2	1/1,000	1/1,000	1/10,000	1/10,000
λ_3	1/10,000	1/10,000	1/100,000	1/100,000
μ_1	1	1/5	1	1/5
μ_2	1/5	1/5	1/5	1/5
μ_3	1/5	1/5	1/5	1/5
$MTTF_{S_0}$ (Eq. (6.178), totally IE) \approx	$1.58 \cdot 10^{+5}$	$9.30 \cdot 10^{+4}$	$1.66 \cdot 10^{+7}$	$9.93 \cdot 10^{+6}$
$MTTF_{S_0}$ (Eq. (6.182), MS) \approx	$1.53 \cdot 10^{+5}$	$9.14 \cdot 10^{+4}$	$1.65 \cdot 10^{+7}$	$9.91 \cdot 10^{+6}$
$MTTF_{S_0}$ (Eq. (6.186), no FF) \approx	$1.59 \cdot 10^{+5}$	$9.33 \cdot 10^{+4}$	$1.66 \cdot 10^{+7}$	$9.93 \cdot 10^{+6}$
$MTTF_{S_0}$ (Method 4, Cutting) \approx	$1.49 \cdot 10^{+5}$	$9.29 \cdot 10^{+4}$	$1.65 \cdot 10^{+7}$	$9.92 \cdot 10^{+6}$
$MTTF_{S_0}$ (only one repair crew) \approx	$1.60 \cdot 10^{+5}$	$9.33 \cdot 10^{+4}$	$1.66 \cdot 10^{+7}$	$9.93 \cdot 10^{+6}$
$1 - PA_S$ (Eq. (6.179), totally IE) \approx	$5.25 \cdot 10^{-6}$	$2.63 \cdot 10^{-5}$	$5.03 \cdot 10^{-8}$	$2.51 \cdot 10^{-7}$
$1 - PA_S$ (Eq. (6.183), MS) \approx	$2.81 \cdot 10^{-5}$	$5.45 \cdot 10^{-5}$	$2.62 \cdot 10^{-7}$	$5.05 \cdot 10^{-7}$
$1 - PA_S$ (Eq. (6.189), no FF) \approx	$6.61 \cdot 10^{-6}$	$6.00 \cdot 10^{-5}$	$6.06 \cdot 10^{-8}$	$5.06 \cdot 10^{-7}$
$1 - PA_S$ (Method 4, Cutting) \approx	$2.99 \cdot 10^{-5}$	$5.56 \cdot 10^{-5}$	$2.65 \cdot 10^{-7}$	$5.06 \cdot 10^{-7}$
$1 - PA_S$ (only one repair crew) \approx	$6.58 \cdot 10^{-6}$	$5.63 \cdot 10^{-5}$	$6.06 \cdot 10^{-8}$	$5.06 \cdot 10^{-7}$

Also given in the above numerical comparison are the results obtained by method 4 of Section 6.7.1 (for a given precision of 10^{-8} on the unavailability $1 - PA_S$) and by dropping the assumption of no further failures at system down in method 3. These results confirm that for $\lambda_i \ll \mu_i$ good approximate expressions for practical applications can be obtained from all the methods presented in Section 6.7.1. The influence of λ_i / μ_i appears, for instance, when comparing columns 1 with 2 and columns 3 with 4. The results obtained with method 1 of Section 6.7.1 (Eqs. (6.178) and (6.179)) give higher values for $MTTF_{S_0}$ and PA_S than those obtained with method 2 (Eqs. (6.182) and (6.183)), because of the assumption that each element has its own repair crew (totally independent elements). Comparing the results from Eqs. (6.186) and (6.189) with those for the case in which the assumption of no further failures at system down is dropped (only one repair crew), shows (for this example) the small influence of this assumption on final results.

For indicative purpose and to support the validity of *approximate expressions*, the following are the state probabilities for the numerical example according to the first column above, obtained by solving (Eq. (6.189)), i.e., with the assumption of *one repair crew and no further failure at system down* as per Fig. 6.20.

$$\begin{aligned}
 P_0 &\approx 0.979650, P_1 \approx 0.9776 \cdot 10^{-2}, P_2 \approx 0.99 \cdot 10^{-2}, P_3 \approx 0.49 \cdot 10^{-3}, P_4 \approx 0.99 \cdot 10^{-5}, P_5 \approx 0.74 \cdot 10^{-7}, \\
 P_6 &\approx 0.50 \cdot 10^{-4}, P_7 \approx 0.1184 \cdot 10^{-3}, P_8 \approx 0.11 \cdot 10^{-6}, P_9 \approx 0.74 \cdot 10^{-9}, P_{10} \approx 0.587 \cdot 10^{-5}, P_{11} \approx 0.62 \cdot 10^{-6} \\
 &\text{(more exactly: } P_0 \approx 0.9796499684018, P_0 + \dots + P_7 \approx 0.9999933933087, P_8 + \dots + P_{11} \approx 0.0000066066913 \text{)}.
 \end{aligned}$$

Supplementary results: From Eqs.(6.290) & (6.29)-Fig. 6.20, $MUT_S \approx 1.52 \cdot 10^5$ h for the 1st and $\approx 9.90 \cdot 10^6$ h for the 4th column (row no FF); $MDT_S = 1/\mu_1$ because of the repair priority on E_1 .

6.8 Systems with Complex Structure (one Repair Crew)

Structures and models investigated in the previous sections of this chapter were based on the existence of a reliability block diagram (RBD) and on some simplifying assumptions ((6.1) - (6.7)). In particular, elements of the RBD with only two states, repaired *as-good-as-new* at failure, and ideal fault coverage & switching. This was, so far, good to understand basic investigation methods and tools (see e.g. Figs. 6.9 & 6.10). However, in practical applications more complex situations can arise. This section uses tools developed in Appendix A7 (summarized in Table 6.2 for Markov & semi-Markov processes) to investigate *complex fault tolerant repairable systems* for cases in which a reliability block diagram does not exist or can not easily be found. *Constant failure* and, in general, also *constant repair rates* are assumed. It is shown that many problems occurring in practical applications can be solved on a *case-by-case basis* using a *diagram of transition probabilities* or a *time schedule*. To improve readability, δt & $1-p_i\delta t$ are omitted from the *diagrams of transition probabilities* in $(t, t+\delta t]$, yielding *diagrams of transition rates*. Of course, new systems can lead to "new models", and a broad literature is known on this subject.

After some general considerations in Section 6.8.1, Section 6.8.2 deals with aspects of *preventive maintenance*. Sections 6.8.3 & 6.8.4 consider *imperfect switching & incomplete coverage* (see also Eqs. (A6.30) & (6.223) for undetected fault time). Elements with more than 2 states or one failure mode are discussed in Section 6.8.5. Section 6.8.6 investigates fault tolerant reconfigurable systems (reconfiguration at failure and phased-mission systems) by considering also *reward and frequency/duration aspects*. Section 6.8.7 deals with systems with *common cause failures*. Section 6.8.8 presents some basic considerations on network reliability, and Section 6.8.9 summarizes the procedure for modeling systems with complex structure. Alternative investigation methods (dynamic FTA, BDD, ETA, Petri nets, computer-aided analysis) are introduced in Section 6.9 and a Monte Carlo procedure useful for *rare events* is given. Human reliability is discussed in Section 6.10.

However, as a general rule,

modeling complex systems is a task which must be solved in close cooperation between project and reliability engineers on a case-by-case basis.

6.8.1 General Considerations

In the context of this book, a structure is *complex* when the reliability block diagram either does *not exist* or cannot be reduced to a *series-parallel structure with independent elements* (p. 52).

If the *reliability block diagram exists*, but not as series-parallel structure, reliability and availability analysis can be performed using *one or more* of the following assumptions (as in previous sections, *failure-free time* is used as a synonym for *failure-free operating time*, *repair* as a synonym for *restoration*):

1. For each element in the reliability block diagram, failure-free times and repair times are statistically *independent*.
2. Failure and repair rates of each element are *constant* (time independent).
3. Each element in the reliability block diagram has *constant failure rate*.
4. The flow of failures is a *Poisson process* (homogeneous or nonhomogeneous).
5. *No further failures* are considered (can occur) at *system down* (no FF).
6. Redundant elements are repaired on-line (no interruptions at system level).
7. After each repair, the repaired *element* is as-good-as-new.
8. After a repair, the *system* is as-good-as-new with respect to a specific state.
9. *Only one repair crew* is available, repair is started as soon as the repair crew is free (*first-in first-out*) or according to a given *repair priority*.
10. Totally independent elements, i. e., each element operates and is repaired *independently of every other element* (n repair crews for n elements).
11. Ideal failures (faults) detection and localization; in particular, no *hidden failures* (faults) and false alarms.
12. Failure-free & repair times are > 0 and continuous with *finite* mean & variance.
13. For each element, the mean time to repair is *much lower* than the mean time to failure ($MTTR_i \ll MTTF_i$).
14. Switches and *switching operations* are 100% reliable and have no aftereffect.
15. *Preventive maintenance* is not considered.

A clear formulation of the assumptions stated is important to *fix the validity of the results* obtained. Often it is tacitly assumed that each element has only 2 states (good/failed), one *failure mode* (e.g. shorts or opens), and a time invariant required function (e.g. continuous operation of all elements). Elements with more than two states or one failure mode are discussed in Section 6.8.5 (see also Section 2.3.6 for the nonrepairable case). A time dependent operation and/or required function can be investigated when constant failure rate is assumed (Section 6.8.6.2).

The following is a brief discussion of the above assumptions. With assumptions 1 and 2, the time behavior of the system can be described by a time-homogeneous *Markov process* with a finite number of states. Equations can be established using the *diagram of transition rates* & Table 6.2. Difficulties can arise for the *large number of states involved* (p. 226). In such cases, a first possibility is to limit investigation to the calculation of the mean time to failure $MTTF_{S_i}$ and the asymptotic & steady-state point and average availability $PA_S = AA_S$, i. e., to the solution of *algebraic equations*. A second possibility is to use *approximate expressions* (Section 6.7) or special software tools (Section 6.9.6). Assumption 3 assures the existence of a *regenerative process* with at least one regeneration state. Assumption 4 often applies to systems with a large number of elements. As shown in Sections 6.3 - 6.6, assumption 5 simplifies calculation of the point availability and interval reliability. It has *no influence on reliability function* & $MTTF_{S_i}$, and can be used for *approximate expressions* when assumption 13 applies (see e. g. Section 6.7.2).

Assumption 6 must be met during the *system design*. If not satisfied,

improvements given by redundancy are questionable; in such cases, at least fault detection & localization should be implemented (Sections 4.2.1, 6.8.4).

Assumptions 7 & 8 are in general satisfied if either assumption 2 or 3 holds. Assumption 7 is frequently used, its validity must be verified. Assumption 8 is used only with 2 or 3 (Table 6.1, pp. 478-479). Assumption 9 simplifies calculation and is useful for deriving *approximate expressions* (if 13 holds). Together with 3, the system behavior can be described by a *semi-regenerative process* (Table 6.1, Appendix A7.7). Assumption 3 alone assures that the involved process is *regenerative with at least one regeneration state*. With assumption 10, point availability can be computed using the reliability equation for the nonrepairable case (Eq. (2.48)). This assumption rarely applies in practical applications. However, it allows a simple calculation of an *upper bound* on the point availability. Assumption 13 is generally met. It leads to *approximate expressions*, as illustrated in Section 6.7 or by using asymptotic expansions [6.19, A7.26]. As shown in Examples 6.8-6.10, the shape of the distribution function of the repair time has small influence on results at system level ($MTTF_{S0}, PA_S, IR_S(\theta)$), if assumption 13 holds. Assumptions 14 & 15 simplify investigations, they are valid for *all models* in Sections 6.2-6.7.

If the *reliability block diagram does not exist*, stochastic processes and tools introduced in Appendix A7 can be used to investigate reliability and availability of *fault tolerant systems*, on the basis of the *diagram of transition rates* or a *time schedule*, see Sections 6.8.3-6.8.7 for some examples on systems with imperfect switching, incomplete coverage, more than two states or one failure mode, reconfigurable structure, and common cause failures.

However, investigation of *large series-parallel structures* or of *complex structures* is in general time-consuming and can become mathematically intractable. As a first step it is thus useful to operate with *Markov models*, refinements can be considered on a *case-by-case basis*, see pp. 277-279, 293-294 for general procedures. Alternative investigation methods (dynamic FTA, BDD, ETA, Petri nets, computer-aided analysis) are introduced in Section 6.9, and a Monte Carlo procedure for *rare events* is given in Section 6.9.6.2. Human reliability is discussed in Section 6.10.

6.8.2 Preventive Maintenance

Preventive maintenance is necessary to avoid *wear-out failures* and to identify and repair *hidden failures*, e. g. failures of redundant elements which cannot be detected during normal operation. This section investigates a *one-item repairable structure* with preventive maintenance at $T_{PM}, 2T_{PM}, \dots$. Results are basic for the investigation of more complex structures and will be useful in the following sections to investigate fault tolerant repairable systems (Section 6.8.6). Further models/strategies for preventive maintenance are possible (Section 4.6).

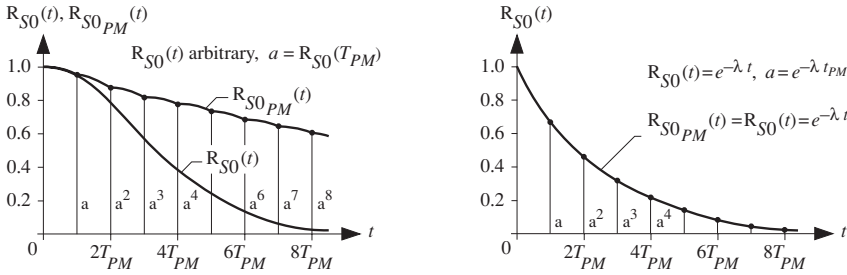


Figure 6.21 Reliability functions for a *one-item structure with preventive maintenance* (of negligible duration) at times $T_{PM}, 2T_{PM}, \dots$ for 2 distribution functions $F(t) = 1 - R_{S_0}(t)$ of the failure-free times (item new at $t = 0, T_{PM}, 2T_{PM}, \dots$; left strictly increasing, right constant failure rate)

The item considered is new at $t = 0$ and has failure-free & repair times distributed according to $F(x)$ & $G(x)$ with densities $f(x)$ & $g(x)$ ($F(0) = G(0) = 0$). Preventive maintenance is of *negligible time duration* (specialized personnel, no logistic delays) and restores the item to *as-good-as-new*. If a preventive maintenance is due at a time in which the item is under repair, one of the following cases will apply:

1. Preventive maintenance will not be performed (included in the running repair, considering that after each repair the item is as-good-as-new).
2. Preventive maintenance is performed, i.e., a running repair is terminated with the preventive maintenance in a negligible time span (this maintenance strategy is known as *block replacement policy* (Section 4.6)).

Both situations can occur in practical applications. In case 2, times $0, T_{PM}, 2T_{PM}, \dots$ are *renewal points*. This case will be considered in the following.

The *reliability function* $R_{S_0 PM}(t)$ for case 2 above can be calculated from

$$R_{S_0 PM}(t) = R_{S_0}(t) = 1 - F(t), \quad \text{for } 0 < t \leq T_{PM}, \quad R_{S_0 PM}(0) = R_{S_0}(0) = 1,$$

$$R_{S_0 PM}(t) = R_{S_0}^n(T_{PM}) R_{S_0}(t - nT_{PM}), \quad \text{for } nT_{PM} < t \leq (n+1)T_{PM}, \quad n \geq 1, \quad (6.192)$$

with $R_{S_0}(x) = 1 - F(x)$ (Eq. (6.14)). Figure 6.21 shows the shape of $R_{S_0}(t)$ and $R_{S_0 PM}(t)$ for an item with strictly increasing (left) and constant (right) failure rate. Because of the *memoryless property* of the exponential distribution function,

$$R_{S_0 PM}(t) = R_{S_0}(t) = e^{-\lambda t} \quad \text{holds for } F(x) = 1 - e^{-\lambda x}. \quad (6.193)$$

From Eq. (6.192), the mean time to failure with preventive maintenance $MTTF_{S_0 PM}$ is

$$MTTF_{S_0 PM} = \int_0^{\infty} R_{S_0 PM}(t) dt = \left[1 + \sum_{n=1}^{\infty} R_{S_0}^n(T_{PM}) \right] \int_0^{T_{PM}} R_{S_0}(t) dt$$

$$= \int_0^{T_{PM}} R_{S_0}(t) dt / [1 - R_{S_0}(T_{PM})] = \int_0^{T_{PM}} (1 - F(x)) dx / F(T_{PM}). \quad (6.194)$$

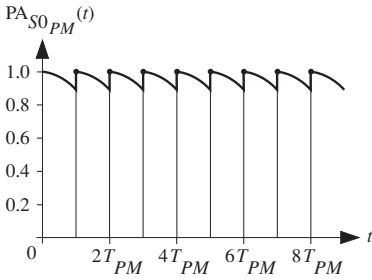


Figure 6.22 Point availability for a repairable *one-item structure with preventive maintenance* (of negligible duration) at times $T_{PM}, 2T_{PM}, \dots$ (item new at $t=0, T_{PM}, 2T_{PM}, \dots$ and after each repair)

For $F(x)=1-e^{-\lambda x}$, Eq. (6.194) yields $MTTF_{S0_{PM}}=1/\lambda = E[\tau]$. For a strictly increasing failure rate $\lambda(x)$ it holds (for $T_{PM} < \infty$) that $MTTF_{S0_{PM}} > E[\tau]$; the contrary is for strictly decreasing $\lambda(x)$. To see this, consider that

$$\int_0^{T_{PM}} R_{S0}(t) dt = \int_0^{\infty} R_{S0}(t) dt - \int_{T_{PM}}^{\infty} R_{S0}(t) dt = E[\tau] - R_{S0}(T_{PM})E[\tau - T_{PM} \mid \tau > T_{PM}],$$

with τ as failure-free time of the item considered and $E[\tau - T_{PM} \mid \tau > T_{PM}]$ as per Eq. (A6.28); the rest of the proof follows from remark 2 to Eq. (A6.28). *Optimization of preventive maintenance period* must consider Eq. (6.194) as well as cost, logistic support, and other relevant aspects ($MTTF_{S0_{PM}} \rightarrow \infty$ for $T_{PM} \rightarrow 0$ and $f(+0)=0$).

Calculation of the *point availability* $PA_{S0_{PM}}(t)$ for case 2 above leads to

$$\begin{aligned} PA_{S0_{PM}}(t) &= PA_{S0}(t), & \text{for } 0 \leq t < T_{PM}, \\ PA_{S0_{PM}}(t) &= PA_{S0}(t - nT_{PM}), & \text{for } nT_{PM} \leq t < (n+1)T_{PM}, \quad n \geq 1, \end{aligned} \quad (6.195)$$

with $PA_{S0}(t)$ from Eq. (6.17). Figure 6.22 shows a typical shape of $PA_{S0_{PM}}(t)$.

If the time duration for the preventive maintenance is not negligible, it is useful to define, in addition to the availabilities introduced in Section 6.2.1, the *overall (or operational) availability* OA_S , defined for $t \rightarrow \infty$ as the ratio of the total up time to the sum of total up and down time in $(0, t]$. Defining $MTTF$ =mean time to failure and MDT =mean down time (with $MTTR$ = mean time to repair, $MTTPM$ = mean time to preventive maintenance, MLD = *mean logistic delay* and T_{PM} = preventive maintenance period (referred to up time) it follows that (see e.g. p. 122)

$$OA_S = \frac{MTTF}{MTTF + MDT} = \frac{MTTF}{MTTF + MTTR + MLD + MTTPM(MTTF/T_{PM})}. \quad (6.196)$$

$MLD=0$ yields the *technical availability*. In some cases, standby times are added to operating time. Other figures are possible, see e.g. [6.12] for railway applications.

Further maintenance strategies are investigated in Section 4.6. *Undetected fault time* τ_{UFT} is considered in Eq. (A6.30), see also Eq. (6.223) for an application.

Example 6.14

Assume a nonrepairable (up to system failure) 1-out-of-2 active redundancy with two identical elements with constant failure rate λ . Give the mean time to failure $MTTF_{S0PM}$ by assuming a preventive maintenance with period $T_{PM} \ll 1/\lambda$. The preventive maintenance is performed in a negligible time span and restores the 1-out-of-2 active redundancy to as-good-as-new.

Solution

For a nonrepairable (up to system failure) 1-out-of-2 active redundancy with two identical elements with constant failure rate λ , the reliability function is given by Eq. (2.22)

$$R_{S0}(t) = 2e^{-\lambda t} - e^{-2\lambda t}$$

The mean time to failure with preventive maintenance follows from Eq. (6.194) as

$$MTTF_{S0PM} = \frac{\int_0^{T_{PM}} R_{S0}(t) dt}{1 - R_{S0}(T_{PM})} = \frac{\frac{2}{\lambda}(1 - e^{-\lambda T_{PM}}) - \frac{1}{2\lambda}(1 - e^{-2\lambda T_{PM}})}{1 - 2e^{-\lambda T_{PM}} + e^{-2\lambda T_{PM}}}$$

Using $e^{-x} \approx 1 - x + x^2/2$ it follows that

$$MTTF_{S0PM} \approx \frac{2T_{PM} - T_{PM}}{\lambda^2 T_{PM}^2} = \frac{1}{\lambda^2 T_{PM}} \quad (= MTBF \cdot MTBF / T_{PM} \text{ for } MTBF = 1/\lambda). \quad (6.197)$$

Without preventive maintenance, Eq. (2.22) yields $MTTF_{S0} = 3/2\lambda = 1.5MTBF$ (for $MTBF = 1/\lambda$). Equation (6.197) clearly shows the *gain* given by the preventive maintenance.

6.8.3 Imperfect Switching

In practical applications, *switching* is necessary for powering down failed elements and powering up repaired elements. In some cases it is sufficient to locate the *switching element* in series with the redundancy on the reliability block diagram, yielding series-parallel structures as investigated in Section 6.6. However, such an approach is often too simple to cover real situations. This section shows this on the basis of practical examples. Further considerations are given in Section 6.8.4 dealing with incomplete coverage.

As a *first example*, Fig. 6.23 shows a situation in which measurement points M_1 and M_2 , switches S_1 and S_2 , as well as a control unit C must be considered. To simplify, let us consider only the reliability function in the nonrepairable case (up to system failure). From a reliability point of view, switch S_i , element E_i , and measurement point M_i in Fig. 6.23 are in series ($i = 1, 2$). Let τ_{b1} and τ_{b2} be the corresponding failure-free times with distribution function $F_b(x)$ and density $f_b(x)$. τ_c is the failure-free time of the control device with distribution function $F_c(x)$ and density $f_c(x)$. Consider first the case of *standby redundancy* and assume that at $t=0$

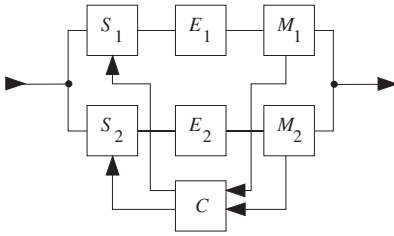


Figure 6.23 Functional block diagram for a 1-out-of-2 active redundancy with switches S_1 and S_2 , measurement points M_1 and M_2 , and control device C

element E_1 is switched on. A system failure in the interval $(0, t]$ occurs with one of the following mutually exclusive events

$$\{\tau_c > \tau_{b1} \cap (\tau_{b1} + \tau_{b2}) \leq t\} \quad \text{or} \quad \{\tau_c < \tau_{b1} \leq t\}.$$

It is implicitly assumed here that a failure of the control device has no influence on the operating element, and does not lead to a commutation to E_2 . A verification of these conditions by an *FMEA* (Section 2.6) is necessary. With these assumptions, the *reliability function* $R_{S0}(t)$ of the system described by Fig. 6.23 is given by (nonrepairable case, system new at $t = 0$)

$$R_{S0}(t) = 1 - \left[\int_0^t f_b(x)(1 - F_c(x))F_b(t - x)dx + \int_0^t f_b(x)F_c(x)dx \right]. \quad (6.198)$$

Assuming further $f_b(x) = \lambda_b e^{-\lambda_b x}$ and $f_c(x) = \lambda_c e^{-\lambda_c x}$, Eq. (6.198) yields

$$R_{S0}(t) = e^{-\lambda_b t} + (1 - e^{-\lambda_c t}) \frac{\lambda_b}{\lambda_c} e^{-\lambda_b t} \quad (6.199)$$

and

$$MTTF_{S0} = \frac{2\lambda_b + \lambda_c}{\lambda_b(\lambda_b + \lambda_c)}. \quad (6.200)$$

$\lambda_c \equiv 0$ leads to the results of Section 2.3.5 for the 1-out-of-2 standby redundancy (Eqs. (2.63), (2.64)). Assuming now an *active redundancy* (at $t=0$, E_1 is put into operation and E_2 into the reserve state), a system failure occurs in the interval $(0, t]$ with one of the following *mutually exclusive events*

$$\{\tau_{b1} \leq t \cap \tau_c > \tau_{b1} \cap \tau_{b2} \leq t\} \quad \text{or} \quad \{\tau_c < \tau_{b1} \leq t\}.$$

The *reliability function* is then given by (nonrepairable case, system new at $t=0$)

$$R_{S0}(t) = 1 - [F_b(t) \int_0^t f_b(x)(1 - F_c(x))dx + \int_0^t f_b(x)F_c(x)dx]. \quad (6.201)$$

From Eq.(6.201) and assuming $f_b(x) = \lambda_b e^{-\lambda_b x}$ and $f_c(x) = \lambda_c e^{-\lambda_c x}$ it follows that

$$R_{S0}(t) = \frac{2\lambda_b + \lambda_c}{\lambda_b + \lambda_c} e^{-\lambda_b t} - \frac{\lambda_b}{\lambda_b + \lambda_c} e^{-(2\lambda_b + \lambda_c)t}, \tag{6.202}$$

and

$$MTTF_{S0} = \frac{2\lambda_b + \lambda_c}{\lambda_b(\lambda_b + \lambda_c)} - \frac{\lambda_b}{(\lambda_b + \lambda_c)(2\lambda_b + \lambda_c)}. \tag{6.203}$$

$\lambda_c \equiv 0$ leads to the results of Section 2.2.6.3 for the 1-out-of-2 active redundancy (Eq. (2.22)). From Eqs. (6.200) and (6.203) one recognizes that for $\lambda_c \gg \lambda_b$

$$MTTF_{S0} \approx 1 / \lambda_b, \quad \text{for } \lambda_c \gg \lambda_b, \tag{6.204}$$

for both standby and active redundancy, i.e., to a situation as *where no redundancy*.

As a *second example* consider a 1-out-of-2 warm redundancy with constant failure rates λ, λ_r & repair rate $\mu \gg \lambda, \lambda_r$. The switching element can fail with constant failure rate λ_σ and failure mode *stuck at the state occupied just before failure*. At first, let us consider the case in which the failure of the switch can be immediately detected and repaired with constant repair rate $\mu_\sigma \gg \lambda_\sigma$. Furthermore, assume only one repair crew, *repair priority on the switch*, and *no further failure at system down*. Asked are mean time to system failure $MTTF_{S0}$ for system new (state Z_0) at $t=0$ and asymptotic & steady-state (stationary) point and average availability $PA_S = AA_S$. The involved process is a time-homogeneous Markov process. Figure 6.24 give the *diagrams of transition rates* for reliability and availability calculation, respectively (down states Z_2, Z_2', Z_2''). From Fig. 6.24a & Table 6.2 or Eq. (A7.126) it follows that $MTTF_{S0}$ is given as solution of the following system ($M_i \equiv MTTF_{S_i}$)

$$\begin{aligned} \rho_0 M_0 &= 1 + \lambda_\sigma M_0 + (\lambda + \lambda_r) M_1, & \rho_0 \cdot M_0 &= 1 + \lambda_r M_1 + \mu_\sigma M_0, \\ \rho_1 M_1 &= 1 + \lambda_\sigma M_1 + \mu M_0, & \rho_1 \cdot M_1 &= 1 + \mu_\sigma M_1, \end{aligned} \tag{6.205}$$

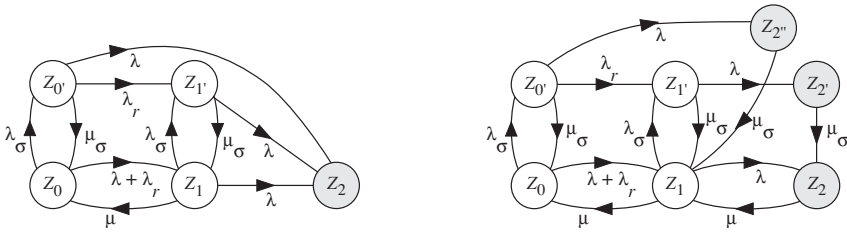
yielding

$$\begin{aligned} MTTF_{S0} &= \frac{(\rho_1 \rho_1 - \lambda_\sigma \mu_\sigma) [\rho_0 \rho_1 + \lambda_\sigma (\rho_1 + \lambda_r)] + (\rho_1 + \lambda_\sigma) [\lambda_r \lambda_\sigma \mu_\sigma + (\lambda + \lambda_r) \rho_0 \rho_1]}{(\rho_1 \rho_1 - \lambda_\sigma \mu_\sigma) (\rho_0 \rho_0 \rho_1 - \rho_1 \lambda_\sigma \mu_\sigma) - \mu \rho_1 [\lambda_r \lambda_\sigma \mu_\sigma + \rho_0 \rho_1 (\lambda + \lambda_r)]} \\ &\approx \frac{\mu + 2\lambda + \lambda_r + (3\lambda + \lambda_r + \lambda_\sigma) \mu / \mu_\sigma}{\lambda (\lambda + \lambda_r) + \lambda \lambda_\sigma \mu / \mu_\sigma} \approx \frac{\mu}{\lambda (\lambda + \lambda_r) + \lambda \lambda_\sigma \mu / \mu_\sigma}. \end{aligned} \tag{6.206}$$

Last approximation assumes $(3\lambda + \lambda_r + \lambda_\sigma) \ll \mu$ & $\mu_\sigma \approx \mu$. From this approximate expression it follows that the *effect of imperfect switching with failure mode stuck at the state occupied just before failure*, immediately detected and repaired, *becomes negligible* for (see Eqs. (6.212) and (6.239) for more severe conditions)

$$\lambda_\sigma \ll (\lambda + \lambda_r) \mu_\sigma / \mu. \tag{6.207}$$

$\lambda_\sigma = 0$ ($0 < \mu, \mu_\sigma < \infty$) yields $MTTF_{S0} = (2\lambda + \lambda_r + \mu) / \lambda (\lambda + \lambda_r)$, as for ideal switch (Table 6.6). $\lambda_\sigma \gg (\lambda + \lambda_r) \mu_\sigma / \mu$ yields $MTTF_{S0} \approx \mu \mu_\sigma / \lambda \lambda_\sigma \mu$, i.e. similar as for a 1-out-of-2 active redundancy with 2 different elements λ, μ & $\lambda_\sigma, \mu_\sigma$ (Eq. (6.100)).



a) For reliability

$$\begin{aligned} \rho_{00'} = \rho_{11'} = \lambda_\sigma; \quad \rho_{01} = \lambda + \lambda_r; \quad \rho_{0'0} = \rho_{1'1} = \mu_\sigma; \\ \rho_{10} = \mu; \quad \rho_{0'1} = \lambda_r; \quad \rho_{0'2} = \rho_{1'2} = \rho_{1'2} = \lambda \\ \rho_0 = \lambda + \lambda_r + \lambda_\sigma; \quad \rho_{0'} = \lambda + \lambda_r + \mu_\sigma \\ \rho_1 = \lambda + \lambda_\sigma + \mu; \quad \rho_{1'} = \lambda + \mu_\sigma; \quad \rho_2 = 0 \end{aligned}$$

b) For availability

$$\begin{aligned} \rho_{00'} = \rho_{11'} = \lambda_\sigma; \quad \rho_{01} = \lambda + \lambda_r; \quad \rho_{10} = \rho_{21} = \mu; \quad \rho_{0'1} = \lambda_r; \\ \rho_{0'0} = \rho_{1'1} = \rho_{2'2} = \rho_{2''2} = \mu_\sigma; \quad \rho_{0'2'} = \rho_{1'2} = \rho_{1'2} = \lambda \\ \rho_0 = \lambda + \lambda_r + \lambda_\sigma; \quad \rho_{0'} = \lambda + \lambda_r + \mu_\sigma; \quad \rho_1 = \lambda + \lambda_\sigma + \mu; \\ \rho_{1'} = \lambda + \mu_\sigma; \quad \rho_2 = \mu; \quad \rho_{2'} = \rho_{2''} = \mu_\sigma \end{aligned}$$

Figure 6.24 Diagram of transition rates for a *repairable 1-out-of-2 warm redundancy with constant failure & repair rates* (λ, λ_r, μ), *imperfect switching* (failure rate λ_σ , repair rate μ_σ , failure mode stuck at the state occupied), *ideal failure detection and localization*, *one repair crew*, switch repaired with *repair priority*, *no further failure at system down*, (Z_2, Z_2', Z_2'' , down states (absorbing for reliability calculation), Markov process)

From Fig. 6.24b and Table 6.2 it follows that $PA_S = AA_S$ is given as solution of

$$\begin{aligned} \rho_0 P_0 = \mu_\sigma P_0 + \mu P_1, \quad \rho_{0'} P_0 = \lambda_\sigma P_0, \quad \rho_1 P_1 = (\lambda + \lambda_r) P_0 + \mu_\sigma P_1 + \mu P_2 + \mu_\sigma P_2'', \\ \rho_{1'} P_1 = \lambda_r P_0 + \lambda_\sigma P_1, \quad \rho_2 P_2 = \lambda P_1 + \mu_\sigma P_2', \quad \rho_{2'} P_2 = \lambda P_1', \quad \rho_{2''} P_2'' = \lambda P_0'. \end{aligned} \quad (6.208)$$

One of the Eq. (6.208), arbitrarily chosen, must be replaced by $\sum P_i = 1$. The *asymptotic & steady-state* point and average availability follows then from

$$\begin{aligned} PA_S = AA_S = P_0 + P_{0'} + P_1 + P_{1'} = \\ \frac{1}{1 + \frac{\rho_{1'} \lambda (\lambda + \lambda_r) (\rho_0 + \mu_\sigma) / \mu + (\lambda / \mu + \lambda / \mu_\sigma) (\mu \lambda_r \lambda_\sigma + \rho_0 \rho_{0'} \lambda_\sigma - \lambda_\sigma^2 \mu_\sigma) + \rho_{1'} \lambda \lambda_\sigma \mu / \mu_\sigma}{\mu \rho_0 \rho_{1'} + \mu \lambda_\sigma (\rho_{1'} + \lambda_r) + (\rho_0 \rho_{0'} - \lambda_\sigma \mu_\sigma) (\rho_{1'} + \lambda_\sigma)}} \\ \approx 1 - \frac{\lambda (\lambda + \lambda_r + \lambda_\sigma \mu^2 / \mu_\sigma^2)}{\mu [\mu + \lambda + \lambda_r + (\lambda_\sigma + 2 \lambda + \lambda_r) \mu / \mu_\sigma]}. \end{aligned} \quad (6.209)$$

Equation (6.209) allows similar conclusions as given by Eq.(6.206), same for $\mu_\sigma = \mu$. $\lambda_\sigma = 0$ yields results for ideal switch ($0 < \mu_\sigma < \infty$).

Further models for imperfect switching are conceivable. For instance, by assuming that for the model of Fig. 6.24 failure of the switch can only be detected and repaired at system down together with failed elements, e.g. at a repair rate μ_g . This situation is known in power systems as *refuse to start*. Figure 6.25 gives the corresponding *diagrams of transition rates* for reliability and availability calculation, respectively (down state Z_2). Results are given in Example 6.15. A further possibility is to assume *no connection* as failure mode (Fig. 6.31) or a probability c that the switch will perform correctly when called to operate (Figs. 6.27, 6.28).

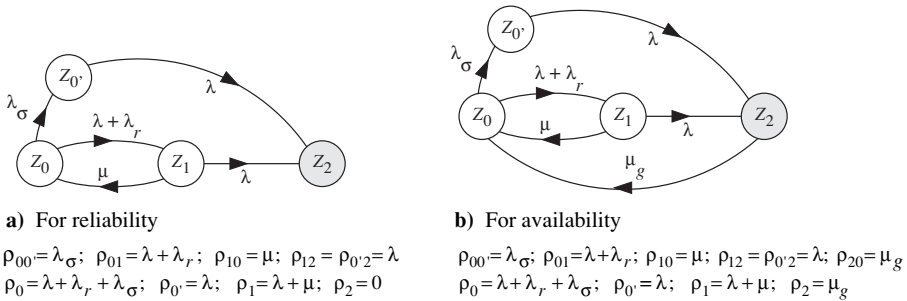


Figure 6.25 Diagram of transition rates for a *repairable 1-out-of-2 warm redundancy with const. failure & repair rates* (λ, λ_r, μ), *imperfect switching* (failure rate λ_{σ} , failure mode *stuck at the state occupied*), *ideal failure detection and localization for the redundant elements, one repair crew, failure of the switch repaired at system down with failed elements at a repair rate μ_g , no further failure at system down* (Z_2 down state (absorbing for rel. cal.), Markov process (see footnote on p. 497))

Example 6.15

Compute the mean time to system failure $MTTF_{S0}$ and the *steady-state* point and average availability $PA_S = AA_S$ for the 1-out-of-2 warm redundancy as per Fig. 6.25 ($\lambda, \lambda_r, \lambda_{\sigma} \ll \mu, \mu_g$).

Solution

From Fig. 6.25a and Table 6.2, $MTTF_{S0}$ is given as solution of ($M_i \equiv MTTF_{Si}$)

$$\rho_0 M_0 = 1 + \lambda_{\sigma} M_0 + (\lambda + \lambda_r) M_1, \quad \rho_1 M_1 = 1 + \mu M_0, \quad \rho_{0'} M_0 = 1, \quad (6.210)$$

yielding

$$MTTF_{S0} = \frac{(2\lambda + \lambda_r + \mu) + \lambda_{\sigma}(\lambda + \mu) / \lambda}{\lambda(\lambda + \lambda_r) + \lambda_{\sigma}(\lambda + \mu)} \approx \frac{\mu(1 + \lambda_{\sigma} / \lambda)}{\lambda(\lambda + \lambda_r) + \lambda_{\sigma}\mu}. \quad (6.211)$$

Because of the not detected failure of the switch, the condition on λ_{σ} to approach results for ideal switching (Table 6.6) is more severe as Eq. (6.207) and given by

$$\lambda_{\sigma} \ll \lambda(\lambda + \lambda_r) / \mu, \quad (\text{which implies } \lambda_{\sigma} / \lambda \ll \ll 1, \text{ considering } \mu \gg \lambda, \lambda_{\sigma}). \quad (6.212)$$

From Fig. 6.25b and Table 6.2 or Eq. (A7.127) it follows that $PA_S = AA_S$ is given as solution of

$$\rho_0 P_0 = \mu P_1 + \mu_g P_2, \quad \rho_{0'} P_0 = \lambda_{\sigma} P_0, \quad \rho_1 P_1 = (\lambda + \lambda_r) P_0, \quad \rho_2 P_2 = \lambda P_1 + \lambda P_0. \quad (6.213)$$

One of the Eq. (6.213), arbitrarily chosen, must be replaced by $P_0 + P_0' + P_1 + P_2 = 1$. The *asymptotic & steady-state* point and average availability $PA_S = AA_S = P_0 + P_0' + P_1$ follows then from

$$PA_S = AA_S = \frac{1}{1 + \frac{\lambda(\lambda + \lambda_r + \lambda_{\sigma}) + \mu\lambda_{\sigma}}{\mu_g(2\lambda + \lambda_r + \lambda_{\sigma}) + \mu\mu_g(1 + \lambda_{\sigma} / \lambda)}} \approx 1 - \frac{\lambda(\lambda + \lambda_r) + \lambda_{\sigma}\mu}{\mu\mu_g}. \quad (6.214)$$

Equation (6.214) allows same conclusions for λ_{σ} as for Eq. (6.211). $\lambda_{\sigma} = 0$ ($0 < \mu, \mu_g < \infty$) yields results for ideal switch (Table 6.6), assuming $\mu_g \approx \mu$ and apart of 2λ instead of λ because of the transition $Z_2 \rightarrow Z_0$. $\lambda_{\sigma} \gg \lambda(\lambda + \lambda_r) / \mu$ yields $MTTF_{S0} \approx 1 / \lambda_{\sigma} + 1 / \lambda$ as for a *non-repairable 1-out-of-2 standby redundancy* with λ_{σ} & λ and $PA_S = AA_S \approx 1 - \lambda_{\sigma} / \mu_g$ as for a *repairable one-item*.

Table 6.11 resumes basic models for the investigation of imperfect switch in a repairable 1-out-of-2 warm redundancy with constant failure and repair rates λ, λ_r, μ (see pp. 257-258 for 2 failure modes for the switch, and Table 6.6 for ideal switch).

Table 6.11 Basic models for imperfect switching in a repairable 1-out-of-2 warm redundancy with constant failure & repair rates ($\lambda_i \ll \mu_i$), one repair crew, no further failures at system down

	$MTTF_{S0} = \frac{1}{\lambda_v + \lambda(\lambda + \lambda_r) / (2\lambda + \lambda_r + \lambda_v + \mu)}$ $PA_S^* = \frac{1}{1 + \frac{\lambda_v}{\mu_v} + \frac{\lambda(\lambda + \lambda_r)}{\mu(\lambda + \lambda_r + \mu)}}$ <p>$\lambda_v = 0$, yields $MTTF_{S0}$ & PA_S as for ideal switch (Table 6.6)</p>
	$MTTF_{S0} \approx \frac{\mu}{\lambda(\lambda + \lambda_r) + \lambda\lambda_\sigma\mu / \mu_\sigma}$ $PA_S^* \approx 1 - \frac{\lambda(\lambda + \lambda_r + \lambda_\sigma\mu^2 / \mu_\sigma^2)}{\mu[\mu + \lambda + \lambda_r + \lambda_\sigma\mu / \mu_\sigma]}$ <p>$\lambda_\sigma \ll (\lambda + \lambda_r)\mu_\sigma / \mu$ yields $MTTF_{S0}$ & PA_S as for ideal switch (Table 6.6)</p>
	$MTTF_{S0} \approx \frac{\mu}{\lambda(\lambda + \lambda_r) + \lambda_\sigma\mu}$ $PA_S^* \approx 1 - \frac{\lambda(\lambda + \lambda_r) + \lambda_\sigma\mu}{\mu\mu_g}$ <p>$\lambda_\sigma \ll \lambda(\lambda + \lambda_r) / \mu$ and $\mu_g = \mu$ yield $MTTF_{S0}$ & PA_S as for ideal switch</p>
	$MTTF_{S0} \approx \frac{\mu + 2\lambda + \lambda_r + \lambda_\sigma + (3\lambda + \lambda_r + \lambda_\sigma)\mu / \mu_\sigma}{\lambda_\sigma\mu + \lambda\lambda_\sigma\mu / \mu_\sigma + \lambda(\lambda + \lambda_r)}$ $PA_S^* \approx 1 - \frac{\lambda_\sigma / \mu_\sigma + \lambda_\sigma(2\lambda + \lambda_r) / \mu_\sigma\mu_\sigma + (\lambda + \lambda_r)(\lambda_\sigma / \mu_\sigma + \lambda / \mu) / \mu + \lambda\lambda_\sigma / \mu_\sigma^2}{1 + (\lambda + \lambda_r) / \mu + (2\lambda + \lambda_r + \lambda_\sigma) / \mu_\sigma}$ <p>$\lambda_\sigma \ll \lambda(\lambda + \lambda_r) / \mu$, $\lambda_\sigma \ll (\lambda + \lambda_r)\mu_\sigma / \mu$ and $\mu_\sigma = \mu_\sigma \approx \mu$ yield $MTTF_{S0}$ & PA_S as for ideal switch (Table 6.6)</p>

* PA_S is used for $PA_S = AA_S$; ** with $2\lambda + \lambda_r$ instead of 3λ and $\lambda + \lambda_r$ instead of 2λ

6.8.4 Incomplete Coverage

Incomplete fault (failure & defect) coverage occurs because of lack or failure in the fault detection and/ or localization (pp.113 & 116). *Fault coverage* is defined as *the proportion of faults that can be detected and localized under given conditions.*⁺⁾ It applies in particular to redundant structures. A fault coverage greater as 0.95 is often required for complex equipment. Lacks in the detection and/or localization lead to *hidden faults*, often not covered by automatic or semi-automatic diagnosis, and thus localizable only at a repair or preventive maintenance. Hidden failures *can cause serious reduction of the advantage given by a redundancy* (Eqs. (6.220) & (6.222) or (6.228) & (6.229)). As a general rule, fault coverage has to be investigated on a *case-by-case basis*, considering following two aspects

- false detection and/or localization (or alternatively false alarm),
- no detection and/or localization possible (or alternatively no alarm emitted).

Following an illustrative example, this section discusses some basic models for incomplete coverage.⁺⁺⁾ A way to compensate incomplete coverage is introduced at the end of the 3th footnote on this page, and illustrated with 2 new models in cases c & d of Table 6.12 (p.256), implying the realization of an *operation monitoring* as per Table 4.1, with the necessary BIT/BITE (see also the remarks on pp.250 & 255). However,

for critical applications, majority redundancy remains the best way to compensate incomplete coverage (in a 2-out-of-3 redundancy, the first failure is captured on line and no switch is necessary, see pp.49,164,295).

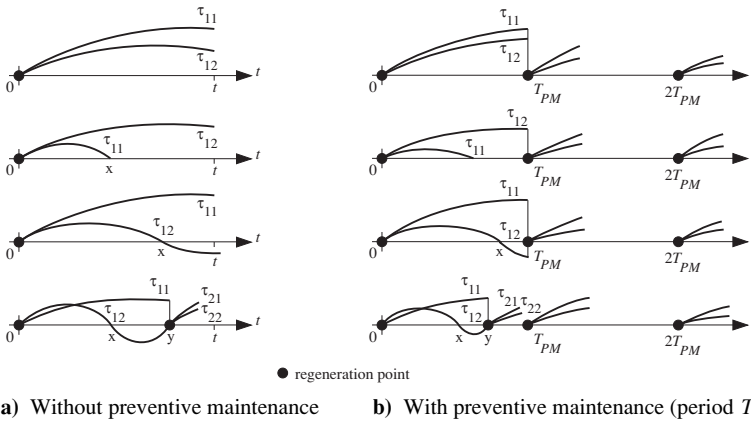
Consider first the case of a 1-out-of-2 active redundancy with two different elements E_1 & E_2 , and assume that *failures of E_1 can be localized and repaired only at a repair of E_2 or at a preventive maintenance*. Elements E_1 and E_2 have constant failure rates ($\lambda_1 \neq \lambda_2$, but still with $\lambda_1 \approx \lambda_2$), the repair time of E_2 is distributed according to $G(x)$ ($G(0)=0$, density $g(x)$), and preventive maintenance, incl. repair of E_1 and/or E_2 , *takes a negligible time* (see Example 6.17 for constant repair rate).⁺⁺⁺⁾ If no *preventive maintenance* is performed, Fig.6.26a shows a possible time schedule of the system (new at $t=0$), yielding for the *reliability function*

$$R_{S0}(t) = e^{-(\lambda_1 + \lambda_2)t} + \int_0^t \lambda_1 e^{-\lambda_1 x} e^{-\lambda_2 t} dx + \int_0^t \lambda_2 e^{-\lambda_2 x} e^{-\lambda_1 t} (1 - G(t-x)) dx + \int_0^t \int_0^y \lambda_2 e^{-\lambda_2 x} e^{-\lambda_1 y} g(y-x) R_{S0}(t-y) dx dy. \quad (6.215)$$

⁺⁾ This often used definition does not consider the effect of undetected faults.

⁺⁺⁾ Undetected fault time τ_{UFT} is investigated by Eq. (A6.30), see also Eq. (6.223) for an application.

⁺⁺⁺⁾ It is tacitly assumed, that at each regeneration point ($t=0$, end of a repair or preventive maintenance), E_2 is put in operation and E_1 in reserve; moreover no common cause failures occur, and automatic failure *detection* in E_1 & E_2 and localization in E_2 , as well as switching operations, are ideal. A possible procedure being that at a failure (output $E_2 \neq$ output E_1), operation is continued with E_1 in the case of failure localized in E_2 , or with E_2 if not (Table 6.12 cases c & d).



a) Without preventive maintenance **b)** With preventive maintenance (period T_{PM})

Figure 6.26 Possible time schedules for the reliability investigation of a repairable 1-out-of-2 active redundancy with hidden failures in E_1 and constant failure rates (see also the footnotes on p. 249)

The Laplace transform of $R_{S0}(t)$ follows as

$$\tilde{R}_{S0}(s) = \frac{(s + \lambda_1)(s + \lambda_1 + \lambda_2) + \lambda_2(s + \lambda_2)(1 - \tilde{g}(s + \lambda_1))}{(s + \lambda_1)(s + \lambda_2)(s + \lambda_1 + \lambda_2) - (s + \lambda_1)(s + \lambda_2)\lambda_2 \tilde{g}(s + \lambda_1)}, \quad (6.216)$$

and the mean time to failure becomes

$$MTTF_{S0} = [\lambda_1(\lambda_1 + \lambda_2) + \lambda_2^2(1 - \tilde{g}(\lambda_1))] / [\lambda_1\lambda_2(\lambda_1 + \lambda_2) - \lambda_1\lambda_2^2\tilde{g}(\lambda_1)]. \quad (6.217)$$

Example 6.16 discusses Eq. (6.217). The point availability $PA_{S0}(t)$ is investigated in Example 6.17 for the case of constant repair rates. If preventive maintenance is performed at times $T_{PM}, 2T_{PM}, \dots$ and after each preventive maintenance (assumed of negligible duration, also considering a possible repair of E_2 and/or E_1) the system is as-good-as-new, the times $0, T_{PM}, 2T_{PM}, \dots$ are regeneration points for the system. $R_{S0_{PM}}(t)$ and $MTTF_{S0_{PM}}$ follow from Eqs. (6.192) & (6.194), with $R_{S0}(t)$ as per Eq. (6.215). For $T_{PM} \gg MTTR$, $PA_{S0_{PM}}(t) \approx PA_{S0}(t) \approx PA_S = AA_S$ can often be used. Optimization of T_{PM} must consider cost and logistic aspects too.

Equations (6.217), (6.218) & (6.220) show that a repairable 1-out-of-2 active redundancy with hidden failures in one element (E_1), which can be localized and repaired only at a repair of the second element or at a preventive maintenance, behaves like a nonrepairable 1-out-of-2 standby redundancy. However, if failure localization and repair of element E_1 can start at failure occurrence (after checking E_2 as per the 3th footnote on p. 249), the situation of an ideal active 1-out-of-2 repairable redundancy is reestablished (even by assuming a lower repair rate for E_1 , e. g. because of a travel time for specialized personnel), see Tab. 6.12 cases c & d;

this bears out, how important it is, in the presence of redundancy to investigate failure modes, failure localization, and check strategy at failure (FMEA).

Example 6.16

Give approximate expressions for the mean time to failure $MTTF_{S0}$ per Eq. (6.217).

Solution

For $\tilde{g}(\lambda_1) \rightarrow 1$, it follows from Eq. (6.217) that

$$MTTF_{S0} \approx (\lambda_1 + \lambda_2) / \lambda_1 \lambda_2 = 1 / \lambda_1 + 1 / \lambda_2. \tag{6.218}$$

A better approximation using $\tilde{g}(\lambda_1) = 1 - \lambda_1 MTTR$ yields (with $MTTR$ as per Eq. (6.111))

$$MTTF_{S0} \approx (\lambda_1 + \lambda_2 + \lambda_2^2 MTTR) / (\lambda_1 \lambda_2 (1 + \lambda_2 MTTR)). \tag{6.219}$$

Example 6.17

Investigate $R_{S0}(t)$ per Eq. (6.216), $MTTF_{S0}$ and $MTTF_{S0PM}$ per Eqs. (6.217) and (6.194), $PA_S = AA_S$ and $PA_{S_{PM}} = AA_{S_{PM}}$, and the undetected fault time τ_{UFT} for the case of constant repair rate μ for E_2 and μ_g for E_1 together with E_2 ($\lambda_1, \lambda_2 \ll \mu, \mu_g$).

Solution

With $\tilde{g}(s + \lambda_1) = \mu / (s + \lambda_1 + \mu)$ it follows from Eq. (6.216) that

$$\tilde{R}_{S0}(s) = [(s + \lambda_1 + \lambda_2)(s + \lambda_1 + \mu) + \lambda_2(s + \lambda_2)] / (s + \lambda_1)(s + \lambda_2)(s + \lambda_1 + \lambda_2 + \mu),$$

and thus (Table A9.7b) $R_{S0}(t) = A e^{-\lambda_1 t} + B e^{-\lambda_2 t} + C e^{-(\lambda_1 + \lambda_2 + \mu)t}$ with

$$A = \frac{\lambda_2(\lambda_2 - \lambda_1 + \mu)}{(\lambda_2 - \lambda_1)(\lambda_2 + \mu)} \approx \frac{\lambda_2}{\lambda_2 - \lambda_1}, \quad B = \frac{-\lambda_1(\lambda_1 - \lambda_2 + \mu)}{(\lambda_2 - \lambda_1)(\lambda_1 + \mu)} \approx \frac{-\lambda_1}{\lambda_2 - \lambda_1}, \quad C = \frac{-\lambda_1 \lambda_2}{(\lambda_1 + \mu)(\lambda_2 + \mu)} \approx 0.$$

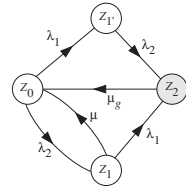
The mean time to failure $MTTF_{S0}$ follows as

$$MTTF_{S0} = \tilde{R}_{S0}(0) = \frac{(\lambda_1 + \lambda_2)(\lambda_1 + \mu) + \lambda_2^2}{\lambda_1 \lambda_2 (\lambda_1 + \lambda_2 + \mu)} \approx \frac{(\lambda_1 + \lambda_2)\mu}{\lambda_1 \lambda_2 (\lambda_1 + \lambda_2 + \mu)} \approx \frac{\lambda_1 + \lambda_2}{\lambda_1 \lambda_2}. \tag{6.220}$$

One recognizes, that $\lambda_1 + \lambda_2 \ll \mu$ yields directly to

$$R_{S0}(t) \approx (\lambda_2 e^{-\lambda_1 t} - \lambda_1 e^{-\lambda_2 t}) / (\lambda_2 - \lambda_1) \quad \text{and} \quad MTTF_{S0} \approx 1 / \lambda_1 + 1 / \lambda_2. \tag{6.221}$$

The point availability $PA_{S0}(t)$ (as well as $R_{S0}(t)$) can be obtained using a 4 states Markov process with up states Z_0, Z_1, Z_1' & down state Z_2 (absorbing for $R_{S0}(t)$), see graph (similar as Fig. 6.25b) and footnote on p. 249. The asymptotic & steady-state point and average availability $PA_S = AA_S$ is obtained by solving (Table 6.2) $(\lambda_1 + \lambda_2)P_0 = \mu P_1 + \mu_g P_2$, $\lambda_2 P_1' = \lambda_1 P_0$, $(\lambda_1 + \mu)P_1 = \lambda_2 P_0$, $P_0 + P_1 + P_1' + P_2 = 1$, yielding



$$PA_S = AA_S = P_0 + P_1 + P_1' = \frac{1}{1 + \frac{\lambda_1 \lambda_2 (\lambda_1 + \lambda_2 + \mu)}{\mu_g [(\lambda_1 + \mu)(\lambda_1 + \lambda_2) + \lambda_2^2]}} \approx 1 - \frac{\lambda_1 \lambda_2}{\mu_g (\lambda_1 + \lambda_2)}. \tag{6.222}$$

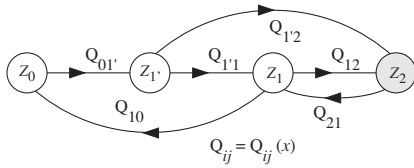
The undetected fault time τ_{UFT} is in this case the stay time in Z_1' , thus (Eqs. (A7.166) & (A7.132))

$$E[\tau_{UFT}] = 1 / \lambda_2 \quad \& \quad E[\text{total undetected time in } (0, t)] = t \cdot P_1 \approx t \cdot \lambda_1 / (\lambda_1 + \lambda_2). \tag{6.223}$$

In the case of preventive maintenance at $T_{PM}, 2T_{PM}, \dots$ (regeneration points at $t = 0, T_{PM}, 2T_{PM}, \dots$), Eq. (6.194) with $R_{S0}(t)$ per Eq. (6.221) yields

$$MTTF_{S0PM} \approx \frac{\lambda_2 (1 - e^{-\lambda_1 T_{PM}}) / \lambda_1 - \lambda_1 (1 - e^{-\lambda_2 T_{PM}}) / \lambda_2}{\lambda_2 (1 - e^{-\lambda_1 T_{PM}}) - \lambda_1 (1 - e^{-\lambda_2 T_{PM}})} \approx \frac{2}{\lambda_1 \lambda_2 T_{PM}}. \tag{6.224}$$

The last part of Eq. (6.224) follows with $e^{-\lambda x} \approx 1 - \lambda x + (\lambda x)^2 / 2$. For $T_{PM} \gg 1 / \mu = MTTR$ $PA_{S0PM}(t) \approx PA_{S0}(t) \approx PA_S = AA_S$ with $PA_S = AA_S$ per Eq. (6.222) can often be used.



$$\begin{aligned}
 Q_{01'}(x) &= 1 - e^{-2\lambda x}; & Q_{12}(x) &= (1 - c)u(x); \\
 Q_{11}(x) &= c u(x); & Q_{10}(x) &= \frac{\mu}{\lambda + \mu}(1 - e^{-(\lambda + \mu)x}); \\
 Q_{12}(x) &= \frac{\lambda}{\mu} Q_{10}(x); & Q_{21}(x) &= 1 - e^{-\mu x}; \\
 u(x) &= 0 \text{ for } x < 0 \text{ and } 1 \text{ for } x \geq 0; & Q_{ij}(\infty) &= p_{ij}
 \end{aligned}$$

Figure 6.27 State transition diagram for a repairable 1-out-of-2 active redundancy with const. failure & repair rates (λ, μ) , incomplete coverage (identification of failed element with probability c), one repair crew (Z_2 down state (absorbing for rel. calculation), semi-Markov proc.; see also Fig. 6.28)

A model often used to consider incomplete coverage assumes that a failure can be localized (BIT/ BITE) only with a probability c (coverage c).^{+) This will be investigated in the following for the case of a 1-out-of-2 active redundancy with identical elements and constant failure & repair rates λ, μ . At a failure, outputs of both elements differ and with probability $1 - c$ the failed element can not be identified and disconnected, yielding a system failure. This case is similar to that of imperfect switching mentioned at the end of Section 6.8.3 and is also known as no start at call [6.34]. Figure 6.27 gives the state transition diagram of the involved semi-Markov process. The transition from state Z_1' occurs instantaneously to Z_1 with probability $p_{11} = c$ or to Z_2 with $p_{12} = 1 - c$. Because of the constant failure & repair rates, investigation can also be based on a Markov process with the diagram of transition rates given in Fig 6.28 (see Examples 6.18 & 6.19 for the equivalence).}

Example 6.18

Give the mean time to system failure $MTTF_{S0}$ and the asymptotic & steady-state point and average availability $PA_S = AA_S$ for the 1-out-of-2 active redundancy as per Fig. 6.27 ($\lambda \ll \mu$).

Solution

From Fig. 6.27 and Table 6.2 or Eq. (A7.173), $MTTF_{S0}$ is given as solution of $M_{1'} = T_{1'} + c M_1$ $M_0 = T_0 + M_1$, $M_1 = T_1 + (\mu / (\lambda + \mu)) M_0$, with $M_i \equiv MTTF_{S_i}$, $T_i = \int_0^\infty (1 - Q_i(x)) dx$, $Q_i(x) = \sum_j Q_{ij}(x)$ (Eqs. (A7.166) and (A7.165)). Considering Fig. 6.27 it follows that $T_0 = 1 / 2\lambda$, $T_{1'} = 0$, $T_1 = 1 / (\lambda + \mu)$, and $T_2 = 1 / \mu$, yielding

$$MTTF_{S0} = \frac{T_0 + T_{1'} + c T_1}{1 - c \mu / (\lambda + \mu)} = \frac{\lambda + \mu + 2\lambda c}{2\lambda(\lambda + \mu - \mu c)} \approx \frac{\mu}{2\lambda^2 + 2\lambda\mu(1 - c)}. \tag{6.225}$$

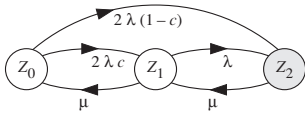
From Fig. 6.27 and Table 6.2 or Eq. (A7.178), $PA_S = AA_S = P_0 + P_{1'} + P_1$ is given as

$$PA_S = AA_S = (p_0 T_0 + p_{1'} T_{1'} + p_1 T_1) / (p_0 T_0 + p_{1'} T_{1'} + p_1 T_1 + p_2 T_2). \tag{6.226}$$

Thereby, p_j are the state probabilities of the embedded Markov chain, obtained as solution of $p_0 = p_1 \mu / (\lambda + \mu)$, $p_{1'} = p_0$, $p_1 = p_{1'} c + p_2$, $p_2 = p_{1'} (1 - c) + p_1 \lambda / (\lambda + \mu)$ (Table 6.2), yielding (considering $p_0 + p_{1'} + p_1 + p_2 = 1$) $p_{1'} = (\lambda + \mu) / (2(\lambda + 2\mu) - \mu c)$, $p_2 = (\lambda + \mu - \mu c) / (2(\lambda + 2\mu) - \mu c)$ $p_0 = p_{1'} \mu / (2(\lambda + 2\mu) - \mu c)$. From Eq. (6.226) it follows then

$$PA_S = AA_S = (\mu^2 + 2\lambda\mu) / (\mu^2 + 2\lambda\mu + 2\lambda(\lambda + \mu - \mu c)) \approx 1 - 2\lambda(\lambda + \mu - \mu c) / (\mu^2 + 2\lambda\mu). \tag{6.227}$$

^{+) A weak point of this model is the assumption of c constant over time and failures; a refinement with share of the failure rate in $\lambda = \lambda_c + \lambda_u$ is in the models c & d introduced in Table 6.12 (p. 256).}



$$\begin{aligned} \rho_{01} &= 2\lambda c; & \rho_{02} &= 2\lambda(1-c); & \rho_{10} &= \mu; \\ \rho_{12} &= \lambda; & \rho_{21} &= \mu \quad (\rho_{21}=0 \text{ for reliability}) \\ \rho_0 &= 2\lambda; & \rho_1 &= \lambda + \mu; & \rho_2 &= \mu \quad (\rho_2=0 \text{ for reliability}) \end{aligned}$$

Figure 6.28 State transition diagram for a repairable 1-out-of-2 active redundancy with const. failure & repair rates (λ, μ) , incomplete coverage (identification of failed element with probability c , i.e., with probability $1-c$ the system goes down because outputs of both elements differ), one repair crew, Markov process (Z_2 down state (absorbing for reliability calculation); see also Table 6.12b)

Example 6.19

Give the mean time to system failure $MTTF_{S0}$ and the asymptotic & steady-state point and average availability $PA_S = AA_S$ for the 1-out-of-2 active redundancy as per Fig. 6.28 ($\lambda \ll \mu$).

Solution

From Fig. 6.28 & Table 6.2 or Eq. (A7.126), $MTTF_{S0}$ is given as solution of (with $M_i \equiv MTTF_{Si}$) $2\lambda M_0 = 1 + 2\lambda c M_1$ and $(\lambda + \mu)M_1 = 1 + \mu M_0$, yielding

$$MTTF_{S0} = [\lambda + \mu + 2\lambda c] / [2\lambda(\lambda + \mu - \mu c)] \approx \mu / [2\lambda^2 + 2\lambda\mu(1-c)]. \tag{6.228}$$

From Fig. 6.28 and Table 6.2 or Eq. (A7.127), $PA_S = AA_S$ is given as solution of $2\lambda P_0 = \mu P_1$, $(\lambda + \mu) P_1 = 2\lambda c P_0 + \mu P_2$ and $P_0 + P_1 + P_2 = 1$, yielding

$$PA_S = AA_S = P_0 + P_1 = \frac{1}{1 + \frac{2\lambda(\lambda + \mu - \mu c)}{\mu^2 + 2\lambda\mu}} \approx 1 - \frac{2\lambda^2 + 2\lambda\mu(1-c)}{\mu^2 + 2\lambda\mu}. \tag{6.229}$$

Comparison of Eqs. (6.225) with (6.228) & (6.227) with (6.229) shows the equivalence of the models of Figs. 6.27 & 6.28 (see Section 6.10 for a further application of semi-Markov processes). For $c=1$, Eqs. (6.228) & (6.229) yield results of Table 6.6 for an ideal 1-out-of-2 active redundancy. For $c=0$, Eqs. (6.228) & (6.229) yield results for a one-item with failure rate 2λ and repair rate μ (most unfavorable case, because at the first failure it is not possible to identify the failed element, yielding to a system down). Comparison of Eqs. (6.92) with (6.228) and (6.87) with (6.229) shows that the effect of incomplete coverage is negligible for

$$2\lambda\mu(1-c) \ll 2\lambda^2 \quad \text{or} \quad c \gg 1 - \lambda/\mu, \quad (\text{e.g. } c > 1 - 0.1\lambda/\mu). \tag{6.230}$$

Condition (6.230) can be hard to realize for complex equipment and remains the same also if repair of a hidden failure brings the system to state Z_0 (Example 6.20). A further possibility is investigated in Example 6.21 by assuming that at the occurrence of a hidden failure, one of the two elements is selected to continue operation and the selected element is not failed with probability p .

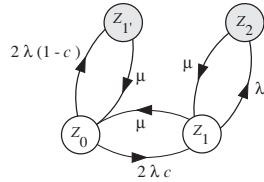
All these investigations show that for critical applications, majority redundancy or a check strategy as described on pp.249 & 255, realized in the models c & d of Table 6.12 (p. 256), has to be preferred.

Example 6.20

Investigate $MTTF_{S0}$ and $PA_S = AA_S$ for the model given by Fig. 6.28 by assuming that a repair for a hidden failure (transition $Z_0 \rightarrow Z_2$) brings the system to state Z_0 and not to Z_1 ($\lambda \ll \mu$).

Solution

$MTTF_{S0}$ is given by Eq. (6. 228). The point availability $PA_{S0}(t)$ can be obtained using a 4 states Markov process with up states Z_0 and Z_1 and down states Z_1' and Z_2 , see graph. The asymptotic & steady-state point and average availability $PA_S = AA_S$ is obtained by solving (Table 6.2) $2\lambda P_0 = \mu P_1' + \mu P_1$, $(\lambda + \mu)P_1' = 2\lambda c P_0 + \mu P_2$, $\mu P_1' = 2\lambda(1 - c)P_0$, and $P_0 + P_1 + P_1' + P_2 = 1$, yielding



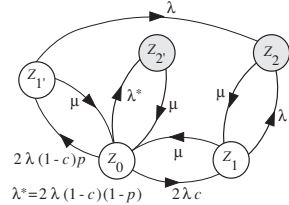
$$PA_S = AA_S = P_0 + P_1 = \frac{1}{1 + \frac{2\lambda[\lambda c + \mu(1 - c)]}{\mu^2 + 2\lambda\mu c}} \approx 1 - \frac{2\lambda[\lambda c + \mu(1 - c)]}{\mu^2} \tag{6.231}$$

Example 6.21

Investigate $MTTF_{S0}$ and $PA_S = AA_S$ for the model considered in Example 6.20 by assuming that at the occurrence of a *hidden failure* (outputs of both elements differ and failed element can not be detected), one of the two elements is selected to continue operation and the selected element is with probability p not failed (safety is not relevant).

Solution

$R_{S0}(t)$ and $PA_{S0}(t)$ can be obtained using a 5 states Markov process with up states Z_0, Z_1, Z_1' and down states Z_2, Z_2' (Z_2, Z_2' absorbing for $R_{S0}(t)$), see graph. $MTTF_{S0}$ is given as solution of (with $M_i \equiv MTTF_{Si}$), $2\lambda M_0 = 1 + 2\lambda c M_1 + 2\lambda(1 - c)p M_1'$, $(\lambda + \mu)M_1 = 1 + \mu M_0$, $(\lambda + \mu)M_1' = 1 + \mu M_0$, yielding



$$MTTF_{S0} = \frac{\lambda + \mu + 2\lambda(c + (1 - c)p)}{2\lambda^2 + 2\lambda\mu(1 - c)(1 - p)} \approx \frac{\mu}{2\lambda^2 + 2\lambda\mu(1 - c)(1 - p)} \tag{6.232}$$

The asymptotic & steady-state point and average availability $PA_S = AA_S$ is obtained by solving (Table 6.2) $2\lambda P_0 = \mu(P_1 + P_1' + P_2)$, $(\lambda + \mu)P_1' = 2\lambda c P_0 + \mu P_2$, $(\lambda + \mu)P_1' = 2\lambda(1 - c)p P_0$, $\mu P_2 = \lambda(P_1 + P_1')$, $P_0 + P_1 + P_1' + P_2 + P_2' = 1$, yielding

$$PA_S = AA_S = P_0 + P_1 + P_1' = \frac{1}{1 + \frac{2\lambda[\lambda + (\mu - \lambda)(1 - c)(1 - p)]}{\mu^2 + 2\lambda\mu[p(1 - c) + c]}} \approx 1 - \frac{2\lambda[\lambda + \mu(1 - c)(1 - p)]}{\mu^2} \tag{6.233}$$

Comparison of Eq.(6.232) with (6.228) and Eq. (6.233) with (6.231) shows that

$$\frac{MTTF_{S0} \text{ } p=0.5}{MTTF_{S0} \text{ } p=0} \approx \frac{2\lambda^2 + 2\lambda\mu(1 - c)}{2\lambda^2 + \lambda\mu(1 - c)} \quad \text{and} \quad \frac{(1 - PA_S) \text{ } p=0}{(1 - PA_S) \text{ } p=0.5} \approx \frac{\lambda c + \mu(1 - c)}{\lambda + \mu(1 - c) / 2} \tag{6.234}$$

Both ratios are 1 for a coverage $c=1$. One recognizes also that results of Example 6.20 are those of Example 6.21 for $p=0$, and that for $p=1$, Eqs. (6.232) & (6.233) yield results for ideal coverage (Table 6.6), as for $c=1$.

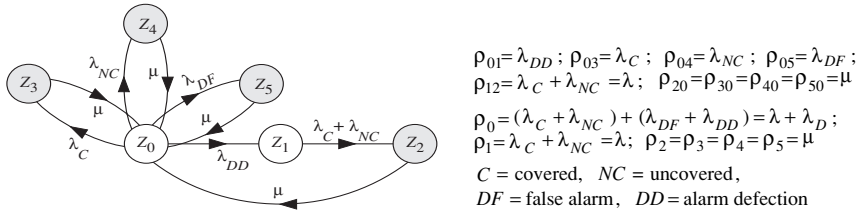


Figure 6.29 Diagram of transition rates for a one-item structure with incomplete coverage and 2 failures modes for the diagnosis (const. failure and repair rates $\lambda_c, \lambda_{NC}, \lambda_{DF}, \lambda_{DD}, \mu$, ideal failure localization, Z_2, Z_3, Z_4, Z_5 down states (absorbing for reliability calculation), Markov process)

Influence of preventive maintenance at $T_{PM}, 2T_{PM}, \dots$ (regeneration points at $t = 0, T_{PM}, 2T_{PM}, \dots$) can be investigated as discussed in Example 6.17, often using

$$R_{S0}(t) \approx e^{-t/MTTF_{S0}} \quad \text{and} \quad |PA_{S0}(t) - PA_S| \approx (1 - PA_S) e^{-\mu t}, \quad (6.235)$$

or $PA_{S0}(t) \approx PA_S = AA_S$, (see Eqs. (6.94) & (6.88) and the discussion to Eq. (6.56)).

Other possibilities to consider for incomplete coverage are conceivable. Assuming, for instance, that in a 1-out-of-2 active redundancy at a failure of one element (outputs of both elements differ), one element is *instantaneously* selected (without any check) to continue operation and with probability p the selected element is not failed, leads to the model of Example 6.20 with $c = p$.

A further possibility, which considers *false alarm* with failure rate λ_{DF} and *alarm deflection* with failure rate λ_{DD} , shown in Fig. 6.29 with a repair rate μ for all failure modes, has been proposed in [6.42] and yields ($\lambda_D = \lambda_{DD} + \lambda_{DF}, \lambda = \lambda_C + \lambda_{NC}$)

$$MTTF_{S0} = \frac{\lambda + \lambda_{DD}}{\lambda(\lambda + \lambda_D)} \quad \& \quad PA_S = AA_S = P_0 + P_1 = \frac{\mu(\lambda + \lambda_{DD})}{\mu(\lambda + \lambda_{DD}) + \lambda(\lambda + \lambda_D)}. \quad (6.236)$$

see also Fig. 3 of [6.42] and Fig. 1 of [1.13] for further refinements.

However,

if the design allows that at a failure in a 1-out-of-2 repairable redundancy (output $E_2 \neq$ output E_1) an appropriate test signal is automatically started (BIT /BITE) and operation is continued with the not failed element, the situation of an ideal active 1-out-of-2 repairable redundancy (Table 6.6) is reestablished (as per the 3th footnote on p.249 and remark on p. 250, assuming no common cause failures and thus that one element is not failed), see cases c & d in Table 6.12.

This bears out, again, how important it is, in presence of redundancy to investigate *failure modes, failure localization, and check strategy at failure*. Table 6.12 resumes basic models for incomplete coverage in a repairable 1-out-of-2 active redundancy with constant failure & repair rates (for the approximations, $\lambda_{1u}/\mu_{1u} \leq \lambda_{1c}/\mu_{1c} \approx \lambda_2/\mu_2$ is assumed in case c ($\lambda_{1u} < \lambda_{1c}$ being a requirement) similar is for case d).

Table 6.12 Basic models for *incomplete coverage in a repairable 1-out-of-2 active redundancy with constant failure & repair rates* ($\lambda_i \ll \mu_i$), *no further failures in a series structure partly down or at system down, one repair crew, no common cause failures* (for c) & d) see remarks on pp. 249 & 255)

<p>1-out-of-2 active</p>	$MTTF_{S0} = \frac{(\lambda_1 + \lambda_2)(\lambda_1 + \mu) + \lambda_2^2}{\lambda_1 \lambda_2 (\lambda_1 + \lambda_2 + \mu)} \approx \frac{\lambda_1 + \lambda_2}{\lambda_1 \lambda_2}$ $PA_S^* = \frac{1}{1 + \frac{\lambda_1 \lambda_2 (\lambda_1 + \lambda_2 + \mu)}{\mu_g [(\lambda_1 + \mu)(\lambda_1 + \lambda_2) + \lambda_2^2]}} \approx 1 - \frac{\lambda_1 \lambda_2}{\mu_g (\lambda_1 + \lambda_2)}$
<p>1-out-of-2 active</p>	$MTTF_{S0} = [\lambda + \mu + 2\lambda c] / [2\lambda(\lambda + \mu - \mu c)]$ $\approx \mu / [2\lambda^2 + 2\lambda\mu(1 - c)]$ $PA_S^* = \frac{\mu^2 + 2\lambda\mu}{\mu^2 + 2\lambda\mu + 2\lambda(\lambda + \mu - \mu c)} \approx 1 - \frac{2\lambda^2 + 2\lambda\mu(1 - c)}{\mu^2 + 2\lambda\mu}$
<p>1-out-of-2 active repair priority on E_2</p>	<p>$MTTF_{S0}$, obtained by solving ($M_i = MTTF_i$, $\lambda_i = \lambda_{1c} + \lambda_{1u}$) $(\lambda_1 + \lambda_2)M_0 = 1 + \lambda_{1c}M_1 + \lambda_{1u}M_1 + \lambda_2M_1$, $(\lambda_2 + \mu_{1c})M_1 = 1 + \mu_{1c}M_0$, $(\lambda_2 + \mu_{1u})M_1 = 1 + \mu_{1u}M_0$, $(\lambda_1 + \mu_2)M_1 = 1 + \mu_2M_0$, yields $MTTF_{S0} \approx 1 / \lambda_2 (\lambda_1 / \mu_2 + \lambda_{1c} / \mu_{1c} + \lambda_{1u} / \mu_{1u})$</p> <p>$PA_S^* = P_0 + P_1 + P_1' + P_1''$, obtained by solving $(\lambda_1 + \lambda_2)P_0 = \mu_{1c}P_1 + \mu_{1u}P_1' + \mu_2P_1''$, $(\lambda_2 + \mu_{1c})P_1 = \lambda_{1c}P_0 + \mu_2P_2$, $(\lambda_2 + \mu_{1u})P_1' = \lambda_{1u}P_0 + \mu_2P_2$, $(\lambda_1 + \mu_2)P_1'' = \lambda_2P_0$, $\mu_2P_2 = \lambda_2P_1' + \lambda_{1c}P_1''$, $P_0 + P_1 + P_1' + P_1'' + P_2 + P_2' = 1$, $\lambda_1 = \lambda_{1c} + \lambda_{1u}$) yields $PA_S^* \approx 1 - \lambda_2 [\lambda_1 / \mu_2 + \lambda_{1c} / \mu_{1c} + \lambda_{1u} / \mu_{1u}] / \mu_2$</p> <p>($MTTF_{S0} \approx \mu / 2\lambda_1\lambda_2$ & $PA_S \approx 1 - 2\lambda_1\lambda_2 / \mu^2$ for $\mu_{1u} = \mu_{1c} = \mu_2 = \mu$)</p>
<p>1-out-of-2 active</p>	<p>$MTTF_{S0}$, obtained by solving ($M_i = MTTF_i$, $\lambda = \lambda_c + \lambda_u$) $2\lambda M_0 = 1 + 2\lambda_c M_1 + 2\lambda_u M_1$, $(\lambda + \mu_c)M_1 = 1 + \mu_c M_0$, $(\lambda + \mu_u)M_1 = 1 + \mu_u M_0$, $(\lambda + \mu_c)M_1 = 1 + \mu_c M_0$, $(\lambda + \mu_u)M_1 = 1 + \mu_u M_0$, yields $MTTF_{S0} \approx [1 + 2(\lambda_c / \mu_c + \lambda_u / \mu_u)] / [2\lambda(\lambda_c / \mu_c + \lambda_u / \mu_u)]$</p> <p>$PA_S^* = P_0 + P_1 + P_1' + P_1'' + P_1'''$, obtained by solving $\mu_c P_2 = \lambda_c P_1 + \lambda_c P_1'$, $(\lambda + \mu_c)P_1 = 2\lambda_c P_0$, $(\lambda + \mu_u)P_1' = 2\lambda_u P_0$, $(\lambda + \mu_c)P_1'' = \mu_c P_2 + \mu_u P_2'$, $(\lambda + \mu_u)P_1''' = \mu_c P_2'' + \mu_u P_2'''$, $\mu_u P_2 = \lambda_c P_1 + \lambda_c P_1'$, $\mu_c P_2' = \lambda_u P_1 + \lambda_u P_1''$, $\mu_u P_2'' = \lambda_u P_1' + \lambda_u P_1'''$, $P_0 + P_1 + P_1' + P_1'' + P_1''' + P_2 + P_2' + P_2'' + P_2''' = 1$, yields $PA_S^* \approx 1 - 2\lambda(\lambda_c / \mu_c^2 + \lambda_u / \mu_u^2)(1 - \lambda_c / \mu_c - \lambda_u / \mu_u)$</p> <p>($MTTF_{S0} \approx \mu / 2\lambda^2$ & $PA_S \approx 1 - 2\lambda^2 / \mu^2$ for $\mu_c = \mu_u = \mu$)</p>

c and u refer to 100% and 0% coverage, respectively; * PA_S^* is used for $PA_S = AA_S$

6.8.5 Elements with more than two States or one Failure Mode

Elements with *more than two states* (good/ failed for instance) or one failure mode (e. g. open or short) often arise in practical applications. Some considerations have been given in Sections 2.3.6 & 6.8.4. This section shows, on the basis of practical examples, that items with more than two states or one failure mode can be investigated using the diagram of transition rates, see also pp. 266-269 for a further application.

As a *first example* consider an item with the three states *good, waiting for repair, repair* [6.14]. Figure 6.30 shows this model. From Fig. 6.30 & Table 6.2 it holds that

$$MTTF_{S0} = 1 / \lambda \quad \text{and} \quad PA_S = AA_S = \mu \mu' / (\mu \mu' + \lambda (\mu + \mu')). \quad (6.237)$$

The item in Fig. 6.30 behaves like a one-item structure with failure rate λ and repair time with mean $MTTR_{tot} = 1/\mu + 1/\mu'$ (Erlang distributed ($n=2$, Eq. (A6.102)) for $\mu = \mu'$). More complex structures can also be investigated, see e. g. [6.14].

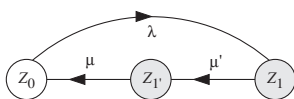
As a *second example* consider a *1-out-of-2 warm redundancy* with constant failure rate λ, λ_r and repair rate μ . The switching element can fail with constant failure rate λ_σ for failure mode *stuck at the state occupied just before failure* or λ_o for failure mode *no connection*. Failure of the switch can be immediately detected and repaired with constant repair rate μ_σ or μ_o . Furthermore, assume only one repair crew, *repair priority* on the switch, and no further failure at system down (also for the switch, no further failure is possible after a failure with one of the two possible failure modes). Asked is the mean time to system failure $MTTF_{S0}$ for system new (in state Z_0) at $t=0$. The involved process is a time-homogeneous Markov process. Figure 6.31 gives the *diagrams of transition rates* for reliability calculation (see Example 6.22 for availability). Comparing Fig. 6.31 with Fig. 6.24a, one recognizes that $MTTF_{S0}$ is given by Eq. (6.206) with $\rho_0 = \lambda + \lambda_r + \lambda_\sigma + \lambda_o$ and $\rho_1 = \lambda + \lambda_o + \lambda_\sigma + \mu$ (i. e. adding λ_o to ρ_0 and ρ_1). From this,

$$MTTF_{S0} \approx \frac{\mu + 2\lambda + \lambda_r + \lambda_o + (3\lambda + \lambda_r + \lambda_\sigma) \mu / \mu_\sigma}{\lambda_o [\mu + 2\lambda + \lambda_r + \lambda_o + 2\lambda \mu / \mu_\sigma] + \lambda \lambda_\sigma \mu / \mu_\sigma + \lambda (\lambda + \lambda_r)}. \quad (6.238)$$

The approximation assumes $\mu, \mu_\sigma \gg \lambda, \lambda_\sigma, \lambda_o$. The failure rate λ_o (for no connection) is *dominant* and acts similarly as λ_σ in Example 6.15 (Eq (6.212)). The *effect of imperfect switching becomes negligible* for

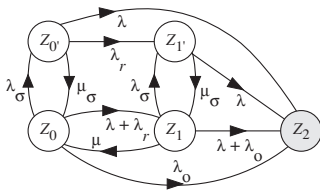
$$\lambda_o \ll \lambda (\lambda + \lambda_r) / \mu \quad \text{and} \quad \lambda_\sigma \ll (\lambda + \lambda_r) \mu_\sigma / \mu \quad (\mu, \mu_\sigma \gg \lambda, \lambda_r, \lambda_\sigma, \lambda_o). \quad (6.239)$$

$\lambda_o = 0$ ($0 < \mu_o < \infty$) leads to Eq. (6.206), $\lambda_o = \lambda_\sigma = 0$ ($0 < \mu_o, \mu_\sigma < \infty$) yields results for ideal switch (Table 6.6).



$\rho_{01} = \rho_0 = \lambda$; $\rho_{11'} = \rho_1 = \mu'$; $\rho_{1'0} = \rho_{1'} = \mu$
 λ = failure rate, μ = repair rate,
 μ' = failure detection rate (including possible travel time)

Figure 6.30 Diagram of transition rates for an item with 3 states: *good, waiting for repair, repair* (constant failure, failure localization & repair rates (λ, μ' & μ), Z_1, Z_1 down states, Markov proc.)



$$\begin{aligned} \rho_{00} &= \lambda_{\sigma}; & \rho_{01} &= \lambda + \lambda_r; & \rho_{0'0} &= \mu_{\sigma}; \\ \rho_{02} &= \lambda_o; & \rho_{0'1} &= \lambda_r; & \rho_{0'2} &= \lambda; & \rho_{10} &= \mu; \\ \rho_{11} &= \lambda_{\sigma}; & \rho_{12} &= \lambda + \lambda_o; & \rho_{1'1} &= \mu_{\sigma}; & \rho_{1'2} &= \lambda \\ \rho_0 &= \lambda + \lambda_r + \lambda_{\sigma} + \lambda_o; & \rho_{0'} &= \lambda + \lambda_r + \mu_{\sigma}; \\ \rho_1 &= \lambda + \lambda_o + \lambda_{\sigma} + \mu; & \rho_{1'} &= \lambda + \mu_{\sigma}; & \rho_2 &= 0 \end{aligned}$$

Figure 6.31 Diagram of transition rates for reliability calculation for a repairable 1-out-of-2 warm redundancy with constant failure & repair rates λ, λ_r, μ , switch with failure modes stuck at the state occupied and no connection with constant failure & repair rates $\lambda_{\sigma}, \mu_{\sigma}$ and λ_o, μ_o , respectively, ideal failure detection and localization, one repair crew, repair priority on switch (Z_2 down state (absorbing for reliability calculation), Markov process)

Example 6.22 investigates $PA_S=AA_S$ for the system described by Fig. 6.31 by assuming a repair rate μ_o for failure mode *no connection* and μ_{σ} for failure mode *stuck at the state occupied just before failure*, one repair crew, and repair priority for switch failures (for the switch only a failure mode is possible at a time). From Eq. (6.240) one recognizes that imperfect switching acts for $PA_S=AA_S$ in a similar way as for $MTTF_{S0}$ (Eq. (6.239)).

A more complex system is considered in Section 6.8.6.3 (pp.266-269). Further models for systems with more than two states or one failure mode are conceivable.

Example 6.22

Investigates the asymptotic & steady-state point and average availability $PA_S=AA_S$ for the model considered in Fig. 6.31 by assuming no further failures at system down ($\lambda_i \ll \mu_i$).

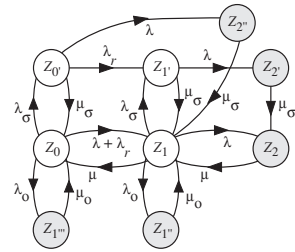
Solution

$PA_S=AA_S$ (as well as $PA_{S0}(t)$) can be obtained using a 9 states Markov process with up states Z_0, Z_0', Z_1, Z_1' and down states $Z_1'', Z_1''', Z_2, Z_2', Z_2''$ (absorbing for reliability calculation), see graph, by solving (Table 6.2) $(\lambda + \lambda_r + \lambda_{\sigma} + \lambda_o)P_0 = \mu_{\sigma}P_0' + \mu_oP_1 + \mu_oP_1'' + \mu_oP_1''' = \lambda_oP_0$, $(\lambda + \lambda_r + \mu_{\sigma})P_0' = \lambda_{\sigma}P_0$, $(\lambda + \mu_{\sigma})P_1 = \lambda_rP_0' + \lambda_{\sigma}P_1'$, $\mu_oP_1'' = \lambda_oP_1$, $\mu P_2 = \lambda P_1 + \mu_{\sigma}P_2'$, $\mu_{\sigma}P_2' = \lambda P_1'$, $\mu_{\sigma}P_2'' = \lambda P_0'$, and $P_0 + P_0' + P_1 + P_1' + P_1'' + P_1''' + P_2 + P_2' + P_2'' = 1$, yielding

$$\begin{aligned} PA_S = AA_S &= P_0 + P_0' + P_1 + P_1' = \\ &= \frac{1}{1 + \frac{a(\lambda + \lambda_r)(a + \lambda_r + \lambda_{\sigma})[\mu_{\sigma}(\mu_o\lambda + \mu\lambda_o) + b\mu_o\lambda\lambda_{\sigma}] + a\mu[\mu\mu_{\sigma}\lambda_o(a + \lambda_r) + \mu_o\lambda\lambda_{\sigma}(b\lambda_r + \mu)]}{\mu\mu_o\mu_{\sigma}(\lambda + \lambda_{\sigma} + \mu_{\sigma})[\mu\mu_{\sigma} + (\lambda + \lambda_r)(\mu + \mu_{\sigma}) + (\lambda + \lambda_r + \lambda_{\sigma})(\lambda + \lambda_r)]}} \\ &\approx 1 - \frac{(\lambda_o/\mu_o)[1 + (2\lambda + \lambda_r)/\mu_{\sigma}] + \lambda\lambda_{\sigma}/\mu_{\sigma}^2 + (\lambda + \lambda_r)(\lambda_o/\mu_o + \lambda/\mu)/\mu}{1 + (\lambda + \lambda_r)/\mu + (2\lambda + \lambda_r + \lambda_{\sigma})/\mu_{\sigma}} \end{aligned} \tag{6.240}$$

$a = \lambda + \mu_{\sigma}, \quad b = (\mu + \mu_{\sigma})/a.$

Equation (6.240) allows similar conclusions as given by Eq. (6.239), same for $\mu_o = \mu_{\sigma} = \mu$. $\lambda_o = 0$ leads to Eq. (6.209), $\lambda_o = \lambda_{\sigma} = 0$ yields results for ideal switch ($0 < \mu_o, \mu_{\sigma} < \infty$).



6.8.6 Fault Tolerant reconfigurable Systems

Fault tolerant structures are able to detect and localize faults (failures & defects) and reconfigure themselves to continue operation with minimum loss of performance and /or safety (*graceful degradation*). Such a characteristic *must be built in during design & development*. Typical examples of fault tolerant systems are safety circuits as well as power and telecommunication networks. Following a short discussion on ideal reconfiguration, this section deals with reconfiguration occurring at given fixed times or at failure by considering also non ideal conditions, for instance imperfect switching in Section 6.8.6.3. Investigation is based on tools introduced in Appendix A7 and summarized in Table 6.2. Constant failure and repair rates are assumed, yielding to time-homogeneous Markov processes. Procedures are illustrated on a *case-by-case basis using diagrams of transition rates*.

6.8.6.1 Ideal case

Each redundant structure belongs to a fault tolerant reconfigurable structure and must be validated for this purpose during design & development, for instance with an FMEA (Section 2.6). For the redundant structures investigated in Sections 2.2, 2.3.1 - 2.3.5, 6.4 - 6.7 and Appendix A7, independent elements (p.52), ideal fault coverage, ideal switching, and no reduction of system performance at failure of a redundant element was assumed. Because of these assumptions, investigations often lead to series - parallel structures (Sections 6.6 & 6.7). Imperfect switching, incomplete coverage, and items (systems) with more than two states or failure modes are considered in Sections 2.3.6, 6.8.3 - 6.8.5, 6.8.6.3. Sections 6.8.6.2 and 6.8.6.3 investigate *time and failure censored reconfiguration*, and Section 6.8.6.4 considers *reward & frequency/duration* aspects. In addition, Sections 6.8.7 - 6.8.9 deal with common cause failures, basic considerations on reliability networks, and a general procedure for complex repairable systems. Alternative investigation methods for complex systems and aspects of human reliability are introduced in Sections 6.9 and 6.10, respectively.

6.8.6.2 Time Censored Reconfiguration (Phased-Mission Systems)

In some practical applications, systems are used for different required functions. If each required function can be considered separately from one another, investigation is performed by considering a reliability block diagram (if it exist) for each required function (p.29). Otherwise, if mission phases follow each other, investigation must consider the *system reconfiguration* at the end of each phase and one define this as a *phased-mission system*. Investigation of phased-mission systems can be more time consuming as stated e. g. in [2.7, 2.18, 6.24, 6.33, 6.41], dealing with

binary state assignment (basically limited to totally independent elements (p. 52)), considering time dependent failure or repair rates (breaking the Markov property), using semi-Markov processes (of limited validity), or missing Assumption 4 below (important when transferring state probabilities at the end of phase k to initial probabilities for phase $k+1$). A *lower bound* R_{S0_l} on the reliability R_{S0} for the whole mission is obtained by connecting the reliability block diagrams for each phase in series for the whole mission duration.^{+) An *upper bound* on R_{S0} is given by the smaller of the reliability for each phase, taken separately, by assuming that all elements involved are as-good-as-new at begin of the phase considered; thus,}

$$R_{S0_l} \leq R_{S0} \leq \min(R_{k,S0}) \quad k = 1, \dots, n \text{ (for } n \text{ phases)}. \quad (6.241)$$

Examples 6.23 - 6.25 illustrate basic aspects. For the availability, Eq. (6.246) applies.

Following some general assumptions in Point (i), a practice oriented procedure for reliability and availability analysis of repairable phased-mission systems, which considers *standby redundancy* and *arbitrary repair strategy*, is given in Point (ii).

(i) *General assumptions:*

1. Failure & repair rates (λ_i & μ_i) of all elements are constant during the sojourn time in any state within each phase, but can change (stepwise) at a state (or phase) change because of change in configuration, component use, stress, repair strategy or other (see also p.38); for all elements it holds that $\lambda_i \ll \mu_i$.
2. At the beginning of the phased-mission all elements are as-good-as-new.
3. Phase duration T_1, \dots, T_n are given (fixed) values, each of them so large that *asymptotic & steady-state values* for availability can be assumed for every phase ($T_1, \dots, T_n > 10/\mu_i$ for all elements, see Section 6.2.5 and Table 6.6).
4. For availability investigation, not used elements in a phase are either as-good-as-new and put in standby (failure rate $\lambda \equiv 0$) at begin of the phase or repaired (Assumption 3) and then put in standby (repair priority on elements used); for reliability investigation, down states at system level are absorbing states and the above rule holds for elements which have not caused system down.
5. The system has only one repair crew and no further failures can occur at system down; system down is an absorbing state for reliability; for availability, the system is restored to an operating state according to a given repair strategy.
6. Fault coverage, switch & logistic support are ideal, no preventive maintenance.
7. For each phase, a reliability block diagram exists.

Reduction of above assumptions is possible, for instance, on the basis of the models discussed in Sections 6.8.2 - 6.8.5.

^{+) Assuming that the mission is of given (fixed) duration, R_{S0} is the *reliability for the whole mission*, similar for $PA_S = AA_S$ (*mission availability* has been reserved for Eq. (6.29)); R_{S0} & $PA_S = AA_S$ are thus numbers within $[0,1]$, not function $R_{S0}(t)$ or $PA_{S0}(t)$, this applies also to Example 6.25.}

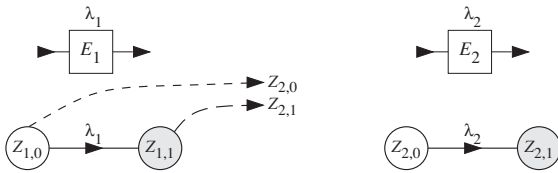


Figure 6.32 Diagrams of transition rates for a one-item used in a mission with phase 1 followed by phase 2 (failure rate λ_1 & λ_2 , duration T_1 & T_2 , respectively); $Z_{1,1}$, $Z_{2,1}$ down states

Example 6.23

A one-item is used in a mission with phase 1 (duration T_1 , const. failure rate λ_1), followed by phase 2 (duration T_2 , const. failure rate λ_2). Compute the reliability function for item new at $t=0$.

Solution

For the reliability R_{S0} for the whole mission it holds that (T_1, T_2 given (fixed))

$$R_{S0} = \Pr \{ \text{phase 1 failure free} \cap \text{phase 2 failure free} \} = \Pr \{ \text{phase 1 failure free} \} \cdot \Pr \{ \text{phase 2 failure free} \mid \text{phase 1 failure free} \} = e^{-\lambda_1 T_1} \cdot e^{-\lambda_2 T_2} = e^{-(\lambda_1 T_1 + \lambda_2 T_2)}. \quad (6.242)$$

The product rule in Eq. (6.242) holds only because of *constant failure rates* (Eqs.(2.14), (A6.29)).

Example 6.24

Show that Eq. (6.242) can be obtained using a Markov approach, i.e., working with two separate transition rate diagrams for phase 1 and for phase 2, and setting final state probabilities from phase 1 as initial-state probabilities for phase 2.

Solution

Figure 6.32 gives the diagrams of transition rates for phase 1 and 2 (separately). For phase 1, the state probability $P'_{1,0}(t)$ follows from $\dot{P}'_{1,0}(t) = -\lambda_1 P'_{1,0}(t)$ (Table 6.2, Eq. (A7.115), yielding $P'_{1,0}(t) = e^{-\lambda_1 t}$, for $P'_{1,0}(0) = 1$. Thus,

$$R_{S0}(T_1) = P'_{1,0}(T_1) = e^{-\lambda_1 T_1} \quad \text{and} \quad P'_{1,1}(T_1) = 1 - e^{-\lambda_1 T_1}.$$

$P'_{1,1}(t)$ follows from $P'_{1,0}(t) + P'_{1,1}(t) = 1$ or by solving $\dot{P}'_{1,1}(t) = \lambda_1 P'_{1,0}(t)$ with $P'_{1,1}(0) = 0$. Similarly, for phase 2 with t starting at $t = T_1$,

$$\dot{P}'_{2,0}(t - T_1) = -\lambda_2 P'_{2,0}(t - T_1), \quad \text{with} \quad P'_{2,0}(T_1) = P'_{1,0}(T_1) = e^{-\lambda_1 T_1};$$

yielding $P'_{2,0}(t - T_1) = e^{-\lambda_1 T_1} e^{-\lambda_2(t - T_1)}$, $T_1 \leq t < T_1 + T_2$, and thus

$$R_{S0}(T_1 + T_2) = P'_{2,0}(T_1 + T_2) = e^{-\lambda_1 T_1} e^{-\lambda_2 T_2} = e^{-(\lambda_1 T_1 + \lambda_2 T_2)} = R_{S0}. \quad (6.243)$$

Example 6.25

A one-item system with reliability function $R_{S0}(t)$ is used for a mission of random duration $\tau_w > 0$ distributed according to $F_w(t) = \Pr\{\tau_w \leq t\}$ with $F_w(0) = 0$ and density $f_w(t)$. Give the reliability, first for the general case and then by assuming constant failure rate λ and exponentially distributed mission duration ($f_w(t) = \delta e^{-\delta t}$).

Solution

As mission duration can take any time between $(0, \infty)$, reliability takes a constant value given by

$$R_{S0} = \int_0^\infty f_w(t) R_{S0}(t) dt, \quad (6.244)$$

(see also Eq. (2.76)). For $f_w(t) = \delta e^{-\delta t}$ and constant failure rate λ , Eq. (6.244) yields

$$R_{S0} = \delta / (\delta + \lambda), \quad \text{and thus,} \quad R_{S0} \approx 1 \text{ for } \delta \gg \lambda \text{ and } R_{S0} \approx \delta / \lambda \text{ for } \delta \ll \lambda. \quad (6.245)$$

Supplement. results: If the mission duration is limited to T_w , $\tau_w > 0$ is a truncated random variable and Eq.(6.245) becomes $R_{S0} = (\delta + \lambda e^{-(\delta + \lambda)T_w}) / (\delta + \lambda)$.

(ii) *Procedure for reliability & availability computation of repairable phased-mission systems with fixed phase duration T_1, \dots, T_n , satisfying the general assumptions (i):*

1. Group *series elements used in all phases* (power supply, cooling, etc.) in one element to be considered in final results (Table 6.10, 2nd row, Eqs. (6.257), (6.258)).
2. Draw the *diagram of transition rates for reliability* evaluation, separately for each phase $(1, \dots, n)$, beginning by phase 1 with $Z_{1,0}$ (1 referring to phase 1 and 0 being the state in which all elements are as-good-as-new); down states at system level are absorbing states; use the same state numbering for the same state appearing in successive phases; however, state $Z_{k,i}$ corresponding to a state $Z_{c,i}$ in a phase c preceding phase k can also contain as-good-as-new elements appearing in phase k but not in a previous phase, or standby elements (not used in phase k) with failure rate $\lambda \equiv 0$; for $k > 1$, state $Z_{k,0}$ contains all as-good-as-new elements used in phase k and (as necessary) elements not used in phase k which are standby with failure rate $\lambda \equiv 0$ (*as-good-as-new* is same as *operating or ready to operate*, because of λ_i const.).
3. For *availability* investigation, use results of Table 6.10 (or extend diagrams of transition rates, allowing a return to an operating state after system down according to a given repair strategy) to compute the asymptotic & steady-state availability for *each phase separately* ($PA_{k,S} = AA_{k,S}$ for phase k), taking care of elements which are not used in the phase considered and can act as standby redundancy ($\lambda \equiv 0$) for working elements; for the whole *mission* it holds then

$$PA_S = AA_S \geq \min(PA_{k,S} = AA_{k,S}), \quad k = 1, \dots, n \text{ (for } n \text{ phases)}. \quad (6.246)$$

4. For *reliability* investigation, compute the reliability function $R_{1,S0}(T_1)$ at the end of phase 1 starting in state $Z_{1,0}$ at $t=0$ in the same way as for a one mission system (Table 6.2), as well as states probabilities $P'_{1,j}(T_1)$ for all up states $Z_{1,j}$; if $Z_{1,j}$ (possibly with further as-good-as-new elements used in phase 2) is an up state in phase 2, $P'_{1,j}(T_1)$ becomes the probability $P'_{2,j}(0)$ to start phase 2 in $Z_{2,j}$; if $Z_{1,j}$ is a (system) down state in phase 2, $P'_{1,j}(T_1)$ adds to the initial probability of starting phase 2 in the (system) down state; if $Z_{1,j}$ does not appear in phase 2, $P'_{1,j}(T_1)$ adds to the initial probability in state $Z_{2,0}$ to give $P'_{2,0}(0)$ (from rule 2 above and verifying that for each phase the sum of all states probabilities is 1); reliability calculation must take care of elements which are not used in the phase considered and can act as standby redundancy ($\lambda \equiv 0$) for working elements; continuing in this way, the *reliability* R_{S0} for the whole mission starting phase 1 in $Z_{1,0}$, follows as

$$R_{S0} = \sum_{Z_j \in U_n} P'_{n,j}(T_n), \quad U_n = \text{set of up states in phase } n. \quad (6.247)$$

5. If a state $Z_{k,i}$ does not appear in the phase $k+1$, the general rule 4 applies.
6. To avoid ambiguities, x starting by $x=0$ at the begin of each phase is used.

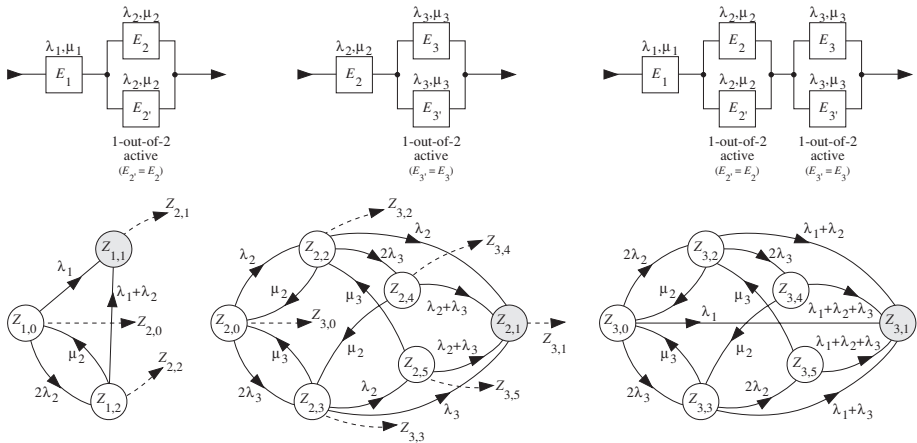


Figure 6.33 Reliability block diagrams and diagram of transition rates for reliability calculation of a *phased-mission system with 3 phases* (the diagram for phase 2 takes care that one element E_2 is put in standby with $\lambda_2 \equiv 0$ as soon as available from phase 1); dashed are indicated to which states the final state probabilities of phase 1 and phase 2 are transferred as initial probabilities for phase 2 and phase 3, respectively (*constant failure & repair rates* (λ_i, μ_i), *ideal failure detection & switch, one repair crew, repair as per first-in first-out*, $Z_{1,1}, Z_{2,1}, Z_{3,1}$ down states, Markov process)

As an example, let us consider the phased-mission system with 3 phases of given (fixed) duration T_1, T_2 and T_3 , described by the 3 reliability block diagrams and the corresponding diagrams of transition rates for reliability investigation given in Fig. 6.33. The diagram of transition rates for phase 2 considers that in phase 2 only one element E_2 is used and assumes that the second element E_2 is put in standby redundancy with failure rate $\lambda_2 \equiv 0$ (either from state $Z_{1,0}$ or as soon as repaired if from state $Z_{1,2}$, assumption 4 on p. 262). Dashed is given to which states the final state probabilities at time T_1 for phase 1 and T_2 ($T_1 + T_2$ with respect to time t) for phase 2 are transferred as initial probabilities for the successive phase. Let us first consider the *asymptotic & steady-state availability* $PA_S = AA_S$ for the whole mission. From Tables 6.10 and 6.6, it follows for the 3 phases (taken separately) that

$$\begin{aligned}
 PA_{1,S} &= AA_{1,S} \approx 1 - (\lambda_1 / \mu_1) - 2(\lambda_2 / \mu_2)^2 \approx 1 - (\lambda_1 / \mu_1), \\
 PA_{2,S} &= AA_{2,S} \approx 1 - (\lambda_2 / \mu_2)^2 - 2(\lambda_3 / \mu_3)^2, \\
 PA_{3,S} &= AA_{3,S} \approx 1 - (\lambda_1 / \mu_1) - 2(\lambda_2 / \mu_2)^2 - 2(\lambda_3 / \mu_3)^2 \approx 1 - (\lambda_1 / \mu_1).
 \end{aligned}
 \tag{6.248}$$

The 2nd equation considers that in phase 2 one of the elements E_2 acts as standby redundancy with failure rate $\lambda_2 \equiv 0$ (assumption 4 on p. 262), combining thus results from Tables 6.6 ($1 - (\lambda_2 / \mu_2)^2$) and 6.10 (2nd row). Equation (6.246) yields then

$$PA_S = AA_S \geq \min(PA_{k,S} = AA_{k,S}) \approx 1 - \lambda_1 / \mu_1, \quad k = 1, 2, 3.
 \tag{6.249}$$

For the reliability R_{S0} , for the whole mission starting in state $Z_{1,0}$ (elements news) at $t=0$, the diagrams of transition rates of Fig. 6.33 yield for phases 1, 2, 3 the following coupled system of differential equations for the state probabilities (Table 6.2; $P'_{i,j}$ is used instead of $P'_{i,j}(x)$, x starts by $x=0$ at the beginning of each phase)

$$\begin{aligned}
 \dot{P}'_{1,0} &= -(\lambda_1 + 2\lambda_2)P'_{1,0} + \mu_2 P'_{1,2}, & \dot{P}'_{1,2} &= -(\lambda_1 + \lambda_2 + \mu_2)P'_{1,2} + 2\lambda_2 P'_{1,0}, \\
 \dot{P}'_{1,1} &= \lambda_1 P'_{1,0} + (\lambda_1 + \lambda_2)P'_{1,2}, & \text{with } P'_{1,0}(0) &= 1, P'_{1,1}(0) = P'_{1,2}(0) = 0; \\
 \\
 \dot{P}'_{2,0} &= -(\lambda_2 + 2\lambda_3)P'_{2,0} + \mu_2 P'_{2,2} + \mu_3 P'_{2,3}, & \dot{P}'_{2,4} &= -(\lambda_2 + \lambda_3 + \mu_2)P'_{2,4} + 2\lambda_3 P'_{2,2}, \\
 \dot{P}'_{2,2} &= -(\lambda_2 + 2\lambda_3 + \mu_2)P'_{2,2} + \lambda_2 P'_{2,0} + \mu_3 P'_{2,5}, & \dot{P}'_{2,5} &= -(\lambda_2 + \lambda_3 + \mu_3)P'_{2,5} + \lambda_2 P'_{2,3}, \\
 \dot{P}'_{2,3} &= -(\lambda_2 + \lambda_3 + \mu_3)P'_{2,3} + 2\lambda_3 P'_{2,0} + \mu_2 P'_{2,4}, & \dot{P}'_{2,1} &= \lambda_2 P'_{2,2} + \lambda_3 P'_{2,3} + (\lambda_2 + \lambda_3)(P'_{2,4} + P'_{2,5}), \\
 \text{with } P'_{2,0}(0) &= P'_{1,0}(T_1), P'_{2,2}(0) = P'_{1,2}(T_1), P'_{2,1}(0) = P'_{1,1}(T_1), P'_{2,3}(0) = P'_{2,4}(0) = P'_{2,5}(0) = 0; \\
 \\
 \dot{P}'_{3,0} &= -(\lambda_1 + 2\lambda_2 + 2\lambda_3)P'_{3,0} + \mu_2 P'_{3,2} + \mu_3 P'_{3,3}, & \dot{P}'_{3,3} &= -(\lambda_1 + 2\lambda_2 + \lambda_3 + \mu_3)P'_{3,3} + 2\lambda_3 P'_{3,0} + \mu_2 P'_{3,4}, \\
 \dot{P}'_{3,2} &= -(\lambda_1 + \lambda_2 + 2\lambda_3 + \mu_2)P'_{3,2} + 2\lambda_2 P'_{3,0} + \mu_3 P'_{3,5}, & \dot{P}'_{3,5} &= -(\lambda_1 + \lambda_2 + \lambda_3 + \mu_3)P'_{3,5} + 2\lambda_2 P'_{3,3}, \\
 \dot{P}'_{3,4} &= -(\lambda_1 + \lambda_2 + \lambda_3 + \mu_2)P'_{3,4} + 2\lambda_3 P'_{3,2}, & \dot{P}'_{3,1} &= \lambda_1 P'_{3,0} + (\lambda_1 + \lambda_2)P'_{3,2} + (\lambda_1 + \lambda_3)P'_{3,3} + (\lambda_1 + \lambda_2 + \lambda_3)(P'_{3,4} + P'_{3,5}), \\
 \text{with } P'_{3,0}(0) &= P'_{2,0}(T_2), P'_{3,2}(0) = P'_{2,2}(T_2), P'_{3,3}(0) = P'_{2,3}(T_2), P'_{3,4}(0) = P'_{2,4}(T_2), \\
 P'_{3,5}(0) &= P'_{2,5}(T_2), P'_{3,1}(0) = P'_{2,1}(T_2). & & (6.250)
 \end{aligned}$$

From Eq. (6.247) it follows then

$$R_{S0} = P'_{3,0}(T_3) + P'_{3,2}(T_3) + P'_{3,3}(T_3) + P'_{3,4}(T_3) + P'_{3,5}(T_3). \quad (6.251)$$

Analytical solution of the system given by Eq. (6.250) is possible, but time consuming. A numerical solution is given in Example 6.26. A lower bound R_{S0l} on the reliability R_{S0} for the whole mission is obtained by connecting the reliability block diagrams for each phase in series (Eq. (6.241)). For Fig. 6.33, this corresponds, nearly, to consider phase 3 for a time span $T_1 + T_2 + T_3$ (per assumption 4 on p. 262, for element E_2 a second element E_2 in standby redundancy is available in phase 2). Using $R_{S0l} \approx e^{-(T_1 + T_2 + T_3)/MTTF_{S0}}$ with $MTTF_{S0}$ as per Table 6.10 (2nd & 3rd row), it follows that

$$R_{S0} > R_{S0l} \approx e^{-(T_1 + T_2 + T_3)(\lambda_1 + 2\lambda_2^2/\mu_2 + 2\lambda_3^2/\mu_3)}. \quad (6.252)$$

An upper bound on R_{S0} follows from Eq. (6.241), see Example 6.26.

If the second element E_2 were not available in phase 2 as standby redundancy, $PA_{2,S} = AA_{2,S} \approx 1 - \lambda_2/\mu_2$ and, from Eq. (6.249), $PA_S = AA_S \approx 1 - \lambda_2/\mu_2$, since $\lambda_1/\mu_1 < \lambda_2/\mu_2$ can be assumed when considering the reliability block diagram for phase 1. In this case, and assuming that the second element E_2 would be repaired before the end of phase 2 (if in a failed state at the end of phase 1), the diagram of transition rates for phase 2 would be equal to that for phase 1, with $\lambda_1 \rightarrow \lambda_2$, $\lambda_2 \rightarrow \lambda_3$, $\mu_2 \rightarrow \mu_3$, $Z_{1,0} \rightarrow Z_{2,0}$, $Z_{1,1} \rightarrow Z_{2,1}$, $Z_{1,2} \rightarrow Z_{2,3}$, and

$$P'_{2,0}(0) = P'_{1,0}(T_1) + P'_{1,2}(T_1), P'_{2,1}(0) = P'_{1,1}(T_1), P'_{2,3}(0) = 0. \quad (6.255)$$

Example 6.26

Give the numerical solution of Eqs. (6.250) and (6.251) for $\lambda_1 = 10^{-4} \text{ h}^{-1}$, $\lambda_2 = 10^{-2} \text{ h}^{-1}$, $\lambda_3 = 10^{-3} \text{ h}^{-1}$, $\mu_1 = \mu_2 = \mu_3 = 0.5 \text{ h}^{-1}$, $T_1 = 168 \text{ h}$, $T_2 = 336 \text{ h}$, and $T_3 = 672 \text{ h}$.

Solution

Numerical solution of the 3 coupled systems of differential equations given by Eq. (6.250) yields

$$\begin{aligned} P'_{3,0}(T_3) &= 0.598655, & P'_{3,2}(T_3) &= 0.023493, & P'_{3,3}(T_3) &= 0.002388, \\ P'_{3,4}(T_3) &= 0.000092, & P'_{3,5}(T_3) &= 0.000094, & P'_{3,1}(T_3) &= 0.375278 \end{aligned} \quad (6.253)$$

(with 6 digits because of $P'_{3,4}(T_3)$ and $P'_{3,5}(T_3)$). R_{S0} follows then from Eq. (6.251)

$$R_{S0} = 1 - P'_{3,1}(T_3) = 0.625. \quad (6.254)$$

Supplementary results: Computing lower and upper bound on R_{S0} as per Eqs. (6.252) and (6.241), yields for the above example $0.55 \leq R_{S0} \leq 0.71$ (considering assumption 4 on p. 262 for R_{S01}).

The corresponding initial probabilities for phase 3 would be

$$\begin{aligned} P'_{3,0}(0) &= P'_{2,0}(T_2), & P'_{3,1}(0) &= P'_{2,1}(T_2), & P'_{3,3}(0) &= P'_{2,3}(T_2), \\ P'_{3,2}(0) &= P'_{3,4}(0) = P'_{3,5}(0) = 0. \end{aligned} \quad (6.256)$$

If an element E_{ser} where common to all 3 phases in Fig. 6.33 (i.e. in series with all 3 reliability block diagrams), Table 6.10 (2nd row) can be used to find

$$PA_{S_{tot}} = AA_{S_{tot}} \approx 1 - \lambda_{ser} / \mu_{ser} - \lambda_1 / \mu_1 \quad (6.257)$$

(considering Eq. (6.249)) and, with R_{S0} from Eq. 6.251,

$$R_{S0_{tot}} \approx R_{S0} \cdot e^{-\lambda_{ser}(T_1+T_2+T_3)}. \quad (6.258)$$

The above procedure can be extended to consider more than one repair crew at system level or any kind of repair (restore) strategy. Other procedures (models) are conceivable. For instance, for *nonrepairable* systems (up to system failure) of complex structure, and with independent elements (parallel redundancy), it can be useful to number the states using binary considerations.

For randomly distributed phase duration, Eq. (6.246) can be used for availability. Reliability can be obtained by expanding results in Examples 6.23 -6.25.

An alternative approach for phased-mission systems is to assume that at the beginning of each mission phase, the system is *as-good-as-new* with respect to the elements used in the mission phase considered (required elements are repaired in a negligible time at the begin of the mission phase, if they are in a failed state, and not required elements can be repaired during a phase in which they are not used). This assumption can be reasonable for some repairable systems and highly simplifies investigation. For this case, results developed in Section 6.8.2 for preventive maintenance can be used, and lead to (for phases 1, 2,...)

$$\begin{aligned}
R_S(t) &= R_{S1}(t), & \text{for } 0 \leq t < T_1^* \\
&= R_{S1}(T_1^*) R_{S2}(t - T_1^*), & \text{for } T_1^* \leq t < T_2^* \\
&= R_{S1}(T_1^*) R_{S2}(T_2^* - T_1^*) R_{S3}(t - T_2^*), & \text{for } T_2^* \leq t < T_3^* \\
&\vdots &
\end{aligned} \tag{6.259}$$

for the reliability function, and

$$\begin{aligned}
PA_S(t) &= PA_{S1}(t), & \text{for } 0 \leq t < T_1^* \\
&= PA_{S2}(t - T_1^*), & \text{for } T_1^* \leq t < T_2^* \\
&= PA_{S3}(t - T_2^*), & \text{for } T_2^* \leq t < T_3^* \\
&\vdots &
\end{aligned} \tag{6.260}$$

for the point availability. S_i is the state from which the i th mission phase starts; $0, T_1^*, T_2^*, \dots$ are the time points on the time axis at which the mission phase 1, 2, 3, ... begin (the mission duration of phase i being here $T_i^* - T_{i-1}^*$ with $T_0^* = 0$).

6.8.6.3 Failure Censored Reconfiguration

In most applications, reconfiguration occurs *at the failure of a redundant element*. Besides cases with ideal fault coverage, ideal switching, and no system performance reduction at failure (Sections 2.2, 2.3, and 6.4 - 6.7), more complex structures often arise in practical applications (see Sections 6.8.3 - 6.8.5 for some examples). Such structures must be investigated on a case-by-case basis, and an FMEA / FMECA (Section 2.6) is mandatory to validate investigations. Often it is necessary to consider that after a reconfiguration, the system performance is reduced, i.e., *reward and frequency / duration* aspects have to be involved in the analysis.

A reasonably simple and comprehensive example is a power system substation. Figure 6.34 gives the functional block diagram and the *diagram of transition rates* for availability calculation, $\mu_g \equiv 0$ for reliability investigation. Z_{12} is the down state. The substation is powered by a reliable network and consists of:

- Two branch *designated by A_1 & A_2 and capable of performing 100% load*, each with HV switch, HV circuit breaker and control elements, transformer, measurement & control elements, and LV switch.
- Two busbars *designated by C_1 & C_2 and capable of performing 100% load* (failure rate basically given by double contingency of faults on control elements).
- A coupler between the busbars, *designated by B and capable of performing 100% load*; failure modes *stuck at the state occupied just before failure* (does not open), failure rate $\lambda_{B\sigma}$, and *no connection* (does not close), failure rate λ_{B0} .

Load is distributed between C_1 and C_2 at 50% rate each. The *diagram of transition rates* is based on an extensive FMEA/FMECA [6.20 (2002)] showing in particular the key position of the coupler B in the reconfiguration strategy. Coupler B is *normally open*. A failure of B is recognized only at a failure of A or C . From state Z_0 , B can fail only with failure mode *no connection* (does not close), from Z_1 or Z_2 only with

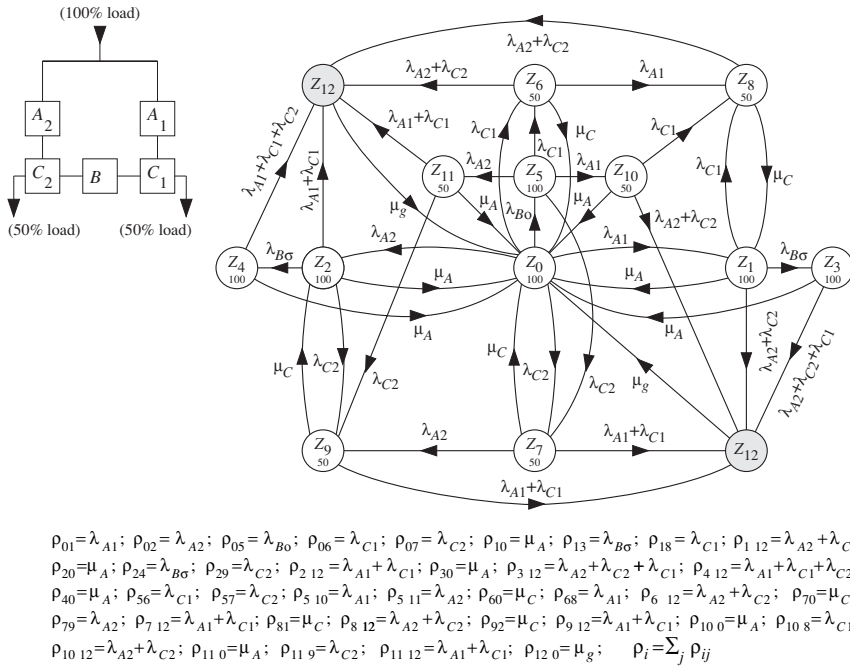


Figure 6.34 Functional block diagram and diagram of transition rates for a repairable power system substitution with active redundancy, constant failure and repair rates ($\lambda_{A1}, \lambda_{A2}, \lambda_{B\sigma}, \lambda_{B0}, \lambda_{C1}, \lambda_{C2}, \mu_A, \mu_C, \mu_g$), imperfect switching of B (failure modes does not open ($\lambda_{B\sigma}$, from Z_1 and Z_2) or no connection (λ_{B0} , from Z_0)), failure of B recognized only at failure of A or C, ideal failure detection & localization for A and C, one repair crew, repair priority on C, no further failure at system down (Z_{12} down state (absorbing for rel. calculation ($\mu_g \equiv 0$)), Markov process)

stuck at the state occupied just before failure (does not open). Constant failure & repair rates $\lambda_{A1}, \lambda_{A2}, \lambda_{B\sigma}, \lambda_{B0}, \lambda_{C1}, \lambda_{C2}$ & μ_A, μ_C, μ_g are assumed. μ_A & μ_C are the same also if a repair of B is necessary; μ_g is larger than μ_A & μ_C . From the down state (Z_{12}) the system returns to state Z_0 . Furthermore, only one repair crew, repair priority on C (followed by C+B, A, A+B), and no further failure at system down (50% load is an up state with reduced performance) are assumed. Asked are mean time to system failure $MTTF_{S0}$ for system new (in state Z_0) at $t = 0$ and asymptotic & steady-state point and average availability $PA_S = AA_S$. The involved process is a time-homogeneous Markov process. If results are required for 100% load, $Z_6 - Z_{12}$ are down states (see Section 6.8.6.4 for reward considerations). To simplify investigation, $\lambda_{A1} = \lambda_{A2} = \lambda_A$ and $\lambda_{C1} = \lambda_{C2} = \lambda_C$ are assumed. To increase readability, the number of states in Fig. 6.34 has been reduced as per Point 2 on p. 277).

From Fig. 6.34 and Table 6.2 or Eq. (A7.126) it follows that $MTTF_{S0}$ is given as solution of the following system of algebraic equations (with $M_i = MTF_{S_i}$)

$$\begin{aligned}
 \rho_0 M_0 &= 1 + \lambda_{B0} M_5 + \lambda_A (M_1 + M_2) + \lambda_C (M_6 + M_7), & \rho_5 M_5 &= 1 + \lambda_A (M_{10} + M_{11}) + \lambda_C (M_6 + M_7), \\
 \rho_1 M_1 &= 1 + \mu_A M_0 + \lambda_C M_8 + \lambda_{B0} M_3, & \rho_2 M_2 &= 1 + \mu_A M_0 + \lambda_C M_9 + \lambda_{B0} M_4, & \rho_3 M_3 &= 1 + \mu_A M_0, \\
 \rho_4 M_4 &= 1 + \mu_A M_0, & \rho_6 M_6 &= 1 + \lambda_A M_8 + \mu_C M_0, & \rho_7 M_7 &= 1 + \lambda_A M_9 + \mu_C M_0, & \rho_8 M_8 &= 1 + \mu_C M_1, \\
 \rho_9 M_9 &= 1 + \mu_C M_2, & \rho_{10} M_{10} &= 1 + \mu_A M_0 + \lambda_C M_8, & \rho_{11} M_{11} &= 1 + \mu_A M_0 + \lambda_C M_9.
 \end{aligned} \tag{6.261}$$

Because of $\lambda_{A1} = \lambda_{A2} = \lambda_A$, $\lambda_{C1} = \lambda_{C2} = \lambda_C$ and the symmetry in Fig. 6.34 it follows that $\rho_2 = \rho_1$, $\rho_4 = \rho_3$, $\rho_7 = \rho_6$, $\rho_9 = \rho_8$, $\rho_{11} = \rho_{10}$ and $M_2 = M_1$, $M_4 = M_3$, $M_7 = M_6$, $M_9 = M_8$, $M_{11} = M_{10}$. This has been considered in solving the system of algebraic equations (6.261). From Eq. (6.261) it follows that

$$\begin{aligned}
 MTTFS_0 &= \\
 &= \frac{a_1 a_2 + 2a_1 a_3 \lambda_A + 2a_2 \lambda_C \rho_5 \rho_{10} (\rho_8 + \lambda_A) + 2a_3 \lambda_A \lambda_C \mu_C \rho_5 \rho_{10} + \lambda_{B0} (a_2 a_4 + a_3 a_6)}{a_1 a_2 \rho_0 - 2\lambda_A \mu_A \rho_8 (\rho_3 + \lambda_{B0}) (a_1 + \lambda_C \mu_C \rho_5 \rho_{10}) - 2a_2 \lambda_C \mu_C \rho_5 \rho_8 \rho_{10} - \lambda_{B0} (a_2 a_5 + a_6 \mu_A \rho_8 (\rho_3 + \lambda_{B0}))},
 \end{aligned} \tag{6.262}$$

with

$$\begin{aligned}
 a_1 &= \rho_5 \rho_6 \rho_8 \rho_{10}, & a_2 &= \rho_6 \rho_8 - \rho_3 \lambda_C \mu_C, & a_4 &= \rho_6 \rho_8 \rho_{10} + 2\lambda_A \rho_6 (\rho_8 + \lambda_C) + 2\lambda_C \rho_{10} (\rho_8 + \lambda_A), \\
 a_3 &= \rho_8 (\rho_3 + \lambda_{B0}) + \rho_3 \lambda_C, & a_5 &= 2\lambda_A \mu_A \rho_6 \rho_8 + 2\lambda_C \mu_C \rho_8 \rho_{10}, & a_6 &= 2\lambda_A \lambda_C \mu_C (\rho_6 + \rho_{10}),
 \end{aligned} \tag{6.263}$$

and

$$\begin{aligned}
 \rho_0 &= 2\lambda_A + 2\lambda_C + \lambda_{B0}, & \rho_1 &= \rho_2 = \lambda_A + 2\lambda_C + \lambda_{B0} + \mu_A, & \rho_3 &= \rho_4 = \lambda_A + 2\lambda_C + \mu_A, & \rho_5 &= 2(\lambda_A + \lambda_C), \\
 \rho_6 &= \rho_7 = 2\lambda_A + \lambda_C + \mu_C, & \rho_8 &= \rho_9 = \lambda_A + \lambda_C + \mu_C, & \rho_{10} &= \rho_{11} = \lambda_A + 2\lambda_C + \mu_A, & \rho_{12} &= \mu_g.
 \end{aligned} \tag{6.264}$$

$MTTFS_0$ per Eq. (6.262) can be approximated by

$$MTTFS_0 \approx \frac{\mu_A + 5(\lambda_A + \lambda_C) + (4\lambda_A + 5\lambda_C)\mu_A / \mu_C + \lambda_{B0} + \lambda_{B0}(\mu_A + \lambda_{B0}) / 2(\lambda_A + \lambda_C)}{(2\lambda_A + 2\lambda_C + \lambda_{B0})(\lambda_A + \lambda_C \mu_A / \mu_C)}, \tag{6.265}$$

yielding $MTTFS_0 \approx \mu / 2(\lambda_A + \lambda_C)^2$ for $\lambda_{B0} = \lambda_{B0} = 0$ and $\mu_A = \mu_C = \mu$ (1-out-of-2 active redundancy with A and C in series, as per Table 6.10, 2nd & 3rd row).

From Fig. 6.34 and Table 6.2 or Eq. (A7.127) it follows that the asymptotic & steady-state point and average availability $PA_S = AA_S$ is given as solution of

$$\begin{aligned}
 \rho_0 P_0 &= \mu_A (P_1 + P_2 + P_3 + P_4 + P_{10} + P_{11}) + \mu_C (P_6 + P_7) + \mu_g P_{12}, & \rho_1 P_1 &= \lambda_A P_0 + \mu_C P_8, \\
 \rho_2 P_2 &= \lambda_A P_0 + \mu_C P_9, & \rho_3 P_3 &= \lambda_{B0} P_1, & \rho_4 P_4 &= \lambda_{B0} P_2, & \rho_5 P_5 &= \lambda_{B0} P_0, \\
 \rho_6 P_6 &= \lambda_C (P_0 + P_5), & \rho_7 P_7 &= \lambda_C (P_0 + P_5), & \rho_8 P_8 &= \lambda_A P_6 + \lambda_C (P_1 + P_{10}), \\
 \rho_9 P_9 &= \lambda_A P_7 + \lambda_C (P_2 + P_{11}), & \rho_{10} P_{10} &= \lambda_A P_5, & \rho_{11} P_{11} &= \lambda_A P_5, \\
 \rho_{12} P_{12} &= (\lambda_A + \lambda_C) (P_1 + P_2 + P_6 + P_7 + P_8 + P_9 + P_{10} + P_{11}) + (\lambda_A + 2\lambda_C) (P_3 + P_4).
 \end{aligned} \tag{6.266}$$

One of the Eq. (6.266) must be dropped and replaced by $\sum P_i = 1$. The solution yields

$$\begin{aligned}
 P_1 &= P_2 = b_1 P_0, & P_3 &= P_4 = b_1 P_0 \lambda_{B0} / \rho_3, & P_5 &= P_0 \lambda_{B0} / \rho_5, & P_8 &= P_9 = b_2 P_0, \\
 P_6 &= P_7 = P_0 \lambda_C (\rho_5 + \lambda_{B0}) / \rho_5 \rho_6, & P_{10} &= P_{11} = P_0 \lambda_A \lambda_{B0} / \rho_5 \rho_{10}, & P_{12} &= b_3 P_0,
 \end{aligned} \tag{6.267}$$

with

$$P_0 = \frac{1}{1 + 2b_2 + 2b_1(1 + \lambda_{B\sigma}/\rho_3) + \lambda_{B0}/\rho_5 + 2\lambda_C(\rho_5 + \lambda_{B0})/\rho_5\rho_6 + 2\lambda_A\lambda_{B0}/\rho_5\rho_{10} + b_3} \quad (6.268)$$

and

$$\begin{aligned} b_1 &= \frac{\rho_5\rho_6\rho_8\rho_{10}\lambda_A + \rho_{10}\lambda_A\lambda_C\mu_C(\rho_5 + \lambda_{B0}) + \rho_6\lambda_A\lambda_C\lambda_{B0}\mu_C}{\rho_1\rho_5\rho_6\rho_8\rho_{10} - \rho_5\rho_6\rho_{10}\lambda_C\mu_C}, \\ b_2 &= b_1 \frac{\lambda_C}{\rho_8} + \frac{\lambda_A\lambda_C(\rho_5 + \lambda_{B0})}{\rho_6\rho_8\rho_5} + \frac{\lambda_A\lambda_C\lambda_{B0}}{\rho_5\rho_8\rho_{10}}, \\ b_3 &= \frac{2(\lambda_A + \lambda_C)}{\rho_{12}} [b_1 + b_2 + \frac{\lambda_C(\rho_5 + \lambda_{B0})}{\rho_5\rho_6} + \frac{\lambda_A\lambda_{B0}}{\rho_5\rho_{10}}] + 2(\lambda_A + 2\lambda_C) \frac{\lambda_{B\sigma}}{\rho_3\rho_{12}}. \end{aligned} \quad (6.269)$$

From Eqs. (6.267) - (6.269) it follows that

$$\begin{aligned} PA_S = AA_S &= \sum_{i=0}^{11} P_i = 1 - P_{12} = 1 - b_3 P_0 \\ &= \frac{1}{1 + \frac{b_3}{1 + 2b_2 + 2b_1(1 + \lambda_{B\sigma}/\rho_3) + \lambda_{B0}/\rho_5 + 2\lambda_C(\rho_5 + \lambda_{B0})/\rho_5\rho_6 + 2\lambda_A\lambda_{B0}/\rho_5\rho_{10}}} \end{aligned} \quad (6.270)$$

$PA_S = AA_S$ per Eq. (6.270) can be approximated by

$$PA_S = AA_S \approx 1 - \frac{2(\lambda_A + \lambda_C)(\lambda_C\mu_A + \mu_C(\lambda_A + \lambda_{B\sigma})) + \lambda_{B0}(\lambda_A\mu_C + \lambda_C(\mu_A + \mu_C\lambda_{B\sigma}/\lambda_{B0}))}{\mu_g[\mu_A\mu_C + 2(\lambda_A\mu_C + \lambda_C\mu_A)(1 + \lambda_{B0}/(\lambda_A + \lambda_C)) + 2\lambda_A\lambda_{B\sigma}\mu_C/\mu_A]} \quad (6.271)$$

yielding $PA_S = AA_S \approx 1 - 2(\lambda_A + \lambda_C)/\mu^2$ for $\lambda_{B\sigma} = \lambda_{B0} = 0$ and $\mu_A = \mu_C = \mu_g = \mu$ (1-out-of-2 active redundancy with A and C in series, as per Table 6.10). Equations (6.265) and (6.271) show the small influence of the coupler B. A numerical evaluation with

$$\begin{aligned} \lambda_{A1} = \lambda_{A2} = \lambda_A &= 4 \cdot 10^{-6} \text{ h}^{-1} && (\approx 0.035 \text{ mean expected failures per year}) \\ \lambda_{C1} = \lambda_{C2} = \lambda_C &= 0.12 \cdot 10^{-6} \text{ h}^{-1} && (\approx 0.001 \text{ mean expected failures per year}) \\ \lambda_{B\sigma} &= 0.08 \cdot 10^{-6} \text{ h}^{-1} && (\approx 0.0007 \text{ mean expected failures per year}) \\ \lambda_{B0} &= 0.6 \cdot 10^{-6} \text{ h}^{-1} && (\approx 0.005 \text{ mean expected failures per year}) \\ \mu_A = \mu_C &= 1/4\text{h}, \quad \mu_g = 1/12\text{h} \end{aligned}$$

yields, from Eqs.(6.262) & (6.270),

$$MTTF_{S0} \approx 7.364 \cdot 10^9 \text{ h} \quad \& \quad PA_S = AA_S \approx 1 - 1.63 \cdot 10^{-9}$$

and, from Eqs. (6.265) & (6.271), $MTTF_{S0} \approx 7.36 \cdot 10^9 \text{ h}$ & $PA_S = AA_S \approx 1 - 1.78 \cdot 10^{-9}$; moreover,

$$\begin{aligned} P_0 &\approx 0.932096, & P_1 = P_2 &\approx 1.491 \cdot 10^{-5}, & P_3 = P_4 &\approx 4.77 \cdot 10^{-12}, & P_5 &\approx 0.067871, \\ P_6 = P_7 &\approx 4.80 \cdot 10^{-7}, & P_8 = P_9 &\approx 1.53 \cdot 10^{-11}, & P_{10} = P_{11} &\approx 1.09 \cdot 10^{-6}, & P_{12} &\approx 1.63 \cdot 10^{-9}. \end{aligned}$$

Considering the substation as a *macro-structure* (first row in Table 6.10), it holds that $PA_S = AA_S \approx 1 - \lambda_S/\mu_S$ and $R_S(t) \approx e^{-\lambda_S t}$, with $\mu_S = \mu_g$ and $\lambda_S = 1/MTTF_{S0}$.

6.8.6.4 Reward and Frequency / Duration Aspects

For some applications, e.g. in power and communication systems, it is of importance to consider system performance also in the presence of failures. *Reward and frequency/duration* aspects are of interest to evaluate *system performability*. For constant failure and repair rates (time-homogeneous Markov processes), asymptotic & steady-state *system failure frequency* f_{udS} , *system repair(restoration) frequency* f_{duS} , *system mean up time* MUT_S , and *system mean down time* MDT_S (mean repair (restoration) duration at system level) are given as (Eqs. (A7.141)-(A7.146))⁺⁾

$$f_{udS} = \sum_{Z_j \in U} P_j (\sum_{Z_i \in \bar{U}} \rho_{ji}) = f_{duS} = \sum_{Z_i \in \bar{U}} P_i (\sum_{Z_j \in U} \rho_{ij}) = 1 / (MUT_S + MDT_S) \quad (6.272)$$

and

$$MDT_S = MUT_S (1 - PA_S) / PA_S = (1 - PA_S) / f_{udS}, \quad PA_S = \sum_{Z_j \in U} P_j, \quad (6.273)$$

respectively (Eq. (6.273) can be heuristically explained, considering that for $T \rightarrow \infty$, $(1 - PA_S)T$ is the total *mean down time* and $T \cdot f_{duS}$ the total *mean number of repairs* in $(0, T]$). U is the set of states considered as *up states* for f_{udS} and MDT_S calculation, \bar{U} is the complement to the totality of states considered. P_j is the asymptotic & steady-state probability of state Z_j and ρ_{ji} the transition rate from Z_j to Z_i . In Eq.(6.272), all transition rates ρ_{ji} leaving state $Z_j \in U$ toward $Z_i \in \bar{U}$ are considered (cumulated states). Example 6.27 gives an application to the substation of Fig. 6.34.

Example 6.27

Give the *failure frequency* f_{udS} and the *mean (expected) failure duration* MDT_S in steady-state for the substation of Fig. 6.34 for failures referred to a load loss of 100% and $\geq 50\%$, respectively.

Solution

For loss of 100% load, Fig. 6.34 with $U = \{Z_0, \dots, Z_{11}\}$, $\bar{U} = \{Z_{12}\}$ yields (P_i as per Eq. (6.267))

$$f_{udS \text{ loss } 100\%} = 2(P_1 + P_6 + P_8 + P_{10})(\lambda_A + \lambda_C) + 2P_3(\lambda_A + 2\lambda_C).$$

For loss of $\geq 50\%$ load, Fig. 6.34 with $U = \{Z_0 - Z_5\}$ and $\bar{U} = \{Z_6 - Z_{12}\}$ yields

$$f_{udS \text{ loss } \geq 50\%} = P_0 2\lambda_C + 2P_1(\lambda_A + 2\lambda_C) + 2P_3(\lambda_A + 2\lambda_C) + P_5 2(\lambda_A + \lambda_C).$$

From Eq. (6.273) it follows that

$$MDT_{S \text{ loss } 100\%} = P_{12} / f_{udS \text{ loss } 100\%}, \quad MDT_{S \text{ loss } \geq 50\%} = (1 - (P_0 + 2P_1 + 2P_3 + P_5)) / f_{udS \text{ loss } \geq 50\%}.$$

The numerical example on p. 269 yields $f_{udS \text{ loss } 100\%} \approx 136 \cdot 10^{-12} \text{ h}^{-1}$ ($\approx 10^{-6}$ expected failures per year), $f_{udS \text{ loss } 50\%} \approx 783 \cdot 10^{-9} \text{ h}^{-1}$ ($\approx 7 \cdot 10^{-3}$ expected failures per year),

$$MDT_{S \text{ loss } 100\%} = 12 \text{ h} = 1/\mu_g \quad \text{and} \quad MDT_{S \text{ loss } \geq 50\%} \approx 4 \text{ h}.$$

Supplementary results: For the system mean up time $MUT_S = MDT_S \cdot PA_S / (1 - PA_S)$, the numerical example on p. 269 yields $MUT_{S \text{ loss } 100\%} \approx (12 / 1.63) 10^9 \text{ h} \cong MTTF_{50}$.

⁺⁾ Similar results hold for semi-Markov processes.

Example 6.28

Give the *mean* (expected) *reward rate* in steady-state for the substation of Fig. 6.34.

Solution

Considering Fig. 6.34 and the numerical example on p. 269 it follows that

$$MIR_S = 1 \cdot (P_0 + 2P_1 + 2P_3 + P_5) + 0.5 \cdot (2P_6 + 2P_8 + 2P_{10}) \approx 0.9999984.$$

The *reward rate* r_i takes care of the performance reduction in the state considered, ($r_i = 0$ for down states, $0 < r_i < 1$ for partially down states, and $r_i = 1$ for up states with 100% performance). From this, the *mean* (expected) *reward rate* in steady-state or for $t \rightarrow \infty$, MIR_S , is given as (Eq. (A7.147))

$$MIR_S = \sum_{i=0}^m r_i P_i, \quad (6.274)$$

see Example 6.28 for an application. The *mean* (expected) *accumulated reward* in steady-state (or for $t \rightarrow \infty$) follows as $MAR_S(t) = MIR_S \cdot t$. P_i in Eq. (6.274) is the asymptotic & steady-state probability of state Z_i , giving also the expected percentage of time the system stays at the performance level specified by Z_i (Eq. (A7.132)).

6.8.7 Systems with Common Cause Failures

In some practical applications it is necessary to consider that common cause failures can occur. *Common cause failures* (C) are multiple failures resulting from a single cause. They must be distinguished from *common mode failures*, which are multiple failures showing the same symptom. Common cause failures can occur in hardware as well as in software. Their causes can be quite different. Some possible causes for common cause failures in hardware are:

- overload (electrical, thermal, mechanical),
- technological weakness (material, design, production),
- misuse (e.g. caused by operating or maintenance personnel),
- external event.

Similar causes can be found for software.

In the following, a 1-out-of-2 active redundancy is used as a basic example for investigating effects of common cause failures. Results (Eqs. (6.276) & (6.280)) show that common cause failure acts (in general) as a *series element* in the system's reliability structure, with failure rate equal the occurrence rate δ_C of the common cause failure and repair (restoration) rate equal the remove rate μ_C of the common cause failure. Equation (6.280) or graphs given by Figs. 2.8 & 6.17, and rules (2.28) & (6.174) can be used to limit effects of common cause failures (δ_C instead of λ_2).

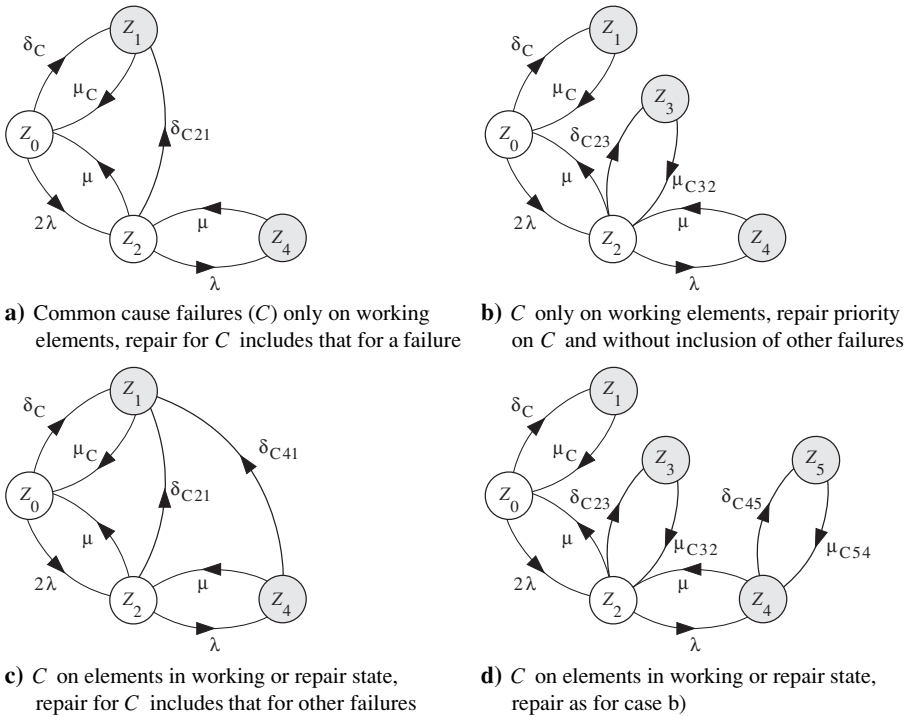
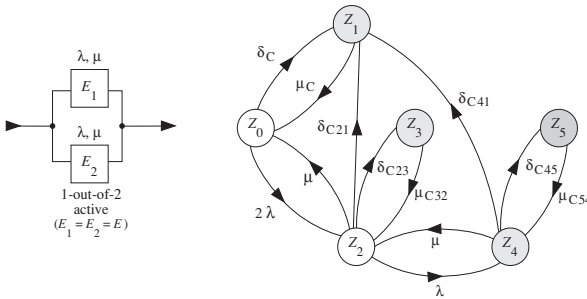


Figure 6.35 Diagram of transition rates for the 1-out-of-2 active redundancy of Fig. 6.36 with common cause failures (C) for 4 different basic possibilities, constant failure and repair rates ($\lambda, \mu, \mu_C, \mu_{C_i}$), constant occurrence rates for C (δ_C, δ_{C_i} often with $\delta_{C_i} = \delta_C$), ideal failure detection and switch, one repair crew, repair priority on C , no further failures at system down (except for $\delta_{C41}, \delta_{C45}$) (Z_1, Z_3, Z_4, Z_5 down states (absorbing for reliability calculation), Markov processes)

Figure 6.35 gives the diagrams of transition rates for the repairable 1-out-of-2 active redundancy of Fig. 6.36 with common cause failures for 4 different basic possibilities (C refers to *common cause failures*, repair priority on C , one repair crew, no further failures at system down except for $\delta_{C41}, \delta_{C45}$). To clarify results, occurrence rates δ_{C_i} and repair rates μ_{C_i} for common cause failures are assumed to be each other different when moving from one state to the other ($\delta_{C_{01}} \equiv \delta_C$ and $\mu_{C_{10}} \equiv \mu_C$ is used to simplify the interpretation of Eqs. (6.276) & (6.279)). The 4 possibilities of Fig. 6.35 are resumed in Fig. 6.36 for investigation. From Fig. 6.36 and Table 6.2, $MTTF_{S0}$ is given as solution of the following system of algebraic equations (all down states (Z_1, Z_3, Z_4, Z_5) are absorbing for reliability investigation)

$$(2\lambda + \delta_C) MTTF_{S0} = 1 + 2\lambda MTTF_{S2}, \quad (\lambda + \delta_{C21} + \delta_{C23} + \mu) MTTF_{S2} = 1 + \mu MTTF_{S0}. \quad (6.275)$$

From Eq. (6.275), $MTTF_{S0}$ follows as (for $\delta_C \equiv \delta_{C01} \leq \lambda$),



$$\begin{aligned}
 \rho_{01} &= \delta_C; \quad \rho_{02} = 2\lambda \quad (\lambda + \lambda_r \text{ for warm redundancy}); \quad \rho_{24} = \lambda; \quad \rho_{21} = \delta_{C21}; \\
 \rho_{23} &= \delta_{C23}; \quad \rho_{41} = \delta_{C41}; \quad \rho_{45} = \delta_{C45}; \quad \rho_{10} = \mu_C; \quad \rho_{32} = \mu_{C32}; \quad \rho_{20} = \rho_{42} = \mu; \\
 \rho_{54} &= \mu_{C54}; \quad \rho_i = \sum \rho_{ij}; \quad \text{for } R_S(t) \text{ set } \rho_{10} = \rho_{32} = \rho_{41} = \rho_{42} = \rho_{45} = 0
 \end{aligned}$$

Figure 6.36 Reliability block diagram and diagram of transition rates for availability calculation of a 1-out-of-2 active redundancy with common cause failures (C) for different possibilities as per Fig. 6.35 (one repair crew, Z_1, Z_3, Z_4, Z_5 down states (absorbing for reliability calculation), Markov process)

$$MTTF_{S0} = \frac{3\lambda + \delta_{C21} + \delta_{C23} + \mu}{(2\lambda + \delta_C)(\lambda + \delta_{C21} + \delta_{C23}) + \mu \delta_C} \leq \frac{1}{\delta_C} . \tag{6.276}$$

Furthermore, from Fig. 6.36 and Table 6.2, the asymptotic & steady-state point and average availability $PA_S = AA_S$ is given as solution of the following system of algebraic equations

$$\begin{aligned}
 \rho_0 P_0 &= \mu_C P_1 + \mu P_2, & \rho_1 P_1 &= \delta_C P_0 + \delta_{C21} P_2 + \delta_{C41} P_4, & \rho_5 P_5 &= \delta_{C45} P_4, \\
 \rho_3 P_3 &= \delta_{C23} P_2, & \rho_4 P_4 &= \lambda P_2 + \mu_{C54} P_5, & \rho_2 P_2 &= 2\lambda P_0 + \mu_{C32} P_3 + \mu P_4.
 \end{aligned} \tag{6.277}$$

One of the Eq.(6.277) must be dropped and replaced by $P_0 + \dots + P_5 = 1$ (the first equation because of the particular cases investigated below). The solution yields

$$PA_S = AA_S = P_0 + P_2 = \frac{1 + a_2}{a_3 + \delta_C / \rho_1 + a_1 a_2 \delta_{C41} / \rho_1 + a_2 \delta_{C21} / \rho_1} . \tag{6.278}$$

with

$$\begin{aligned}
 a_1 &= \lambda \rho_5 / (\rho_4 \rho_5 - \delta_{C45} \mu_{C54}), & a_2 &= 2\lambda \rho_3 / (P_2 \rho_3 - \delta_{C23} \mu_{C32} - a_1 \mu \rho_3), \\
 a_3 &= 1 + a_2 (1 + \delta_{C23} / \rho_3) + a_1 a_2 (1 + \delta_{C45} / \rho_5), & \rho_0 &= 2\lambda + \delta_C, \quad \rho_1 = \mu_C, \\
 \rho_2 &= \lambda + \delta_{C21} + \delta_{C23} + \mu, & \rho_3 &= \mu_{C32}, \quad \rho_4 = \delta_{C41} + \delta_{C45} + \mu, \quad \rho_5 = \mu_{C54}.
 \end{aligned}$$

Considering $\lambda \ll \mu, \delta_C \ll \mu_C, \delta_{Ci} \ll \mu_{Ci}$ it follows that

$$PA_S = AA_S \lesssim \mu_C / (\delta_C + \mu_C) \approx 1 - \delta_C / \mu_C . \tag{6.279}$$

Equations (6.276) and (6.278) show that the effect of common cause failures becomes negligible for

$$\delta_C \ll 2\lambda^2 / \mu, \quad \text{assuming } \delta_C, \delta_{C21}, \delta_{C23} \ll \lambda \ll \mu . \tag{6.280}$$

Equations (6.276) & (6.278) can be used to investigate Fig. 6.35 (for instance, with $\delta_{C23} = \delta_{C41} = \delta_{C45} = 0$, $0 < \mu_{C32}, \mu_{C54} < \infty$ for case a), yielding

$$MTTF_{S0} = \frac{1}{\delta_C + \frac{2\lambda(\lambda + \delta_{C21} - \delta_C)}{3\lambda + \delta_{C21} + \mu}} \leq \frac{1}{\delta_C}$$

$$PA_S \approx 1 - \frac{\delta_C}{\mu_C} - \frac{2\lambda}{2\lambda + \delta_{C21} + \mu} \left(\frac{\lambda}{\mu} + \frac{\delta_{C21}}{\mu_C} - \frac{\delta_C}{\mu_C} \right)$$

$$MTTF_{S0} = \frac{1}{\delta_C + \frac{2\lambda(\lambda + \delta_{C23} - \delta_C)}{3\lambda + \delta_{C23} + \mu}} \leq \frac{1}{\delta_C}$$

$$PA_S \approx 1 - \frac{\delta_C}{\mu_C} - \frac{2\lambda}{2\lambda + \mu} \left(\frac{\lambda}{\mu} + \frac{\delta_{C23}}{\mu_{C32}} - \frac{\delta_C}{\mu_C} \right)$$

a) Common cause failures (C) only on working elements, repair for C can include that for a failure

b) C only on working elements, repair priority on C and without inclusion of other failures

$$MTTF_{S0} = \frac{1}{\delta_C + \frac{2\lambda(\lambda + \delta_{C21} - \delta_C)}{3\lambda + \delta_{C21} + \mu}} \leq \frac{1}{\delta_C}$$

$$PA_S \approx 1 - \frac{\delta_C}{\mu_C} - \frac{2\lambda}{2\lambda + \delta_{C21} + \mu} \left(\frac{\lambda}{\mu} + \frac{\delta_{C21}}{\mu_C} - \frac{\delta_C}{\mu_C} + \frac{\lambda \delta_{C41}}{\mu \mu_C} \right)$$

$$MTTF_{S0} = \frac{1}{\delta_C + \frac{2\lambda(\lambda + \delta_{C23} - \delta_C)}{3\lambda + \delta_{C23} + \mu}} \leq \frac{1}{\delta_C}$$

$$PA_S \approx 1 - \frac{\delta_C}{\mu_C} - \frac{2\lambda}{2\lambda + \mu} \left(\frac{\lambda}{\mu} + \frac{\delta_{C23}}{\mu_{C32}} - \frac{\delta_C}{\mu_C} + \frac{\lambda \delta_{C45}}{\mu \mu_{C54}} \right)$$

c) C on elements in working or repair state, repair for C can include that for other failures

d) C on elements in working or repair state, repair as for case b)

Often $\delta_{C21} = \delta_{C23} = \delta_{C41} = \delta_{C45} = \delta_C$ & $\mu_{C32} = \mu_{C54} = \mu_C$ can be assumed. Case b) corresponds then to a 1-out-of-2 active redundancy in series with a switch (Eqs. (6.157), (6.159)). Further approximations are possible, e.g. using $1 - PA_S = \overline{PA_S} = P_1 + P_3 + P_4 + P_5$.

Equations (6.276) - (6.280) clearly show the effect (consequence) of common cause failures on a 1-out-of-2 active redundancy:

The common cause failure acts as a series element with failure rate equal the occurrence rate δ_C of the common cause failure and repair (restoration) rate μ_C equal the removal rate of the common cause failure; it becomes negligible for $\delta_C \ll 2\lambda^2 / \mu$ (Eq. (6.280), see also Fig. 6.17).^{)}*

The above rule can be extended to cover situations in which the common cause failure acts on all redundant elements of a redundant structure. From this:

Good protection against common cause failures can only be given if each element of a redundant structure is realized with different technology (materials & tools), electrically, mechanically and thermally separated, and not designed by the same designer (true also for common faults in software).

Concrete protection against common cause failures must be worked out on a *case-by-case basis*. In verifying such a protection, an FMEA/FMECA is mandatory for hardware and software. In some applications, common cause failures can occur with a time delay on elements of a redundant structure (e.g. drop of a cooling ventilator); in this cases, *automatic fault detection can avoid secondary failures*. Some practical considerations on failure rates for common cause failures in electronic equipment are in [A2.6 (61508-6)], giving $\delta_C / \lambda \approx 0.005$ as achievable value (see rule (6.174)).

^{*)} Situation similar to that of imperfect switch with no connection (Eqs. (6.238), (6.239)).

6.8.8 Basic Considerations on Network Reliability

A network (telecommunication, power, neuronal, or other) can often be regarded, for modeling purposes, as a graph with N nodes and up to $\binom{N}{2}$ edges (or links). Edges can be directed or bi-directional. Nodes and/or edges can fail and can have two or more states. Furthermore, for reliability investigations, distinction is made between 2-terminal and k -terminal ($2 < k \leq N$) connections. Networks can thus have very complex (meshed) reliability structures, some of which have been investigated since the 1950s, with increasing interest in the last years, see e. g. [2.32, 6.51-6.70].

For the case of only two states for nodes and edges, small networks can be investigated with methods introduced in Sections 2.3.1 - 2.3.3 (nonrepairable) or 6.2 - 6.8.7 (repairable). For large networks, solutions using minimal path or cut sets, i. e. based on Boolean functions (Section 2.3.4), are possible, manually, using binary decision diagrams (Section 6.9.3), or with help of dedicated computer programs, see e.g. [6.53 (2007, 2009), 6.56, 6.58, 6.59]. Multi-states for nodes and/or edges have to be considered when dealing with capacity problems, and some results for 2-terminal networks are known, see e. g. [6.53 (2009), 6.56-6.60, 6.64].

In the following, two basic network structures are investigated using the *key item method* given in Section 2.3.1 (see also Points 7 & 8 of Table 2.1 for further examples).

Figure 6.37a shows a network with 3 nodes N_1, N_2, N_3 and 3 bi-directional edges E_{12}, E_{13}, E_{23} . The reliability block diagram (RBD) for connection N_1, N_2 is given in Fig. 6.37b if only edges can fail and in Fig. 6.37c if nodes and edges can fail. The reliability function (nonrepairable) related to Fig. 6.37c follows as for Eq. (2.26)

$$R_{S0_{N_1, N_2}} = R_{N_1} R_{N_2} [R_{E_{12}} + R_{E_{13}} R_{E_{23}} R_{N_3} - R_{E_{12}} R_{E_{13}} R_{E_{23}} R_{N_3}], \tag{6.281}$$

with $R_{S0_{N_1, N_2}} = R_{S0_{N_1, N_2}}(t)$, $R_i = R_i(t)$, $R_i(0) = 1$. Figure 6.37d gives the RBD for *all-terminal*. For this case, all nodes are in series and $\{(N_1, N_2) \cap (N_1, N_3) \cap (N_2, N_3)\} = \{(N_1, N_2) \cap (N_1, N_3)\}$ is used. The reliability function (nonrepairable case) can be computed using e.g. E_{12} as *key item* (Eq. (2.29)), yielding

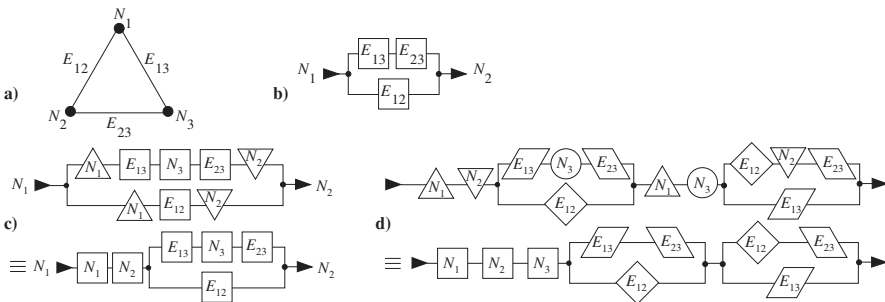


Figure 6.37 a) Network with 3 nodes & bi-directional connection from each node to each other node; b) 2-terminal RBD for connection N_1, N_2 , nodes 100% reliable; c) 2-terminal RBD for connection N_1, N_2 , edges and nodes can fail; d) RBD for all-terminal reliability, edges and nodes can fail

$$R_{S0\ all} = R_{N_1}R_{N_2}R_{N_3} [R_{E_{12}}(R_{E_{13}}+R_{E_{23}}-R_{E_{13}}R_{E_{23}}) + \bar{R}_{E_{12}}R_{E_{13}}R_{E_{23}}], \quad (6.282)$$

with $\bar{R}_i=1-R_i$, $R_{S0\ all}=R_{S0\ all}(t)$, $R_i=R_i(t)$, $R_i(0)=1$. Considering Eq. (2.48), $PA_i(t)$ instead of $R_i(t)$ in Eqs. (6.281) & (6.282) leads to the point availability $PA_{S0}(t)$ for the case of *totally independent elements* $N_1, N_2, N_3, E_{12}, E_{13}, E_{23}$ (p.52). To compute the reliability for the repairable case or the point availability for non totally independent elements, the states space method introduced above in this chapter can be used.

Figure 6.38a shows a network with 4 nodes N_1, N_2, N_3, N_4 and 6 bi-directional edges $E_{12}, E_{13}, E_{14}, E_{23}, E_{24}, E_{34}$. Assuming that nodes and edges can fail, the reliability block diagram is given in Fig. 6.37b for connection N_1, N_2 and Fig. 6.38c for all-terminal. Successively use of the *key item method* (on E_{12}, E_{34}, N_3, N_4) yields

$$R_{S0\ N_1, N_2} = R_{N_1}R_{N_2} [R_{E_{12}} + \bar{R}_{E_{12}} \{ R_{E_{34}} [R_{N_3} \{ R_{N_4} (R_{E_{13}} + R_{E_{14}} - R_{E_{13}}R_{E_{14}}) (R_{E_{23}} + R_{E_{24}} - R_{E_{23}}R_{E_{24}}) + \bar{R}_{N_4}R_{E_{13}}R_{E_{23}} \} + \bar{R}_{N_3}R_{N_4}R_{E_{14}}R_{E_{24}} \} + \bar{R}_{E_{34}} (R_{N_3}R_{E_{13}}R_{E_{23}} + R_{N_4}R_{E_{14}}R_{E_{24}} - R_{N_3}R_{E_{13}}R_{E_{23}}R_{N_4}R_{E_{14}}R_{E_{24}}) \}], \quad (6.283)$$

Similarly, Fig. 6.38c leads to (*key item method* on $E_{12}, E_{13}, E_{14}, E_{24}$)

$$R_{S0\ all} = R_{N_1}R_{N_2}R_{N_3}R_{N_4} [R_{12} \{ R_{13} [1 - (1 - R_{14})(1 - R_{24})(1 - R_{34})] + \bar{R}_{13} [R_{14} (R_{23} + R_{34} - R_{23}R_{34}) + \bar{R}_{14}R_b] \} + \bar{R}_{12} \{ R_{13} [R_{14} (R_{23} + R_{24} - R_{23}R_{24}) + \bar{R}_{14}R_b] + \bar{R}_{13}R_{14}R_b \}], \quad (6.284)$$

with $R_b = R_{24}(R_{23} + R_{34} - R_{23}R_{34}) + \bar{R}_{24}R_{23}R_{34}$; from this, $R_{S0\ all} = R_N^4 [16R^3 - 33R^4 + 24R^5 - 6R^6]$ for $R_{N_i} = R_N, R_{E_{ij}} = R$ (see also the remark to Eq. (6.282) for the repairable case).

Besides deterministic networks, some kinds of stochastic and evolving networks have been investigated, for instance by assuming that for bi-directional edges, every pair of nodes has a probability p to be connected (Erdős-Renyi) or there is a probability $p(k)$ that a randomly selected node has k edges ($p(k)$ can be a Poisson distribution (Erdős-Renyi) or a given power law), see e.g. [6.51-6.55] for greater details. However, because of their complexity, investigation of networks is still in progress.

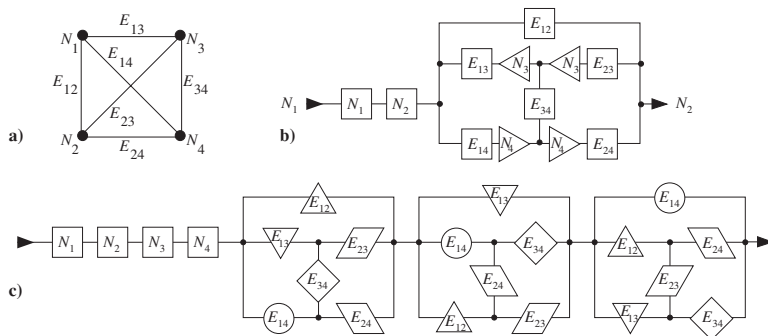


Figure 6.38 a) Network with 4 nodes & bi-directional connection from each node to each other node; b) 2-terminal RBD for nodes N_1 & N_2 , edges and nodes can fail, c) RBD for all-terminal reliability, edges and nodes can fail (RBD= reliability block diagram)

6.8.9 General Procedure for Modeling Complex Systems

On the basis of the tools introduced in Appendix A7 and results in Sections 6.8.1-6.8.8, following procedure can be given for reliability and availability investigation of complex systems, both when a reliability block diagram exists or not (for series-parallel structures, Section 6.7 applies, in particular Table 6.10, p. 233).

1. As a first step operate with time-homogeneous *Markov processes*, i.e., assume that *failure and repair rates of all elements are constant* during the stay time in every state, and can change (stepwise) only at state changes, e.g. because of change in configuration, component use, stress, repair strategy or other (dropping this assumption leads to *non-Markovian* processes, as shown e.g. in Section 6.4.2, pp. 204-207). In a further step, refinements can be considered on a *case-by-case basis* using more complex regenerative processes.
2. Group series elements and assign to each macro-structure E_1, \dots, E_n a failure rate $\lambda_S = \lambda_1 + \dots + \lambda_n$ and repair (restoration) rate $\mu_S = \lambda_S / (\lambda_1 / \mu_1 + \dots + \lambda_n / \mu_n)$ (Table 6.10). A further *reduction of a diagram of transition rates* is possible in some cases (see e.g. [6.32, 6.40], p. 229, Figs. 6.27 & 6.28, 6.30, 6.39).
3. Perform an FMEA (Section 2.6) to fix all relevant *failure modes* and to verify actual system capability for *detection, localization, reconfiguration, graceful degradation* at failure, and protection against *common cause/mode failures*.
4. Draw the *diagram of transition rates* and verify its correctness (see Fig. 6.20, p. 235 & Fig. 6.34, p. 267 for two comprehensive examples); important is the identification of up states which have a direct transition to a down state at system level (e.g. $Z_1, Z_3 - Z_7$ in Fig. 6.20), i.e. of *critical operating states*.
5. Identify the transition rates between each state (combination of failure and repair rates), by considering assumed repair (restoration) priorities, retained failure modes, and particularities specific to the system considered (dependence between elements, sequence of failure or failure modes, etc.).
6. For reliability calculation, the *mean time to system failure* $MTTF_{S_i}$ for system entering state Z_i at $t = 0$ is obtained by solving (Eq. (A7.126))

$$\rho_i MTTF_{S_i} = 1 + \sum_{Z_j \in U, j \neq i} \rho_{ij} MTTF_{S_j}, \quad Z_i \in U, \quad \rho_i = \sum_{j=0, j \neq i}^m \rho_{ij}. \quad (6.285)$$

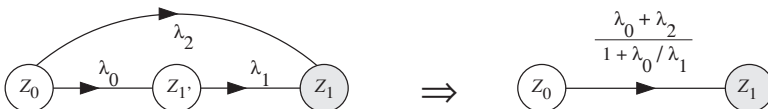


Figure 6.39 Example for a reduction of a diagram of transition rates for $MTTF_{S_0}$ calculation (note that $(\lambda_0 + \lambda_2) / (1 + \lambda_0 / \lambda_1) = (1 + \lambda_2 / \lambda_0) / (1 / \lambda_0 + 1 / \lambda_1)$)

Thereby, U is the set of *up states*, \bar{U} the set of *down states* ($U \cup \bar{U} = \{Z_0, \dots, Z_m\}$), ρ_{ij} the transition rate from state $Z_i \in U$ to state $Z_j \in U$, and ρ_i the *sum of all transition rates leaving state Z_i* (Table 6.2). The system of algebraic equations (6.285) delivers all $MTTF_{S_i}$ for any $Z_i \in U$ entered at $t=0$ (note that for Markov processes, the condition " Z_i is entered at $t=0$ " can be replaced by "system in Z_i at $t=0$ "). At system level,

$$R_{S0}(t) \approx e^{-t/MTTF_{S0}} \tag{6.286}$$

can often be used (in Z_0 all elements are operating or ready to operate, i. e., as-good-as-new because of the *memoryless* Markov property).

7. The *asymptotic* ($t \rightarrow \infty$) & *steady-state (stationary) point and average availability* $PA_S = AA_S$ is given as (Eq. (A7.134))

$$PA_S = AA_S = \sum_{Z_j \in U} P_j \tag{6.287}$$

with P_j as solution of (Eq. (A7.127), for irreducible embedded Markov chain)

$$\rho_j P_j = \sum_{i=0, i \neq j}^m P_i \rho_{ij}, \quad \text{with } P_j > 0, \sum_{j=0}^m P_j = 1, \rho_j = \sum_{i=0, i \neq j}^m \rho_{ji}, \quad j=0, \dots, m. \tag{6.288}$$

One equation for P_j , arbitrarily chosen, must be replaced by $\sum P_j = 1$. Equation (6.288) states that *in steady-state, the probability to live Z_j is equal to the probability to come to Z_j* . For further availability figures see pp. 180-182.

8. Considering the constant failure rate for all elements, the asymptotic & steady-state *interval reliability* follows as (Eq. (6.27))

$$IR_S(t, t + \theta) \approx PA_S e^{-\theta/MTTF_{S0}} = \left(\sum_{Z_j \in U} P_j \right) e^{-\theta/MTTF_{S0}}. \tag{6.289}$$

9. The asymptotic & steady-state *system failure frequency* f_{udS} and *system mean (expected) up time* MUT_S are given as (Eqs. (A7.141) & (A7.142))

$$f_{udS} = \sum_{Z_j \in U, Z_i \in \bar{U}} P_j \rho_{ji} = \sum_{Z_j \in U} P_j \left(\sum_{Z_i \in \bar{U}} \rho_{ji} \right) \tag{6.290}$$

and

$$MUT_S = PA_S / f_{udS}, \tag{6.291}$$

respectively. U is the set of states considered as *up states for f_{udS} and MUT_S calculation*, \bar{U} the complement to the totality of states considered. The same is for the *system repair (restoration) frequency* f_{duS} and the *system mean (expected) down time* MDT_S , given as (Eqs. (A7.143) & (A7.144))

$$f_{duS} = \sum_{Z_i \in \bar{U}, Z_j \in U} P_i \rho_{ij} = \sum_{Z_i \in \bar{U}} P_i \left(\sum_{Z_j \in U} \rho_{ij} \right) \tag{6.292}$$

and

$$MDT_S = (1 - PA_S) / f_{duS}, \tag{6.293}$$

respectively. MUT_S is the mean of the time in which the system is moving in the set of up states $Z_j \in U$ before a transition in the set of down states $Z_i \in \bar{U}$ occurs, in steady-state or for $t \rightarrow \infty$. MDT_S is the mean repair (restoration) time at system level. f_{udS} is the *system failure intensity* $z_S(t)$ (Eq.(A7.230), in steady-state or for $t \rightarrow \infty$. It is not difficult to recognize that one has

$$f_{udS} = f_{duS} = z_S = 1 / (MUT_S + MDT_S), \tag{6.294}$$

see Example 6.29 for a practical application. Equations (6.291), (6.293), (6.294) lead to the following important relation

$$MDT_S = MUT_S (1 - PA_S) / PA_S \quad (\text{as per } PA_S = MUT_S / (MUT_S + MDT_S)). \tag{6.295}$$

$MUT_S \cong MTTFS_0$ can often be used in practical applications; however, $\sum_{Z_j \in U} P_j MTTFS_j$ can not be used for MUT_S (see the remark on p. 500).

10. The asymptotic & steady-state *mean* (expected) *reward rate* MIR_S is given by (Eq. (A7.147))

$$MIR_S = \sum_{i=0}^m r_i P_i. \tag{6.296}$$

Thereby, $r_i = 0$ for down states, $0 < r_i < 1$ for partially down states, and $r_i = 1$ for up states with 100% performance. The asymptotic & steady-state *mean* (expected) *accumulated reward* MAR_S follows as (Eq. (A7.148))

$$MAR_S(t) = MIR_S \cdot t. \tag{6.297}$$

If the process involved is non-Markovian, it can be useful to operate with a time schedule (see e. g. Figs. 6.10 & A7.11), and the above steps have to be changed, as necessary. Alternative investigation methods are introduced in Section 6.9. *Failure-free time* means *failure-free operating time* and *repair* is used as a synonym for *restoration*.

Example 6.29

Investigate MUT_S , MDT_S , f_{udS} , and f_{duS} for the 1-out-of-2 redundancy of Fig. 6.8a.

Solution

The solution of Eq. (6.84) with $\dot{P}_i(t) = 0$, $i = 0, 1, 2$, yields (Eq. (6.87))

$$P_0 = \mu^2 / [(\lambda + \lambda_r)(\lambda + \mu) + \mu^2] \quad \text{and} \quad P_1 = \mu(\lambda + \lambda_r) / [(\lambda + \lambda_r)(\lambda + \mu) + \mu^2].$$

From Fig. 6.8a and Eqs. (6.290) & (6.291) it follows that (see also Eq. (6.95) for MUT_S)

$$MUT_S = \frac{\lambda + \lambda_r + \mu}{\lambda(\lambda + \lambda_r)}, \quad MDT_S = \frac{1}{\mu}, \quad f_{udS} = f_{duS} = \frac{1}{MUT_S + MDT_S} = \frac{\mu\lambda(\lambda + \lambda_r)}{(\lambda + \lambda_r)(\lambda + \mu) + \mu^2}.$$

For this example it holds that $MUT_S = MTTFS_1$ (with $MTTFS_1$ from Eq.(6.285) or, from Eq. (6.89) with $P_1'(0) = 1$, see also Eq. (A7.154)); this is because the system enters state Z_1 after each system failure. Furthermore, because of the return from the down state Z_2 to the up state Z_1 as in Fig. 6.8a it holds that $MDT_S = 1/\mu = MTTR$ (follow also from the memoryless property of the time-homogeneous Markov process and Fig. 6.8a).

6.9 Alternative Investigation Methods

The methods given in sections 6.1 to 6.8 are based on Markov, semi-Markov and semi-regenerative processes, according to the involved distributions for failure-free and repair times. They have the advantage of great flexibility (arbitrary redundancy and repair strategy, incomplete coverage or switch, common cause failures, etc.) and transparency. Further tools are known to model repairable systems, e. g. based on dynamic fault trees or Petri nets. For very large or complex systems, numerical solution or Monte Carlo simulation can become necessary. Many of these tools are similar in performance and versatility (Petri nets are equivalent to Markov models), other have limitations (fault tree analyses are basically limited to totally independent elements and Monte Carlo simulations delivers only numerical solutions), so that choice of the tool is often related to the personal experience of the analyst (see e. g. [A2.6 (61165, 60300-3-1), 6.30, 6.39 (2005)] for comparisons). However,

modeling large complex systems requires a close cooperation between project and reliability engineers.

After a recall for systems with totally independent elements, Sections 6.9.2 to 6.9.5 introduce dynamic fault trees, BDD, event trees and Petri nets. Sections 6.9.6 & 6.9.7 consider numerical solutions & approximate expressions for large complex systems. Human reliability is discussed in Section 6.10.

6.9.1 Systems with Totally Independent Elements

Totally independent elements means that each element operates and, if repairable, is repaired independently of any other element in the system considered. Elements are boxes in a reliability block diagram and, for repairable elements, total independence implies that each element *has its repair crew and continues operation during the repair of a failed element*. This does not imply that the (physically) same element cannot appear more times in a reliability block diagram (Example 2.3). The reliability function $R_{S0}(t)$ of nonrepairable (up to system failure) systems with totally independent elements has been investigated in Chapter 2. As stated with Eq. (2.48), *equation for $R_{S0}(t)$ is also valid for the point availability $PA_{S0}(t)$ of repairable systems, substituting $PA_i(t)$ to $R_i(t)$* . This rule can be used to get an upper bound on $PA_{S0}(t)$ for the case in which each element does not have its repair crew. Basically, the reliability function for repairable systems can not be given using Boolean methods; however, an approximation can be found in some cases (Section 6.9.7).

6.9.2 Static and Dynamic Fault Trees

A fault tree (FT) is a graphical representation of the conditions or other factors causing or contributing to the occurrence of a defined undesirable event, referred as

top event. In its original form, as introduced in Section 2.6 (p. 76), a fault tree contains only static gates (essentially AND and OR for coherent systems) and is thus termed *static fault tree*. Such a fault tree can handle combinatorial events, qualitatively (similar as for an FMEA, Section 2.6) or quantitatively (as with Boolean functions, Section 2.3.4). As in the current literature [2.85, 6.38, A2.6(IEC 61025)], "0" will be used also here for operating and "1" for failure (this in contrast to the notation used in Sections 2.2 & 2.3 for reliability investigations based on the reliability block diagram with 1 for *up* and 0 for *down*). With this notation, OR gates represent in fault trees a *series structure* and AND gates a *parallel structure with active redundancy* (Figs. 2.14, 6.40-6.42). In setting up a fault tree, a reliability block diagram can be useful. However, fault trees can also consider external events. Figure 6.40 gives two examples of reliability structures with corresponding static fault trees (see Table 2.1 and Example 6.30 for computations based on the reliability block diagram, Section 6.9.3 for computations based on binary decision diagrams).

Static fault trees can be used to compute reliability and availability for the case of *totally independent elements* (active redundancy and each element has its own repair crew). Reliability computation for the non-repairable case (up to system failure) using fault tree analysis (FTA) leads to

$$1 - R_{S0}(t) = 1 - \prod_{i=1}^n R_i(t) \quad \text{or} \quad \bar{R}_{S0}(t) = 1 - \prod_{i=1}^n (1 - \bar{R}_i(t)), \quad (6.298)$$

for the *series structure with independent elements*, and to

$$1 - R_{S0}(t) = 1 - \sum_{i=k}^n \binom{n}{i} R^i(t) (1 - R(t))^{n-i} \quad \text{or} \quad \bar{R}_{S0}(t) = 1 - \sum_{i=k}^n \binom{n}{i} (1 - \bar{R}(t))^i \bar{R}(t)^{n-i}, \quad (6.299)$$

for the *k-out-of-n active redundancy with identical and independent elements* (Eqs. (2.17) and (2.23), $\bar{R}_i(t) = 1 - R_i(t) =$ failure probability). For complex structures, computation uses binary decision diagrams (based on the Shannon decomposition of the fault tree structure function, see Section 6.9.3) or minimal path or cut sets (Eqs. (2.42), (2.44)), often supported by computer programs.

However, because of their basic structure, static fault trees can not handle *states or time dependencies* (in particular standby redundancy & repair strategy). For these cases, it is necessary to extend static fault trees, adding so called *dynamic gates* to obtain *dynamic fault trees*. Important dynamic gates are [2.85, 6.38, A2.6(IEC 61025)]:

- Priority AND gate (PAND), the output event (failure) occurs only if all input events occur and in sequence from left to right.
- Sequence enforcing gate (SEQ), the output event occurs only if input events occur in sequence from left to right and there are more than two input events.
- Spare gate (SPARE), the output event occurs if the number of spares is less than required.

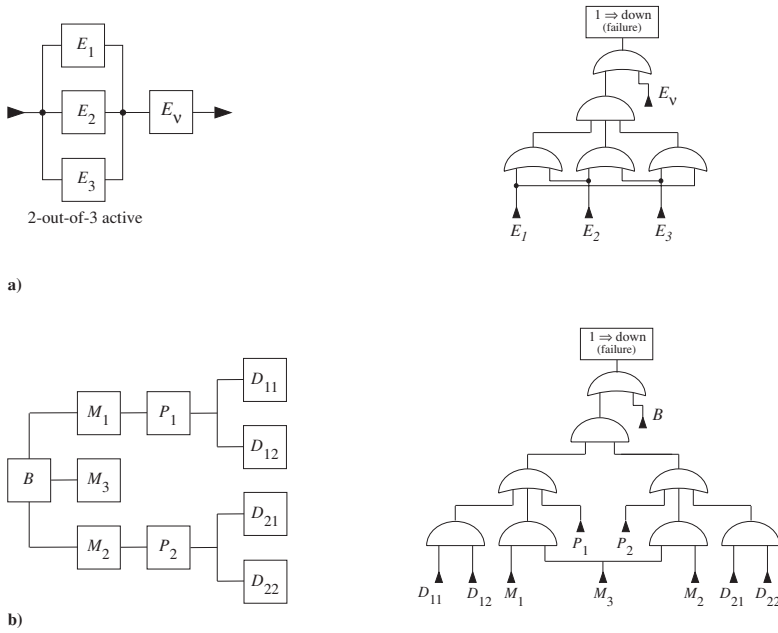


Figure 6.40 a) Reliability block diagram and corresponding static fault tree for a 2-out-of-3 active redundancy with switch element; b) Functional block diagram and corresponding static fault tree for a redundant computer system [6.30]; **Note:** "0" holds for operating (up), "1" for failure (down)

Further gates (choice gate, redundancy gate, warm spare gate) have been suggested, e. g. in [6.38]. All above dynamic gates requires a Markov analysis, i. e., states probabilities must be computed by a Markov approach (constant failures & repair rates), yielding results used as occurrence probability for the basic event replacing the corresponding dynamic gate. Use of dynamic gates in dynamic fault tree analysis, with corresponding computer programs, has been carefully investigated, e. g. in [2.85, 6.36, 6.38].

Fault tree analysis (FTA) is an established methodology for reliability and availability analysis (emerging in the nineteen-sixties with investigations on nuclear power plants). However, the necessity to use Markov approaches to solve dynamic gates can limit its use in practical applications. Moreover, FTA has the same limits as those of methods based on binary considerations (fault trees, reliability block diagrams (RBD), binary decision diagrams (BDD), etc.). However, reliability block diagrams and fault trees are valid support in generating transition rates diagrams for Markov analysis. So once more,

combination of investigation tools is often a good way to solve difficult problems.

6.9.3 Binary Decision Diagrams

A *binary decision diagram* (BDD) is a directed acyclic graph obtained by successive *Shannon decomposition* (Eq. (2.38)) of a *Boolean function*. It applies in particular to the *structure functions* developed in Section 2.3.4 for coherent systems, using *minimal path or cut sets*. This allows for easy computation of the reliability function $R_{S0}(t)$ for the *nonrepairable case* (Eqs.(2.45),(2.47)) or point availability $PA_{S0}(t)$ for *repairable totally independent elements* (Eqs. (2.45), (2.48)). Frequently, BDDs are used to compute $R_{S0}(t)$ or $PA_{S0}(t)$ for systems completely described by a *fault tree* with corresponding *fault tree structure function* $\phi_{FT}(\zeta_1, \dots, \zeta_n)$. $\phi_{FT}(\zeta_1, \dots, \zeta_n)$ follows from a fault tree, see e. g. Figs. 6.41 & 6.42, or from the corresponding reliability block diagram, considering "0" for operating (up) and "1" for failure (down).

In relation to fault trees, a BDD is constructed starting from the *top event*, i.e. from $\phi_{FT}(\zeta_1, \dots, \zeta_n)$, down to the sink boxes using the Shannon decomposition (Eq. (2.38)) of the fault tree structure function at the node considered. Each node refers to a variable of $\phi_{FT}(\zeta_1, \dots, \zeta_n)$ and has 2 outgoing edges, 0-edge for operating and 1-edge for failure. Input to a node can be one or more outgoing edges from other nodes. The BDD terminates in 2 sink boxes labeled 0 for operating (up), 1 for failure (down). Indication 0 or 1 and an arrow help to identify the outgoing edge. Figure 6.41 gives two basic reliability block diagrams with corresponding fault trees, ϕ_{FT} , and BDDs. Also given are the reliability functions for the *nonrepairable case* $R_{S0}(t)$ and $\bar{R}_{S0}(t)$:

To obtain $R_{S0}(t)$, one moves from the top of the BDD following all possible paths down to the sink box "0", taking in a multiplicative way $R_i(t)$ or $\bar{R}_i(t)=1-R_i(t)$ according to the value 0 or 1 assumed by the variable ζ_i considered (similarly for $\bar{R}_{S0}(t)$, for $PA_{S0}(t)$ consider Eq. (2.48) or (2.45)).

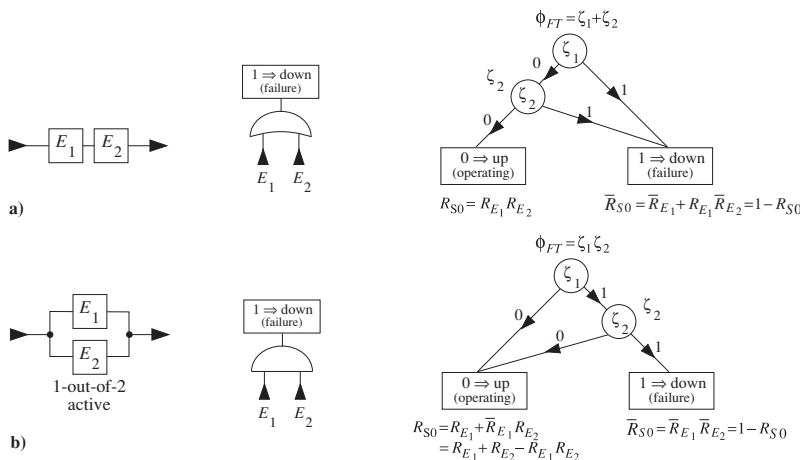


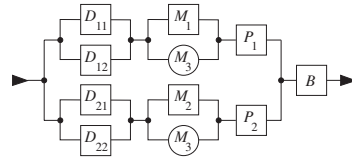
Figure 6.41 Basic reliability block diagrams with corresponding *fault trees*, ϕ_{FT} , & *binary decision diagrams* (ζ_i refers to E_i , "0" operating, "1" failure; $R_{S0} = R_{S0}(t)$, $R_i = R_i(t)$, $R_i(0) = 1$, $\bar{R}_i = 1 - R_i$)

Example 6.30

Give the reliability function $R_{S0}(t)$ for the nonrepairable case and the point availability $PA_{S0}(t)$ for the system of Fig. 6.40b, by assuming totally independent elements and using the reliability block diagram's method with $R_{D_{11}}=R_{D_{12}}=R_{D_{21}}=R_{D_{22}}=R_D$, $R_{M_1}=R_{M_2}=R_M$, $R_{P_1}=R_{P_2}=R_P$, $R_i(t)=R_i$.

Solution

The reliability block diagram follows from the functional block diagram of Fig. 6.40b (Section 2.2.2), or from the corresponding fault tree (Fig. 6.40b, considering "0" for operating (up) and "1" for failure (down)). As element M_3 appears twice in the reliability block diagram, computation of the reliability function (nonrepairable case) make use of the key item method given in Section 2.3.1, yielding



$$R_{S0} = R_{M3} \{ 2 [(2R_D - R_D^2)R_P] - [(2R_D - R_D^2)R_P]^2 \} R_B + (1 - R_{M3}) \{ 2 [(2R_D - R_D^2)R_M R_P] - [(2R_D - R_D^2)R_M R_P]^2 \} R_B, \tag{6.300}$$

with $R_i = R_i(t)$, and $R_i(0) = 1$. Following the assumed total independence of the elements (each of the 10 elements has its own repair crew), the point availability $PA_{S0}(t)$ is also given by Eq. (6.300) substituting R_i with $PA_i(t)$ ($PA_i = AA_i$ for steady-state or $t \rightarrow \infty$).

Figure 6.42 considers the basic structures given in Fig. 6.40. The reliability function $R_{S0}(t)$ for the *nonrepairable case* follows, for the structure of Fig. 6.42b, from

$$R_{S0} = R_B \{ R_{M3} [R_{P1} R_{D11} + R_{P1} \bar{R}_{D11} R_{D12} + R_{P1} \bar{R}_{D11} \bar{R}_{D12} R_{P2} (R_{D21} + \bar{R}_{D21} R_{D22}) + \bar{R}_{P1} R_{P2} (R_{D21} + \bar{R}_{D21} R_{D22})] + \bar{R}_{M3} [R_{M1} R_{M2} R_{P1} (R_{D11} + \bar{R}_{D11} R_{D12}) + R_{M1} R_{M2} R_{P1} \bar{R}_{D11} \bar{R}_{D12} R_{P2} (R_{D21} + \bar{R}_{D21} R_{D22}) + R_{M1} R_{M2} \bar{R}_{P1} R_{P2} (R_{D21} + \bar{R}_{D21} R_{D22}) + R_{M1} \bar{R}_{M2} R_{P1} (R_{D11} + \bar{R}_{D11} R_{D12}) + \bar{R}_{M1} R_{M2} R_{P2} (R_{D21} + \bar{R}_{D21} R_{D22})] \}, \tag{6.301}$$

with $R_{S0} = R_{S0}(t)$, $R_i = R_i(t)$, $R_i(0) = 1$, $\bar{R}_i = 1 - R_i$. Setting $R_{M1} = R_{M2} = R_M$, $R_{P1} = R_{P2} = R_P$, $R_{D11} = R_{D12} = R_{D21} = R_{D22} = R_D$, one obtains Eq. (6.300). Similarly,

$$\bar{R}_{S0} = \bar{R}_B + R_B \{ R_{M3} [(R_{P1} \bar{R}_{D11} \bar{R}_{D12} + \bar{R}_{P1}) (\bar{R}_{P2} + R_{P2} \bar{R}_{D21} \bar{R}_{D22}) + \bar{R}_{M3} [\bar{R}_{M1} \bar{R}_{M2} + R_{M1} R_{M2} (\bar{R}_{P1} + R_{P1} \bar{R}_{D11} \bar{R}_{D12}) (\bar{R}_{P2} + R_{P2} \bar{R}_{D21} \bar{R}_{D22}) + R_{M1} \bar{R}_{M2} (\bar{R}_{P1} + R_{P1} \bar{R}_{D11} \bar{R}_{D12}) + \bar{R}_{M1} R_{M2} (\bar{R}_{P2} + R_{P2} \bar{R}_{D21} \bar{R}_{D22})] \}, \tag{6.302}$$

which verify $1 - \bar{R}_{S0} = R_{S0}$. Assuming totally independent elements (Section 6.9.1), Eq. (6.301) delivers $PA_{S0}(t)$ by substituting R_i with $PA_i(t)$ (or with PA_i for PA_S).

Evaluation of binary decision diagrams (and fault trees) is generally supported by dedicated computer programs, see e.g. [2.32, 2.36, 2.37, 6.63 (2009), 6.66]. For hand evaluation, it is often more favorable to work directly with the *key item method* introduced in Section 2.3.1 (as in Example 6.30).

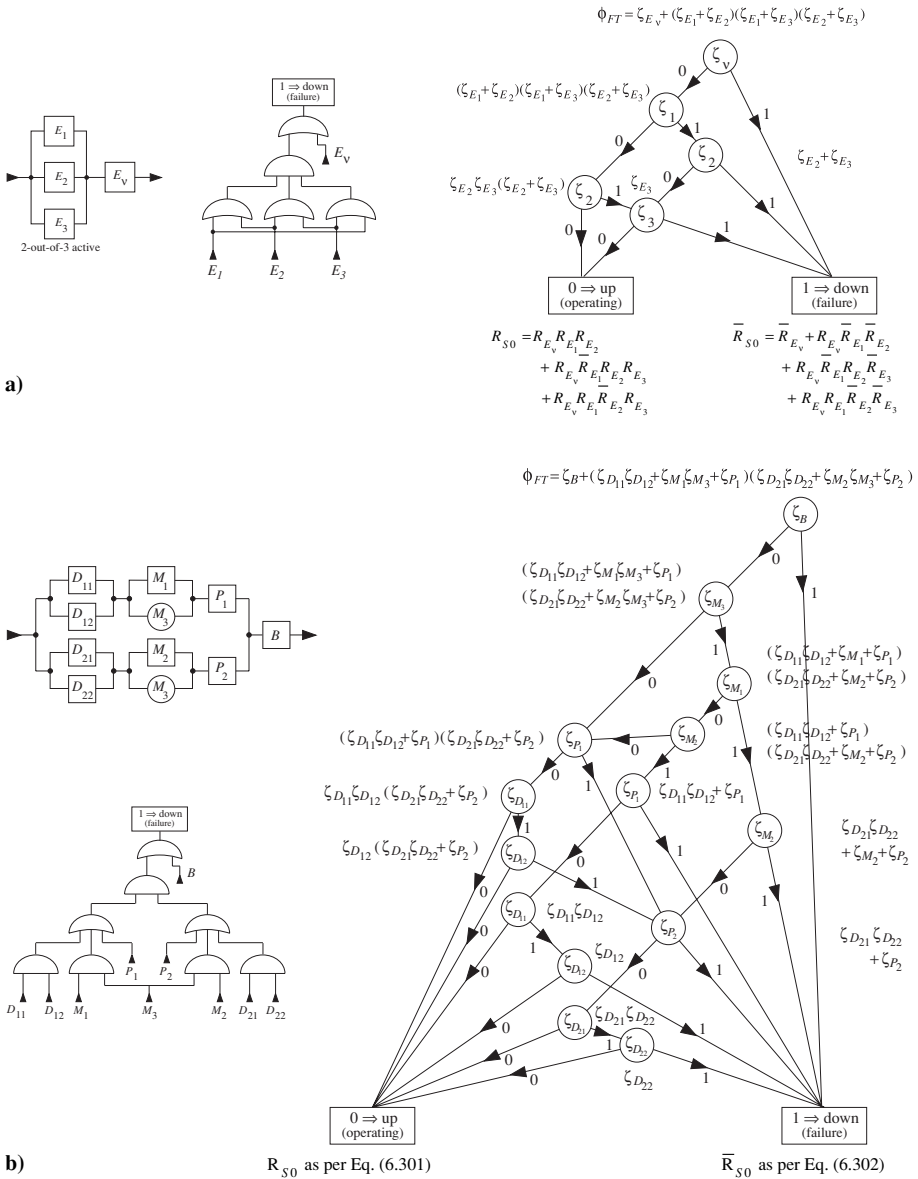


Figure 6.42 Reliability block diagrams with corresponding fault trees, Φ_{FT} , and binary decision diagrams (BDDs) for the 2 structures of Fig. 6.40 (ζ_i refers to E_i ; "0" holds for operating, "1" for failure; $R_{S_0} = R_{S_0}(t)$, $R_i = R_i(t)$, $R_i(0) = 1$, $\bar{R}_i = 1 - R_i$)

To consider "1" for operating (up) and "0" for failure (down), as in Sections 2.2 and 2.3, it is sufficient to change AND with OR and R_i with \bar{R}_i .

6.9.4 Event Trees

Event trees can be used to support and extend effectiveness of failure modes and effects analyses introduced in Section 2.6 [A2.6 (IEC 62502)]. *Event tree analysis* (ETA) is a bottom-up (inductive) logic procedure combining advantages of FMEA/FMECA and FTA. It applies, in particular, for risk analysis of large complex systems of any type with interacting internal and external factors (technical, environmental, human). The basic idea is to give an answer to the question

What happens if a given initiating event occurs?

The answer is given by investigating *propagation of initiating events*, in particular efficacy of mitigations (barriers) introduced to limit effects of the initiating event considered (column 8 in Table 2.6). An initiating event can be a fault or an external event (e. g. loss of power, fire, sabotage). A comprehensive list of initiating events must be prepared at the begin of the analysis.

Figure 6.43 shows the basic structure of an event tree for the case of two coupled systems (*A* and *B*), each with two mitigating factors (barriers) δ_i for the initiating event α considered. Each mitigation is successful with $\Pr\{\delta_i\}$ and unsuccessful (failure) with $\Pr\{\bar{\delta}_i\} = 1 - \Pr\{\delta_i\}$. The probability for the outcome ω in Fig. 6.43 is computed following the path leading to ω and is given by (Eq. (A6.12))

$$\Pr\{\omega\} = \Pr\{\alpha \cap \delta_{A1} \cap \delta_{A2} \cap \bar{\delta}_{B1} \cap \delta_{B2}\} = \Pr\{\alpha\} \Pr\{\delta_{A1} \mid \alpha\} \Pr\{\delta_{A2} \mid (\alpha \cap \delta_{A1})\} \Pr\{\bar{\delta}_{B1} \mid (\alpha \cap \delta_{A1} \cap \delta_{A2})\} \Pr\{\delta_{B2} \mid (\alpha \cap \delta_{A1} \cap \delta_{A2} \cap \bar{\delta}_{B1})\}. \quad (6.303)$$

Computation of conditional probabilities can be laborious. Substituting λ_α to $\Pr\{\alpha\}$, Eq. (6.303) delivers the failure rate (occurrence frequency) of the outcoming event ω .

As for FMEA/FMECA & FTA, time evolution can not be easily considered in ETA. An extension like for dynamic FT (Section 6.9.2) is possible. In particular, $\Pr\{\delta_i\}$ can be issued from the top event of an FT, allowing handling of *common cause events*.

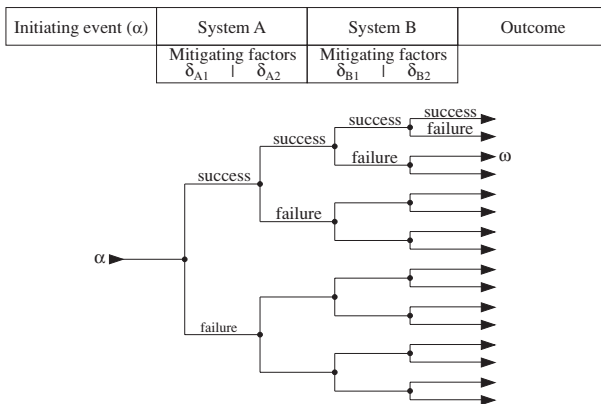


Figure 6.43 Basic structure of an event tree

6.9.5 Petri Nets

Petri nets (PN) were introduced 1962 [6.35, 6.6] to investigate in particular synchronization, sequentiality, concurrency, and conflict in parallel working digital systems. They are well established in the literature, see e. g. [2.40, 6.0, 6.6, 6.8, 6.30, 6.39 (1999), A2.6 (IEC 62551)]. Important for reliability investigations was the possibility to create algorithmically the diagram of transition rates belonging to a given Petri net. With this, investigation of time behavior on the basis of *time-homogeneous Markov processes* was open (stochastic Petri nets). Extension to semi-Markov process is easy [6.8]. This section introduces Petri nets from a reliability analysis point of view.

A Petri net (PN) is a directed graph involving 3 kind of elements:

- *Places* P_1, \dots, P_n (drawn as circles): A place P_i is an *input* to a transition T_j if an arc exist from P_i to T_j and is an *output* of a transition T_k and input to a place P_l if an arc exist from T_k to P_l ; places may contain *token* (black spots) and a PN with token is a *marked* PN.
- *Transitions* T_1, \dots, T_m (drawn as empty rectangles for timed transitions or bars for immediate transitions): A transition *can fire*, taking one token from each input place and putting one token in each output place.
- *Directed arcs*: An arc connects a place with a transition or vice versa and has an arrowhead to indicate the direction; multiple arcs are possible and indicate that by firing of the involved transition a corresponding number of tokens is taken from the involved input place (for input multiple arc) or put in the involved output place (for output multiple arc); inhibitor arcs with a circle instead of the arrowhead are also possible and indicate that for firing condition no token must be contained in the corresponding place.

Firing rules for a transition are:

1. A transition is enabled (can fire) only if all places with an input arc to the given transition contain at least one token (no token for inhibitor arcs).
2. Only one transition can fire at a given time; the selection occurs according to the embedded Markov chain describing the stochastic behavior of the PN.
3. Firing of a transition can be immediate or occurs after a time interval $\tau_{ij} > 0$ (timed PN); $\tau_{ij} > 0$ is in general a random variable (stochastic PN) with distribution function $F_{ij}(x)$ when firing occurs from transition T_i to place P_j (yielding a Markov process for $F_{ij}(x) = 1 - e^{-\lambda_{ij}x}$, i. e. with transition rate λ_{ij} , or a semi-Markov process for $F_{ij}(x)$ arbitrary, with $F_{ij}(0) = 0$).

From rule 3, practically only Markov processes (i. e. constant failure and repair rates) will occur in Petri nets for reliability applications (Section 6.4.2). Two further concepts useful when dealing with Petri nets are those of *marking* and *reachability*:

- A *marking* $M = \{m_1, \dots, m_n\}$ gives the number m_i of token in the place P_i at a given time point and defines thus the *state* of the PN.
- M_j is immediately *reachable* from M_i , if M_j can be obtained by firing a transition enabled by M_i .

With M_0 as marking at time $t=0$, M_1, \dots, M_k are all the (different) marking reachable from M_0 ; they define the PN states and give the *reachability tree*, from which, the diagram of transition rates of the corresponding Markov model follows. Figure 6.44 gives some examples of reliability structures with corresponding PN.

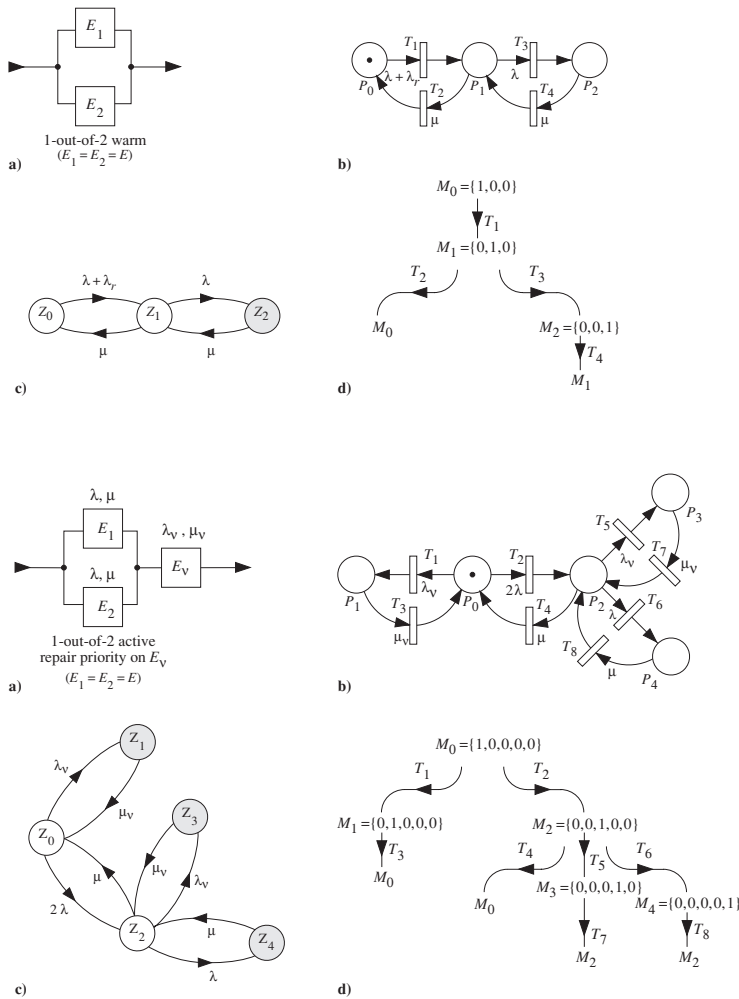


Figure 6.44 Top: Reliability block diagram (a), diagram of transition rates (c), Petri net (PN) (b), and reachability tree (d) for a *repairable 1-out-of-2 warm redundancy with two identical elements, const. failure & repair rates (λ, λ_r, μ), one repair (restoration) crew (Z_2 down state, Markov proc.)*
Bottom: Reliability block diagram (a), diagram of transition rates (c), Petri net (b), and reachability tree (d) for a *repairable 1-out-of-2 active redundancy with two identical elements and switch in series, constant failure and repair rates ($\lambda, \lambda_v, \mu, \mu_v$), one repair crew, repair priority on switch, no further failures at system down (Z_1, Z_3, Z_4 down states, Markov process)*

6.9.6 Numerical Reliability and Availability Computation

Investigation of large series - parallel structures or of *complex systems* (for which a reliability block diagram does not exist) is in general time-consuming and can become mathematically intractable. A large number of computer programs for numerical solution of reliability and availability equations as well as for Monte Carlo simulation have been developed. Such a numerical computation can be, in some cases, the only way to get results. However, although appealing, numerical solutions can deliver only *case-by-case* solutions and can cause problems (instabilities in the presence of sparse matrices, prohibitive run times for Monte Carlo simulation of rare events or if confidence limits are required). As a general rule, analytically exact solutions (Sections 6.2 to 6-6, 6.8) or approximate expressions (Sections 6.7, 6.9.7) should be preferred whenever possible.

Section 6.9.6.1 discusses requirements for a versatile program for the numerical solution of reliability & availability equations. Section 6.9.6.2 gives basic considerations on Monte Carlo simulation and introduces an approach useful for rare events.

6.9.6.1 Numerical Computation of System's Reliability and Availability

Analytical solution of algebraic or differential / integral equations for reliability and availability computation of large or complex systems can become time-consuming. Software tools exist to solve this kind of problems. From such a software package one generally expects high *completeness, usability, robustness, integrity, and portability* (Table 5.4). The following is a comprehensive list of requirements:

General requirements:

1. Support interface with CAD/CAE and *configuration management* packages.
2. Provide a large component data bank with the possibility for manufacturer and company-specific labeling, and storage of non application-specific data.
3. Support different failure rate models [2.20 - 2.30].
4. Have flexible output (regarding medium, sorting capability, weighting), graphic interface, single & multi-user capability, high usability & integrity.
5. Be portable to different platforms.

Specific for nonrepairable (up to system failure) systems:

1. Consider reliability block diagrams (RBD) of *arbitrary complexity* and with a large number of elements ($\geq 1,000$) and levels (≥ 10); possibility for any element to appear more than once in the RBD; automatic editing of series and parallel models; powerful algorithms to handle complex structures; constant or time dependent failure rate for each element; possibility to handle as element macro-structures or items with more than one failure mode.
2. Easy editing of *application-specific* data, with user features such as:
 - automatic computation of the ambient temperature at component level with freely selectable temperature difference between elements,

- freely selectable duty cycle from the system level downwards,
 - global change of environmental and quality factors, manual selection of stress factors for tradeoff studies or risk assessment, manual introduction of field data and of *default values* for component families or assemblies.
3. Allow reuse of elements with arbitrary complexity in a RBD (libraries).

Specific for repairable systems:

1. Consider elements with *constant failure rate* and constant or *arbitrary repair rate*, i.e., handle Markov and (as far as possible) semi-regenerative processes.
2. Have *automatic* generation of the transition rates ρ_{ij} for Markov model and of the involved semi Markov transition probabilities $Q_{ij}(x)$ for systems with constant failure rates, one repair crew, and arbitrary repair rate (starting e.g. from a given set of *successful paths*); automatic generation and solution of the equations describing the system's behavior.
3. Allow *different repair strategies* (first-in first-out, one repair crew or other).
4. Use sophisticated algorithms for quick inversion of *sparse matrices*.
5. Consider at least 20,000 states for the *exact solution* of the *asymptotic & steady-state* availability $PA_S = AA_S$ and mean time to system failure $MTTF_{Si}$.
6. Support investigations yielding approximate expressions (macro-structures, totally independent elements, cutting states or other, see Section 6.7.1).

A scientific software package satisfying many of the above requirements has been developed at the Reliability Lab. of the ETH [2.50]. Refinement of the requirements is possible. For basic reliability computation, commercial programs are available [2.50-2.60]. Specialized programs are e. g. in [2.6, 2.18, 2.59, 2.85, 6.23, 6.24, 6.43]; considerations on numerical methods for reliability evaluation are e.g. in [2.56].

6.9.6.2 Monte Carlo Simulations

The Monte Carlo technique is a numerical method based on a probabilistic interpretation of quantities obtained from algorithmically generated random variables. It was introduced 1949 by N. Metropolis and S. Ulman [6.31]. Since this time, a large amount of literature has been published, see e.g. [6.4, 6.13, A7.18]. This section deals with some basic considerations on Monte Carlo simulation useful for reliability analysis and gives an approach for the simulation of rare events which avoids the difficulty of time truncation because of amplitude quantization of the digital numbers used.

For reliability purposes, a Monte Carlo simulation can basically be used to estimate a value (e. g. an unknown probability) or simulate (reproduce) the stochastic process describing the behavior of a complex system. In this sense, a Monte Carlo simulation is useful to achieve results, numerically verify an analytical solution, get an idea of the possible time behavior of a complex system or determine interaction among variables. Two main problems related to Monte Carlo simulation

are the generation of uniformly distributed *random numbers* ($\zeta_0, \zeta_1, \dots, \zeta_{2^n-1}$ with $p_i = 1/2^n$) in the interval $[0,1)$ and the transformation of these numbers in random variables with prescribed distribution functions. A congruential relation

$$\zeta_{n+1} = (a\zeta_n + b) \pmod m, \tag{6.304}$$

where *mod* is used for *modulo*, is frequently used to generate *pseudorandom numbers* [6.29] (for simplicity, *pseudo* will be omitted in the following). Transformation to an arbitrary distribution function $F(x)$ is often performed with help of the inverse function $F^{-1}(x)$, see Example A6.18 on p. 448. The method of the inverse function is simple but not necessarily good enough for critical applications.

A further question arising with Monte Carlo simulation is that of how many repetitions n must be run to have an estimate of the unknown quantity within a given interval $\pm \epsilon$ at a given confidence level γ . For the case of an event with probability p and assuming n sufficiently large as well as p or $(1-p)$ not very small ($\min(np, n(1-p)) \geq 5$), Eq. (A6.152) yields for p known

$$n = \left(\frac{t_{(1+\gamma)/2}}{\epsilon}\right)^2 p(1-p) \quad \text{i.e.} \quad n_{\max} = \left(\frac{t_{(1+\gamma)/2}}{2\epsilon}\right)^2 \quad \text{for } p = 0.5, \tag{6.305}$$

where $t_{(1+\gamma)/2}$ is the $(1+\gamma)/2$ quantile of the standard normal distribution; for instance, $t_{(1+\gamma)/2} = 1.645$ for $\gamma = 0.9$ and 1.96 for $\gamma = 0.95$ (Appendix A9.1). For p totally unknown, the value $p = 0.5$ has to be taken. Knowing the number of realizations k in n trials, Eq. (A8.43) can be used to find confidence limits for p .

To simulate (reproduce) a time-homogeneous Markov process, following procedure is useful, starting by a transition in state Z_i at the arbitrary time $t=0$:

1. Select the next state Z_j to be visited by generating an event with probability

$$P_{ij} = \frac{\rho_{ij}}{\rho_i}, \quad j \neq i \quad (P_{ii} \equiv 0), \quad \rho_i = \sum_{j=0, j \neq i}^m \rho_{ij}, \quad \sum_{j=0, j \neq i}^m P_{ij} = 1, \tag{6.306}$$

according to the *embedded Markov chain* (for uniformly distributed random numbers ξ in $[0,1)$ it holds that $\Pr\{\xi \leq x\} = x$, i.e. $\Pr\{x_i < \xi \leq x_j\} = x_j - x_i = p_{ij}$).

2. Find the stay time (sojourn time) in state Z_i up to jump to the next state Z_j by generating a random variable with distribution function (Example A6.18)

$$F_{ij}(x) = 1 - e^{-\rho_i x}. \tag{6.307}$$

3. Jump to state Z_j .

Extension to semi-Markov processes is easy [A7.2 (Ph.D. thesis 1974)]. For semi-regenerative processes, states visited during a cycle must be considered (Fig. A7.11). The advantage of this procedure is that transition sequence and stay (sojourn) times are generated with only a few random numbers. A disadvantage is that the stay times are *truncated* because of the amplitude quantization of $F_{ij}(x)$.

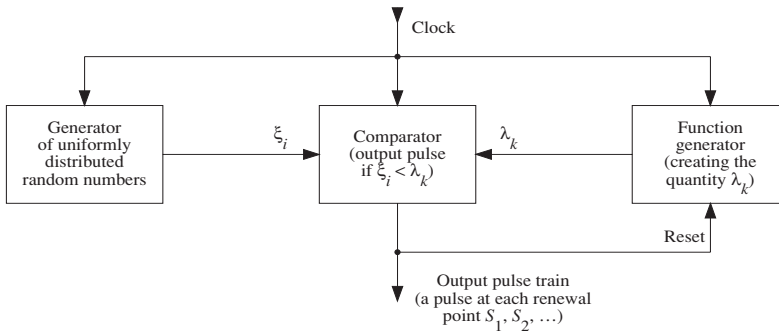


Figure 6.45 Block diagram of the programmable generator for *renewal processes*

To avoid truncation problems, in particular when dealing with rare events distributed on the time axis, an alternative approach implemented as hardware generator for semi-Markov processes in [A7.2 (Ph. D. thesis 1974)] can be used. To illustrate the basic idea, Fig. 6.45 shows the structure of the generator for renewal processes. The generator is driven by a clock $\Delta t = \Delta x$ and consists of three main elements:

- a generator for pseudorandom numbers ξ_i uniformly distributed in $[0,1)$, $\xi_0, \xi_1, \dots, \xi_{2^n-1}$ with $p_i = 1/2^n$ for digital computers ($\xi_i < \lambda_k$ in Fig. 6.45);
- a comparator, comparing at each clock the actual random number ξ_i with λ_k and giving an output pulse, marking a renewal point, for $\xi_i < \lambda_k$;
- a function generator creating λ_k and starting with λ_1 at each renewal point.

It can be shown ($\lambda_k \equiv w_k$ in [A7.2 (1974 & 1977)]) that for

$$\lambda_k = (F(k\Delta x) - F((k-1)\Delta x)) / (1 - F((k-1)\Delta x)), \quad k=1, 2, \dots, F(0)=0, \quad (6.308)$$

the sequence of output pulses is a realization of an ordinary renewal process with distribution function $F(k\Delta x)$ for times (τ) between successive renewal points. λ_k is the failure rate related to the arithmetic random variable (τ) with distribution function $F(k\Delta x)$, $\lambda_k \equiv \lambda(k) = \Pr\{\tau = k\Delta x \mid \tau > (k-1)\Delta x\}$, as given on p. 428. Generated random times (τ) are not truncated, since the last part of $F(k\Delta x)$ can be approximated by a geometric distribution ($\lambda_k = \text{const.}$, Eq. (A6.132)). A software realization of the generator of Fig 6.45 is easy, and hardware limitations can be better avoided.

The homogeneous Poisson process (HPP) can be generated using $\lambda_k = \text{constant}$, the generated random time interval have then a geometric distribution. For a non-homogeneous Poisson process (NHPP) with mean value function $M(t)$, generation can be based on the considerations given on pp. 517-518 (for fixed $t=T$, generate k according to a Poisson distribution with parameter $M(T)$) (Eq. (A7.190), similar as for Eq. (6.306)) and then k random variables with density $m(t)/M(T)$; the ordered values are the k occurrence times of the NHPP on $(0, T)$, see Example A7.13, p. 519). Also is the extension to semi-Markov processes easy [A7.2 (Ph. D. thesis 1974)].

6.9.7 Approximate Expressions for Large Complex Systems: Basic Considerations

Approximate expressions for the reliability and availability of large series-parallel structures, whose elements E_1, E_2, \dots, E_n have constant failure and repair rates $\lambda_i, \mu_i, i=1, \dots, n$, have been developed in Section 6.7, in particular using *macro-structures* (Table 6.10) or *totally independent elements* (Table 6.9). Thereby, based on the results obtained for the repairable 1-out-of-2 redundancy (Eqs. (6.88) & (6.94) with $\lambda_r = \lambda$), a series, parallel, or simple series - parallel structure is considered as a one-item structure with constant failure and repair rates λ_S, μ_S for calculations, and integrated into further macro-structures bottom up to system level.

Expressions for small complex systems, for which a reliability block diagram either does not exist or cannot be reduced to a series-parallel structure with independent elements, have been carefully investigated in Sections 6.8.2 - 6.8.7, assuming no further failures at system down and taking care of imperfect switching, incomplete coverage, more than one failure mode, reconfiguration strategy (time censored (phased-mission) or failure censored), and common cause failures.

Investigation methods and tools for large complex systems are still in progress. Clustering of states (p. 229) is often possible by conserving exact results. Cutting states with more than one failure (p. 229) is applicable, simplify investigations and delivers approximate expressions for reliability and availability often sufficiently good for practical applications (see, for instance, the numerical evaluations on pp. 237, 269). State merging in Markov transition diagrams is conceivable, but basically limited to the case in which transitions from a block of merged states to an unmerged state have the same transition rates [6.40]. To give a feeling for $MTTF_{S0}$ calculation, consider the state reduction in Fig. 6.39 and the possibility to eliminate state Z_0 in Fig. 6.25a (p. 247) by introducing between Z_0 and Z_2 the transition rate

$$\lambda\lambda_{\sigma}(\lambda + \mu) / [\lambda(2\lambda + \lambda_r + \mu) + \lambda_{\sigma}(\lambda + \mu)]. \quad (6.309)$$

Also limited is the exploitation of symmetries in Markov transition diagrams [6.32].

A general procedure delivering often useful upper bounds on the mean time to failure $MTTF_{S0}$ and the asymptotic & steady-state availability $PA_S = AA_S$ at system level can be (for coherent systems (p. 57)):

1. Assume *totally independent elements* (Section 6.9.1) E_1, \dots, E_n with *constant failure rates* λ_i and *repair rates* $\mu_i = \mu, i=1, \dots, n$.
2. Compute $PA_S = AA_S$ as per Eq. (2.48), i.e., substituting in the structure function $\phi(\zeta_1, \dots, \zeta_n)$, given by Eqs. (2.42) or (2.44), ζ_i with

$$PA_{S_i} = \mu / (\lambda_i + \mu), \quad i=1, \dots, n. \quad (6.310)$$

3. Compute $MTTF_{S0}$ from $PA_S = MTTF_S / (MTTF_S + MTTR_S)$ (Eq. (A7.189))

$$MTTF_{S0} \approx PA_S / \mu(1 - PA_S), \quad (6.311)$$

i. e. by assuming

$$MTTF_S \approx MTTF_{S0} \quad \text{and} \quad MTTR_S \approx 1/\mu. \quad (6.312)$$

On the basis of the results obtained for the 1-out-of-2 redundancy (Eqs. (6.88) and (6.94) with $\lambda_r = \lambda$),

$$R_{S0}(t) \approx e^{-t/MTTF_{S0}} \quad \text{and} \quad PA_{S0}(t) \approx PA_S \quad (6.313)$$

can often be assumed at system level. To give a touch for the above approximations, consider a k -out-of- n active redundancy. Comparison of results in Table 6.9 (or Eq. (6.148)) for totally independent elements (IE) and in Table 6.10 for macrostructures (MS) with one repair crew and no further failures at system down, yields

$$MTTF_{S0_{IE}} / MTTF_{S0_{MS}} \approx (n-k)! \quad (6.314)$$

and

$$(1 - PA_{S0_{IE}}) / (1 - PA_{S0_{MS}}) = \overline{PA}_{S0_{IE}} / \overline{PA}_{S0_{MS}} \approx 1 / (n-k+1)!. \quad (6.315)$$

Thus, for weak redundancy levels (small values of $n-k$), the assumption of totally independent elements can yield good *upper bounds* on mean time to failure $MTTF_{S0}$ and asymptotic & steady-state availability $PA_S = AA_S$ at system level. However, exact evaluation of the validity of Eqs. (6.311)-(6.313) can be performed only on a case-by-case basis, and for very complex systems a dedicated computer program or a Monte Carlo simulation can be often the only practicable way to get results.

6.10 Human Reliability

For complex equipment and systems, human and ergonomic factors can have a great influence on the reliability, maintainability, availability, and safety. Disregarding of design and manufacturing flaws, experience show that in emergency situations more than 80% of the safety related system failures are caused by human errors during operation or maintenance (false detection, diagnosis, action planing or execution). Although the behavior of a homogenous human population is often known, the reaction of a *single person* can become unpredictable, in particular when under stress or faced to unexpected events (pp. 10, 158). Thus, wherever possible, humans should be *bypassed in safety critical decisions* or, at least, *two-step actions should be introduced* (the first step being reversible). Moreover, although training and motivation of operators and maintainers is important, extensive requirements and design guidelines are necessary to avoid human errors or limit their effects, in particular in space, nuclear, military and medical applications, see e.g. [5.14, 6.82].

All tools discussed in Section 2.6 and Chapter 6 are useful to investigate human reliability, in particular FMEA / FMECA (including human errors as possible causes), FTA, event trees, and stochastic models. Procedures to evaluate the probability of human errors, in view also of *risk assessment*, have been developed since the 1970s [6.83]; many computer supported, e. g. REHMS-D [6.78], and most of them for

nuclear applications, see e. g. [6.71] for a recent extensive review. These procedures can be grouped in two classes based on

- *reliability techniques used for hardware* (e. g. THERP & SPAR [6.89 & 6.75]),
- *cognitive human models* (e. g. REHMS-D [6.78] & CREAM [6.76 (1998)]).

The method used for the first class is to partition the task performed by the human in subtasks and assign to each subtask a misleading probability; the human error probability can then be expressed as a function of misleading probabilities, from a product to elaborated expressions (p. 10). A further possibility used, is to assign constant failure & repair rates to the human and integrate them in Markov models [6.73]. Cognitive models are more complex, and consider human functions as based on four subfunctions (sensing, information processing, decision, response) assisted by a memory, taking care also of the variability of the human performances caused by temporary psychological, physical, or environmental changes, see e. g. [6.76 (2009)].

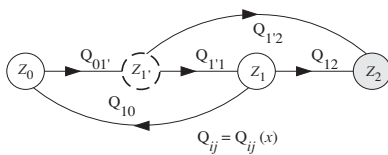
Because of its complexity, and of the necessity to distinguish between *failures* for hardware and *errors* for human activities,

human reliability continues to be a research field (for models & data); modeling must be supported by extensive preventive actions during the development of complex equipment and systems (as for software) and, wherever possible, humans should be bypassed in safety critical decisions (e. g. using majority redundancy also for actuators, or two-step actions).

Section 5.2.5 (p. 158) deals with *design guidelines* useful to avoid human errors or to limit their effects. In the following, three basic models, combining human error probability and time necessary to accomplish a task assigned to a human, are introduced. This, using *semi-Markov processes* (Appendix A7.6), which are characterized by the property that given a state Z_i entered at time t , the next state Z_j to be visited is selected with a probability \mathcal{P}_{ij} and the stay time in Z_i is a random variable $\tau_{ij} > 0$ whose distribution depends only on Z_i and Z_j , not on t (for instance, Z_i is a partial failure or a failure of a redundant element, \mathcal{P}_{ij} an error probability, and τ_{ij} is lognormally distributed). Use of *Markov processes* is less appropriate because of their memoryless property. Investigated in this section is the reliability, extension to safety or to availability is possible (e. g. Example 6. 31 for the model of Fig. 6.46). It turn out that these new models are refinements of those developed for *imperfect switching & incomplete coverage* (Figs. 6.25 & 6.27). To simplify investigations,

it is assumed that no system failure is caused by human during the time it takes a decision (state Z_1 , in Figs. 6.46 -6.48 & Example 6.31).

Consider first a repairable 1-out-of-2 active redundancy with $E_1=E_2=E$ and constant failure & repair rates λ & μ , and assume that at a failure of E_1 or E_2 , the human performance is characterized by a probability p_h to take a wrong decision or make a false action; i. e., for instance, the probability for disconnecting (or causing failure of) the not failed element. Further, assume that the time to take the decision and make a corresponding action is a random variable $\tau_h > 0$ with distribution $F_h(x)$



$$\begin{aligned}
 Q_{01'}(x) &= 1 - e^{-2\lambda x}; & Q_{12'}(x) &= p_h F_h(x); \\
 Q_{11'}(x) &= (1 - p_h) F_h(x); & Q_{10}(x) &= \frac{\mu}{\lambda + \mu} (1 - e^{-(\lambda + \mu)x}); \\
 Q_{12}(x) &= \frac{\lambda}{\mu} Q_{10}(x); \\
 p_h &= \Pr \{ \text{human action incorrect} \}, & \tau_{1'2} &\equiv \tau_{11} \text{ (only one } \tau)
 \end{aligned}$$

Figure 6.46 State transition diagram for reliability calculation of a repairable 1-out-of-2 active redundancy ($E_1=E_2=E$) with const. failure & repair rates (λ, μ), incomplete human performance (false action with probability p_h yielding $Z_{1'} \rightarrow Z_2$), Z_2 down state, semi-Markov proc. (see Fig. 6.27)

and mean $E[\tau_h] = M_h < \infty$ ($F_h(x)$ is e.g. a lognormal distribution (Eq. (A6.110)), not necessarily an exponential because of its memoryless property (Eq. (A6.87)). Considering the constant failure and repair rates λ & μ and that τ_h is common to the good and wrong decision and action, the system can be investigated using a semi-Markov process (Appendix A7.7). ^{+) Figure 6.46 gives the corresponding state transition diagram for reliability calculation (see Example 6.31 for availability). From Fig. 6.46 and Table 6.2 or Eq. (A7.173), $MTTF_{S0}$ is given as solution of}

$$M_0 = T_0 + M_1', \quad M_1' = T_1' + (1 - p_h)M_1, \quad M_1 = T_1 + (\mu / (\lambda + \mu))M_0, \quad (6.316)$$

with $M_i \equiv MTTF_{Si}$, $T_i = \int_0^\infty (1 - Q_i(x)) dx$, $Q_i(x) = \sum_j Q_{ij}(x)$ (Eqs. (A7.166) & (A7.165)). Considering Fig. 6.46 it follows that $T_0 = 1/2\lambda$, $T_1 = M_h$ & $T_1' = 1/(\lambda + \mu)$, yielding

$$MTTF_{S0} = \frac{(\lambda + \mu)(1 + 2\lambda M_h) + 2\lambda(1 - p_h)}{2\lambda(\lambda + \mu p_h)} \approx \frac{\mu(1 + 2\lambda M_h)}{2\lambda(\lambda + \mu p_h)} \approx \frac{\mu}{2\lambda(\lambda + \mu p_h)}. \quad (6.317)$$

The approximation considers $0 \leq p_h \leq 1$ and assumes $2\lambda \ll \mu, 1/M_h$. For

$$\mu p_h \ll \lambda \quad \text{i.e.} \quad p_h \ll \lambda / \mu, \quad (6.318)$$

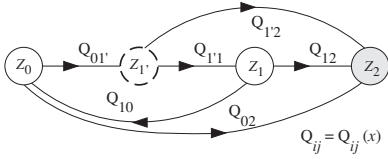
the human influence become negligible. However, would become should be used instead of become to point out that the effect (consequence) of a failure has not been considered. $M_h = 0$ implies the unit step function for $F_h(x)$, yielding to the model of Fig. 6.27 with $c = 1 - p$ (Eq. (6.225)), which can be described also by a time-homogeneous Markov process (Fig. 6.28, Examples 6.18, 6.19). For the reliability function, the approximation $R_{S0}(t) \approx e^{-t/MTTF_{S0}}$ can often be used (Eq. (6.94)).

As a second example, consider a repairable 1-out-of-2 active redundancy with elements $E_1 = E_2 = E$, a series element E_v and constant failure & repair rates $(\lambda, \lambda_v, \mu, \mu_v)$, and assume that at a failure of E_1 or E_2 , the human performance is characterized by a probability p_h to take a wrong decision or make a false action; i.e., for instance, the probability for disconnecting (or causing failure of) the not failed element. Figure 6.46 leads to Fig. 6.47 and (Table 6.2 or Eq. (A7.173))

$$M_0 = T_0 + 2\lambda M_1' / (2\lambda + \lambda_v), \quad M_1' = T_1' + (1 - p_h)M_1, \quad M_1 = T_1 + \mu M_0 / (\lambda + \lambda_v + \mu). \quad (6.320)$$

with $M_i \equiv MTTF_{Si}$, $T_i = \int_0^\infty (1 - Q_i(x)) dx$, $Q_i(x) = \sum_j Q_{ij}(x)$ (Eqs. (A7.166) & (A7.165)).

^{+) Two τ with $\Pr\{\tau_{11} \leq x\} = \Pr\{\tau_{12} \leq x\}$ would imply $p_{11} = p_{12} = 1/2$ (Eqs. (A7.100) & (2.76)).}



$$\begin{aligned}
 Q_{01'}(x) &= \frac{2\lambda}{2\lambda + \lambda_v} (1 - e^{-(2\lambda + \lambda_v)x}); & Q_{1'2}(x) &= p_h F_h(x); \\
 Q_{11'}(x) &= (1 - p_h) F_h(x); & Q_{02}(x) &= \frac{\lambda_v}{2\lambda} Q_{01'}(x); \\
 Q_{12}(x) &= \frac{\lambda + \lambda_v}{\mu} Q_{10}(x); \\
 Q_{10}(x) &= \frac{\mu}{\lambda + \lambda_v + \mu} (1 - e^{-(\lambda + \lambda_v + \mu)x}); \\
 p_h &= \Pr \{ \text{human action incorrect} \}, & \tau_{1'2} &\equiv \tau_{11} \text{ (only one } \tau)
 \end{aligned}$$

Figure 6.47 State transition diagram for reliability calculation of a repairable 1-out-of-2 active redundancy with elements $E_1 = E_2 = E$ and series element E_v , constant failure & repair rates $(\lambda, \lambda_v, \mu, \mu_v)$, incomplete human performance (false action with probability p_h yielding $Z_1' \rightarrow Z_2$), Z_2 down state, semi-Markov process (see also Fig. 6.27)

Using Fig. 6.47 it follows that $T_0 = 1/(2\lambda + \lambda_v), T_{1'} = M_h$ & $T_1 = 1/(\lambda + \lambda_v + \mu)$, yielding

$$MTTF_{S0} = \frac{(\lambda + \lambda_v + \mu)(1 + 2\lambda M_h) + 2\lambda(1 - p_h)}{2\lambda(\lambda + \lambda_v) + \lambda_v(\lambda + \lambda_v + \mu) + 2\lambda\mu p_h} \approx \frac{\mu}{2\lambda(\lambda + \lambda_v) + \lambda_v\mu + 2\lambda\mu p_h}. \quad (6.321)$$

The approximation considers $0 \leq p_h \leq 1$ & $\lambda_v < \lambda$, and assumes $2\lambda \ll \mu, 1/M_h$. For

$$\mu p_h \ll \lambda + \lambda_v \quad \text{i.e.} \quad p_h \ll (\lambda + \lambda_v) / \mu, \quad (6.322)$$

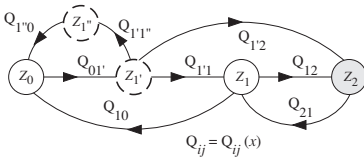
the human influence becomes negligible (apart for the consequence). The influence of series element E_v has been investigated on p. 221. $p_h = (1 - c), \lambda_v = M_h = 0$ yields Eq. (6.225) for incomplete coverage. Fig. 6.47 can also be used for a k -out-of- $(k+1)$ active redundancy with series element E_v and no further failure at system down.

Example 6.31

Investigate $PA_S = AA_S$ for the model of Fig. 6.46 by assuming that the false decision (with p_h) can cause a failure or a disconnection of the not failed element with probability p_{sf} or $1 - p_{sf}$.

Solution

For the availability computation, the state transition diagram of Fig. 6.46 becomes

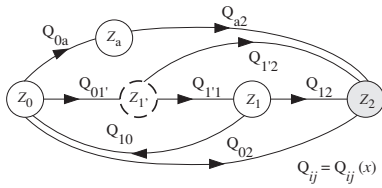


$$\begin{aligned}
 Q_{01'}(x) &= 1 - e^{-2\lambda x}; & Q_{1'2}(x) &= p_h p_{sf} F_h(x); \\
 Q_{11'}(x) &= (1 - p_h) F_h(x); & Q_{10}(x) &= \frac{\mu}{\lambda + \mu} (1 - e^{-(\lambda + \mu)x}); \\
 Q_{21}(x) &= Q_{1'0}(x) = 1 - e^{-\mu x}; & Q_{1'1'}(x) &= p_h (1 - p_{sf}) F_h(x); \\
 Q_{12}(x) &= \frac{\lambda}{\mu} Q_{10}(x); & \tau_{1'2} &\equiv \tau_{11} \text{ (only one } \tau), \\
 p_h &= \Pr \{ \text{human action incorrect} \}, & p_{sf} &= \Pr \{ \text{system failure} \}
 \end{aligned}$$

$PA_S = AA_S$ follows from (Table 6.2) $PA_S = AA_S = \sum_i \mathcal{P}_i T_i / \sum_{k=0}^m \mathcal{P}_k T_k$ with $T_i = \int_0^\infty (1 - Q_i(x)) dx$, $Q_i(x) = \sum_j Q_{ij}(x)$, $\mathcal{P}_{ij} = Q_{ij}(\infty)$; i.e., $T_0 = 1/2\lambda$, $T_1 = 1/(\lambda + \mu)$, $T_{1'} = M_h$, $T_{1''} = T_2 = 1/\mu$, $\mathcal{P}_{01'} = \mathcal{P}_{21} = \mathcal{P}_{1'0} = 1$, $\mathcal{P}_{11} = 1 - p_h$, $\mathcal{P}_{12} = p_h p_{sf}$, $\mathcal{P}_{1'1'} = p_h (1 - p_{sf})$, $\mathcal{P}_{10} = \mu/(\lambda + \mu)$, $\mathcal{P}_{12} = \lambda/(\lambda + \mu)$ & \mathcal{P}_i from $\mathcal{R}_0 = \mathcal{P}_{1'} + \mathcal{P}_1 \mu/(\lambda + \mu)$, $\mathcal{R}_1 = \mathcal{R}_0$, $\mathcal{P}_{1'} = \mathcal{P}_1 (1 - p_h) + \mathcal{P}_2$, $\mathcal{P}_{1''} = \mathcal{P}_1 p_h (1 - p_{sf})$, $\mathcal{P}_0 + \mathcal{P}_1 + \mathcal{P}_{1'} + \mathcal{P}_{1''} + \mathcal{P}_2 = 1$, yielding

$$PA_S = AA_S = \frac{\mathcal{P}_0 T_0 + \mathcal{P}_{1'} T_{1'} + \mathcal{P}_1 T_1}{\mathcal{P}_0 T_0 + \mathcal{P}_1 T_1 + \mathcal{P}_{1'} T_{1'} + \mathcal{P}_{1''} T_{1''} + \mathcal{P}_2 T_2} = 1 / \left(1 + \frac{\mathcal{P}_h (1 - p_{sf}) + a / \mu}{\mu/2\lambda + (a + (1 - p_h)\mu)/(\lambda + \mu) + \mu M_h} \right), \quad (6.319)$$

with $a = (\lambda + \mu) \mathcal{P}_h p_{sf} + \lambda (1 - p_h)$. $p_h = (1 - c), p_{sf} = 1, M_h = 0$ yields Eq. (6.227) for incomplete coverage.



$$\begin{aligned}
 Q_{01'}(x) &= \frac{2\lambda}{2\lambda + \lambda_v + \lambda_a} (1 - e^{-(2\lambda + \lambda_v + \lambda_a)x}); \\
 Q_{11'}(x) &= (1 - p_h)F_h(x); \quad Q_{02}(x) = \frac{\lambda_v}{2\lambda} Q_{01'}(x); \\
 Q_{12}(x) &= \frac{\lambda + \lambda_v}{\mu} Q_{10}(x); \quad Q_{1'2}(x) = p_h F_h(x); \\
 Q_{10}(x) &= \frac{\mu}{\lambda + \lambda_v + \mu} (1 - e^{-(\lambda + \lambda_v + \mu)x}); \\
 Q_{0a}(x) &= \frac{\lambda_a}{2\lambda} Q_{01'}(x); \quad Q_{a2}(x) = 1 - e^{-(2\lambda + \lambda_v)x}; \\
 p_h &= \Pr \{ \text{human action incorrect} \}, \quad \tau_{1'2} \equiv \tau_{11} \text{ (only one } \tau)
 \end{aligned}$$

Figure 6.48 State transition diagram for reliability calculation of a repairable 1-out-of-2 active redundancy with elements $E_1=E_2=E$ and series element E_v , constant failure & repair rates $(\lambda, \lambda_v, \mu, \mu_v)$, incomplete human performance (false action with probability p_h yielding $Z_{1'} \rightarrow Z_2$), alarm circuitry with constant failure rate λ_a (detection and repair only at system down), Z_2 down state, semi-Markov process (see also Fig. 6.27)

As a third example, consider a 1-out-of-2 active redundancy with $E_1=E_2=E$, a series element E_v and constant failure & repair rates $(\lambda, \lambda_v, \mu, \mu_v)$, and assume that at a failure of E_1 or E_2 an alarm is given and the human performance is characterized by a probability p_h to take a wrong decision or make a false action; i. e., the probability for disconnecting (or causing failure of) the not failed element. Furthermore, the alarm circuitry has constant failure rate (λ_a) , failure detection & repair can only occur at system down, and after a failure of the alarm circuitry, a failure of E_1, E_2 or E_v is a system failure. Fig 6.47 leads to Fig. 6.48 and (Table 6.2 or Eq. (A7.173))

$$M_0 = T_0 + \frac{2\lambda M_{1'} + \lambda_a M_a}{2\lambda + \lambda_v + \lambda_a}, \quad M_1 = T_1 + \frac{\mu M_0}{\lambda + \lambda_v + \mu}, \quad M_a = \frac{1}{2\lambda + \lambda_v}, \quad M_{1'} = T_{1'} + (1 - p_h)M_1, \tag{6.323}$$

with $M_i \equiv MTTF_{Si}$, $T_i = \int_0^\infty (1 - Q_i(x)) dx$, $Q_i(x) = \sum_j Q_{ij}(x)$ (Eqs. (A7.166) & (A7.165)). Using Fig. 6.48 it follows that $T_0 = 1 / (2\lambda + \lambda_v + \lambda_a)$, $T_{1'} = M_h$ & $T_1 = 1 / (\lambda + \lambda_v + \mu)$, and thus

$$\begin{aligned}
 MTTF_{S0} &= \frac{(\lambda + \lambda_v + \mu) [1 + \lambda_a / (2\lambda + \lambda_v) + 2\lambda M_h] + 2\lambda(1 - p_h)}{2\lambda(\lambda + \lambda_v) + (\lambda_v + \lambda_a)(\lambda + \lambda_v + \mu) + 2\lambda\mu p_h} \\
 &\approx \frac{\mu}{2\lambda(\lambda + \lambda_v) + \mu(\lambda_v + \lambda_a) + 2\lambda\mu p_h}. \tag{6.324}
 \end{aligned}$$

The approximation considers $0 \leq p_h \leq 1$ & $\lambda_v < \lambda$, and assumes $\lambda_a \ll 3\lambda \ll \mu, 1/M_h$. For

$$\mu p_h \ll \lambda + \lambda_v \quad \text{i. e.} \quad p_h \ll (\lambda + \lambda_v) / \mu, \tag{6.325}$$

the human influence becomes negligible (apart for the consequence). For $p_h \equiv M_h \equiv 0$, the influence of the alarm circuitry becomes negligible for

$$\mu \lambda_a \ll 2\lambda(\lambda + \lambda_v) \quad \text{i. e.} \quad \lambda_a \ll 2\lambda(\lambda + \lambda_v) / \mu, \tag{6.326}$$

which is similar to the influence of the series element E_v (Eq. (6.160)).

7 Statistical Quality Control and Reliability Tests

Statistical quality control and *reliability tests* are performed to estimate or demonstrate quality and reliability characteristics on the basis of data collected from sampling tests. *Estimation* leads to *point or interval estimate*, marked with $\hat{}$ in this book; *demonstration* is a test of a given *hypothesis* on the unknown characteristic. Estimation and demonstration of an *unknown probability* is investigated in Section 7.1 for the case of a defective probability p and in Section 7.2.1 for some reliability figures. Procedures for availability estimation and demonstration for the case of continuous operation (steady-state) are given in Section 7.2.2. Estimation and demonstration of a *constant failure rate* λ (or *MTBF* for the case $MTBF=1/\lambda$) are discussed in depth in Sections 7.2.3. The case of an *MTTR* is considered in Section 7.3. Basic models for *accelerated tests* are discussed in Section 7.4. *Goodness-of-fit tests* based on graphical & analytical procedures are summarized in Section 7.5. General reliability data analysis, including test on nonhomogeneous Poisson processes and *trend tests*, are discussed in Section 7.6; models for reliability growth in Section 7.7. A comprehensive introduction to the mathematical foundations for this chapter is given in Appendix A8. To simplify the notation, *sample* is used for *random sample*, *mean* for *expected value*, and *independent* for *totally* (mutually, statistically, stochastically) *independent*. Furthermore, the indices S_i , with S referring to system (the highest integration level of the item considered) and i for the state entered at $t=0$,

are omitted in this chapter (*MTBF* used for $MTBF_{S0}$ and *PA* for PA_S).

Selected examples illustrate the practical aspects.

7.1 Statistical Quality Control

One of the main purposes of *statistical quality control* is to use *sampling tests* to *estimate* or *demonstrate* the *defective probability* p of a given item, to a required accuracy and often on the basis of tests by *attributes* (i. e., tests of type good/bad). However, considering p as an *unknown probability*, a broader field of applications can be covered by the same methods. Other topics, such as *tests by variables* and *statistical processes control* [7.1-7.5], are not considered in this book.

In this section, p will be considered as a *defective probability* (fraction of defective items). It will be assumed that p is the same for each element in the sample considered and that each sample element is independent from each other. These assumptions presuppose that the lot is *homogeneous* and *much larger* than the sample. They allow the use of the *binomial distribution* (Appendix A6.10.7).

7.1.1 Estimation of a Defective Probability p

Let n be the size of a (random) sample from a large homogeneous lot. If k defective items have been observed within the sample of size n , then (Eq. (A8.29))

$$\hat{p} = k/n \tag{7.1}$$

is the *maximum likelihood point estimate* of the defective probability p for an item in the lot under consideration. $\hat{p} = k/n$ is unbiased ($E[\hat{p}] = p$) and k is a sufficient statistic (delivers the complete information about p , Appendix A8.2.1). Furthermore, $\text{Var}[\hat{p}] = \text{Var}[k]/n^2 = p(1-p)/n$ (Eqs. (A6.123), (A6.40), (A6.46)). For a given *confidence level* $\gamma = 1 - \beta_1 - \beta_2$ ($0 < \beta_1 < 1 - \beta_2 < 1$), the *lower* \hat{p}_l and *upper* \hat{p}_u limit of the *confidence interval* for p can be obtained from

$$\sum_{i=k}^n \binom{n}{i} \hat{p}_l^i (1 - \hat{p}_l)^{n-i} = \beta_2 \quad \text{and} \quad \sum_{i=0}^k \binom{n}{i} \hat{p}_u^i (1 - \hat{p}_u)^{n-i} = \beta_1 \tag{7.2}$$

for $0 < k < n$, and from

$$\hat{p}_l = 0 \quad \text{and} \quad \hat{p}_u = 1 - \sqrt[n]{\beta_1} \quad \text{for } k = 0 \quad (\gamma = 1 - \beta_1), \tag{7.3}$$

or from

$$\hat{p}_l = \sqrt[n]{\beta_2} \quad \text{and} \quad \hat{p}_u = 1 \quad \text{for } k = n \quad (\gamma = 1 - \beta_2), \tag{7.4}$$

see Eqs. (A8.37) to (A8.40) and the remarks given there. β_1 is the risk that the true value of p is larger than \hat{p}_u and β_2 the risk that the value of p is smaller than \hat{p}_l . The *confidence level* is nearly equal to (but not less than) $\gamma = 1 - \beta_1 - \beta_2$. It can be considered as the relative frequency of cases in which the interval $[\hat{p}_l, \hat{p}_u]$ overlaps (covers) the true value of p , in an increasing series of repetitions of the experiment of taking a random sample of size n .

In many practical applications, a graphical determination of \hat{p}_l and \hat{p}_u is sufficient. The upper diagram in Fig. 7.1 can be used for $\beta_1 = \beta_2 = 0.05$, the lower diagram for $\beta_1 = \beta_2 = 0.1$ ($\gamma = 0.9$ and $\gamma = 0.8$, respectively). The continuous lines in Fig. 7.1 are the envelopes of the staircase functions (k, n integer) given by Eq. (7.2). They converge rapidly, for $\min(np, n(1-p)) \geq 5$, to the *confidence ellipses* (dashed lines in Fig. 7.1). Using the confidence ellipses (Eq. (A8.42)), \hat{p}_l and \hat{p}_u can be calculated from (Eq. (A8.43))

$$\hat{p}_{l,u} = \frac{k + 0.5b^2 \pm b\sqrt{k(1-k/n) + b^2/4}}{n + b^2}, \quad \beta_1 = \beta_2 = (1 - \gamma)/2. \tag{7.5}$$

b is the $1 - (1 - \gamma)/2 = (1 + \gamma)/2$ quantile of the standard normal distribution $\Phi(t)$, given for some typical values of γ by (Table A9.1)

$\gamma =$	0.6	0.8	0.9	0.95	0.98	0.99
$b =$	0.84	1.28	1.64	1.96	2.33	2.58

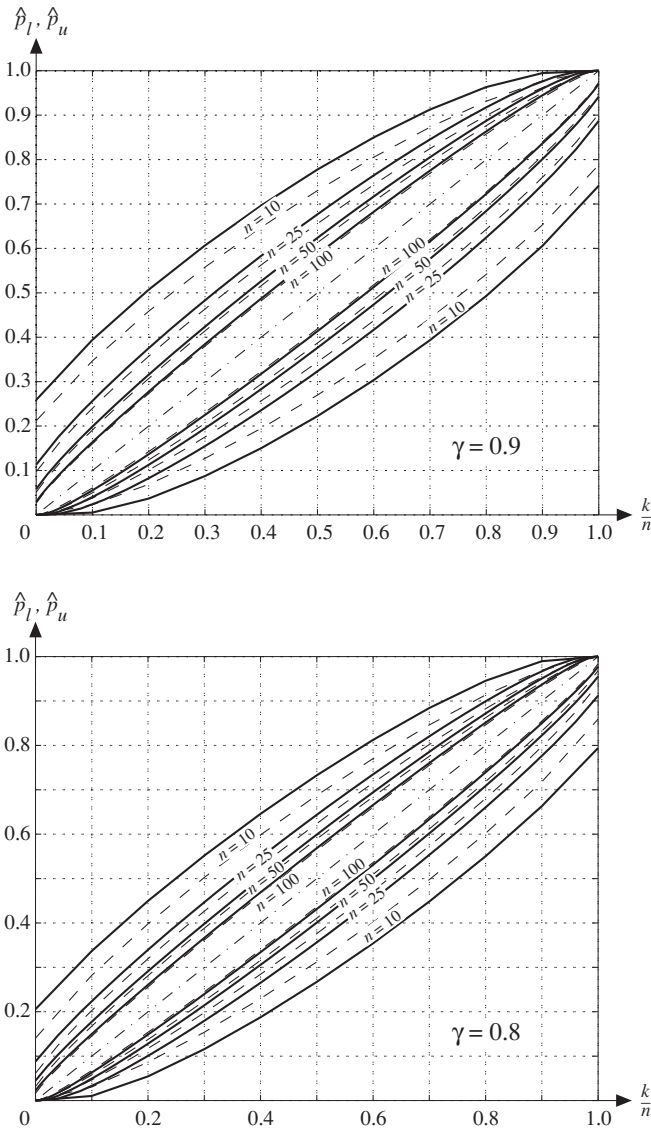


Figure 7.1 Confidence limits \hat{p}_l and \hat{p}_u for an unknown probability p (e.g. defective probability) as a function of the observed relative frequency k/n ($n =$ sample size, $k =$ observed events); $\gamma =$ confidence level $= 1 - \beta_1 - \beta_2$, here with $\beta_1 = \beta_2$ (continuous lines are the exact solution per Eqs. (7.2) - (7.4), dashed the confidence ellipses per Eq. (7.5))

Example: $n = 25, k = 5$ gives $\hat{p} = k/n = 0.2$ and for $\gamma = 0.9$ the confidence interval $[0.08, 0.38]$ $([0.0823, 0.3754]$ using Eq. (7.2), and $[0.1011, 0.3572]$ using Eq. (7.5))

The confidence limits \hat{p}_l and \hat{p}_u can also be used as *one-sided confidence intervals*. In this case (Eq. (A8.44)),

$$\begin{aligned} 0 \leq p \leq \hat{p}_u & \quad (\text{or simply } p \leq \hat{p}_u), & \quad \text{with } \gamma = 1 - \beta_1 \\ \hat{p}_l \leq p \leq 1 & \quad (\text{or simply } p \geq \hat{p}_l), & \quad \text{with } \gamma = 1 - \beta_2. \end{aligned} \quad (7.6)$$

Example 7.1

In a sample of size $n = 25$, $k = 5$ items were found to be defective. Determine for the underlying defective probability p , (i) the point estimate, (ii) the interval estimate for $\gamma = 0.8$ ($\beta_1 = \beta_2 = 0.1$), (iii) the upper bound on p for a one sided confidence interval with $\gamma = 0.9$.

Solution

(i) Equation (7.1) yields the point estimate $\hat{p} = 5/25 = 0.2$. (ii) For the interval estimate, the lower part of Fig. 7.1 leads to the confidence interval $[0.10, 0.34]$, $[0.1006, 0.3397]$ using Eq. (7.2) and $[0.1175, 0.3194]$ using Eq. (7.5). (iii) With $\gamma = 0.9$ it holds $p \leq 0.34$.

Supplementary result: The upper part of Fig. 7.1, would lead to $p \leq 0.38$ with $\gamma = 0.95$.

Note that the role of k/n and p can be *reversed* and Eq. (7.5) can be used to calculate the limits k_1 and k_2 of the number of observations k in n *independent trials* (e.g. the number k of defective items in a sample of size n) for *given* probability $\gamma = 1 - \beta_1 - \beta_2$ (with $\beta_1 = \beta_2$) and *known* values of p and n (Eq. (A8.45))

$$k_{1,2} = n p \pm b \sqrt{n p (1 - p)}. \quad (7.7)$$

As in Eq. (7.5), the quantity b in Eq. (7.7) is the $(1 + \gamma)/2$ quantile of the standard normal distribution (e.g. $b = 1.64$ for $\gamma = 0.9$, Table A9.1). For a graphical solution, Fig. 7.1 can be used by taking the ordinate p as known, and by reading k_1/n and k_2/n from the abscissa.

7.1.2 Simple Two-sided Sampling Plans for the Demonstration of a Defective Probability p

In the context of *acceptance testing*, the *demonstration* of a defective probability p is often required, instead of its estimation (Section 7.1.1). The main concern of this test is to check a *zero hypothesis* $H_0: p < p_0$ against an *alternative hypothesis* $H_1: p > p_1$ on the basis of the following agreement between producer and consumer:

The lot should be accepted with a probability nearly equal to (but not less than) $1 - \alpha$ if the true (unknown) defective probability p is lower than p_0 , but rejected with a probability nearly equal to (but not less than) $1 - \beta$ if p is greater than p_1 ($p_0, p_1 > p_0$, and $0 < \alpha < 1 - \beta < 1$ are given (fixed) values).

p_0 is the *specified* defective probability and p_1 is the *maximum acceptable* defective

probability. α is the allowed *producer's risk* (type I error), i.e., the probability of *rejecting a true hypothesis* $H_0: p < p_0$. β is the allowed *consumer's risk* (type II error), i.e., the probability of *accepting* the hypothesis $H_0: p < p_0$ when the alternative hypothesis $H_1: p > p_1$ is true. Verification of the agreement stated above is a problem of statistical hypothesis testing (Appendix A8.3) and can be performed, for instance, with a *simple two-sided sampling plan* or a *sequential test*. In both cases, the basic model is the sequence of *Bernoulli trials*, as introduced in Appendix A6.10.7.

7.1.2.1 Simple Two-sided Sampling Plan

The procedure (*test plan*) for the *simple two-sided sampling plan* is as follows (Appendix A8.3.1.1):

1. From p_0 , p_1 , α , and β , determine the smallest integers c and n which satisfy

$$\sum_{i=0}^c \binom{n}{i} p_0^i (1-p_0)^{n-i} \geq 1-\alpha \quad (7.8)$$

and

$$\sum_{i=0}^c \binom{n}{i} p_1^i (1-p_1)^{n-i} \leq \beta. \quad (7.9)$$

2. Take a sample of size n , determine the number k of defective items in the sample, and

$$\begin{aligned} &\bullet \text{ reject } H_0: p < p_0, && \text{if } k > c \\ &\bullet \text{ accept } H_0: p < p_0, && \text{if } k \leq c. \end{aligned} \quad (7.10)$$

The graph of Fig. 7.2 visualizes the validity of the above rule (see Appendix A8.3.1.1 for a proof). It satisfies inequalities (7.8) & (7.9), and is known as *operating characteristic curve* (or *acceptance probability curve*). For each value of p , it gives the probability of having no more than c defective items in a sample of size n . Since the operating characteristic curve decreases monotonically in p , the risk for a false decision decreases for $p < p_0$ and $p > p_1$, respectively. It can be shown that the quantities c and np_0 depend only on α , β , and the ratio p_1 / p_0 (*discrimination ratio*). Table 7.3 (p. 323) gives c and np_0 for some important values of α , β and p_1 / p_0 for the case where the *Poisson approximation* (Eq. (A6.129)) applies.

Using the operating characteristic curve, the *Average Outgoing Quality (AOQ)* can be calculated. *AOQ* represents the mean percentage of defective items that reach the customer, assuming that all rejected samples have been 100% inspected, and that the defective items have been replaced by good ones, and is given by

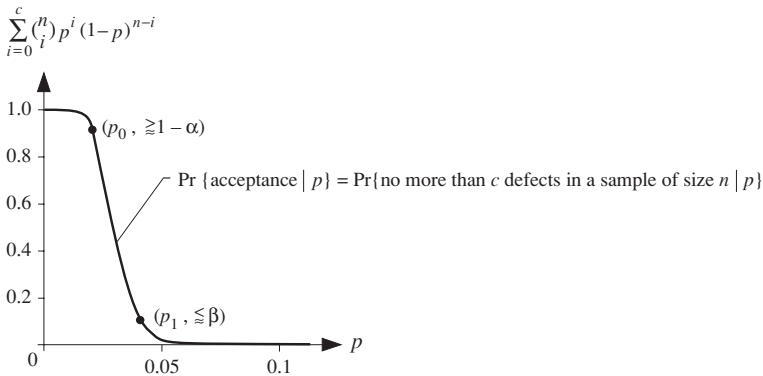


Figure 7.2 Operating characteristic curve (acceptance probability curve) as a function of the defective probability p for $p_0=2\%$, $p_1=4\%$, $\alpha=\beta \approx 0.1$, $n=510$, $c=14$ as per Table 7.3 (see also Fig. 7.3)

$$AOQ = \Pr\{p \cap \text{acceptance}\} = p \Pr\{\text{acceptance} \mid p\} = p \sum_{i=0}^c \binom{n}{i} p^i (1-p)^{n-i}. \quad (7.11)$$

The maximum value of AOQ is the *Average Outgoing Quality Limit* [7.4, 7.5].

Obtaining the solution of inequalities (7.8) and (7.9) is time-consuming. For small values of p_0 & p_1 (up to a few %), the *Poisson approximation* (Eq. (A6.129))

$$\binom{n}{i} p^i (1-p)^{n-i} \approx \frac{(np)^i}{i!} e^{-np}$$

can be used. Introducing the Poisson approximation in Eqs. (7.8) and (7.9) leads to a Poisson distribution with parameters $m_1 = np_1$ and $m_0 = np_0$, which can be solved using a table of the χ^2 -distribution (Table A9.2). Alternatively, the curves of Fig. 7.3 provide graphical solutions, sufficiently good for practical applications. Exact solutions are in Table 7.3 (p. 323).

Example 7.2

Determine, using the Poisson approximation, the sample size n and the number of allowed defective items c to test the null hypothesis $H_0: p < p_0 = 1\%$ against the alternative hypothesis $H_1: p > p_1 = 2\%$ with producer and consumer risks $\alpha = \beta = 0.1$ (which means $\alpha \approx \beta \approx 0.1$).

Solution

Considering $\alpha=\beta=0.1$ & $p_1/p_0=2$, Table 7.3 (p. 323) yields $c=14$ and $np_0 = \lambda_0 T = 10.17$ from which $n=1017$, for $\alpha \approx \beta \approx 0.093$. The graph of Fig. 7.3 yields practically the same result: $c=14$, $m_0 \approx 10.2$ and $m_1 \approx 20.4$ for $\alpha \approx \beta \approx 0.1$. Results using directly Table A9.2 lead to $v=30$ (value of v for which $t_{v,q_2} / t_{v,q_1} = 2$ with $q_1 = \alpha \leq 0.1$ $q_2 = 1 - \beta \geq 0.9$) and, with linear interpolation, $F(20.34) \approx 0.093 \leq \alpha = 0.1$ and $F(40.68) \approx 0.906 \geq 1 - \beta = 0.9$; thus, $c=v/2-1=14$ and $n=20.34/(2 \cdot 0.01)=1017$. (Graphical and analytical methods require a solution by successive approximation: choice of c , starting at $c=0$, and check of conditions for α and β by considering the ratio p_1/p_0 .)

7.1.2.2 Sequential Test

The procedure for a *sequential test* is as follows (Appendix A8.3.1.2):

1. In a Cartesian coordinate system draw the *acceptance line* $y_1(n) = a n - b_1$ and the *rejection line* $y_2(n) = a n + b_2$, with

$$a = \frac{\ln \frac{1-p_0}{1-p_1}}{\ln \frac{p_1}{p_0} + \ln \frac{1-p_0}{1-p_1}}, \quad b_1 = \frac{\ln \frac{1-\alpha}{\beta}}{\ln \frac{p_1}{p_0} + \ln \frac{1-p_0}{1-p_1}}, \quad b_2 = \frac{\ln \frac{1-\beta}{\alpha}}{\ln \frac{p_1}{p_0} + \ln \frac{1-p_0}{1-p_1}}. \quad (7.12)$$

2. Select one item after another from the lot, test the item, enter the test result in the diagram drawn in step 1, and stop the test as soon as either the rejection or the acceptance line is crossed.

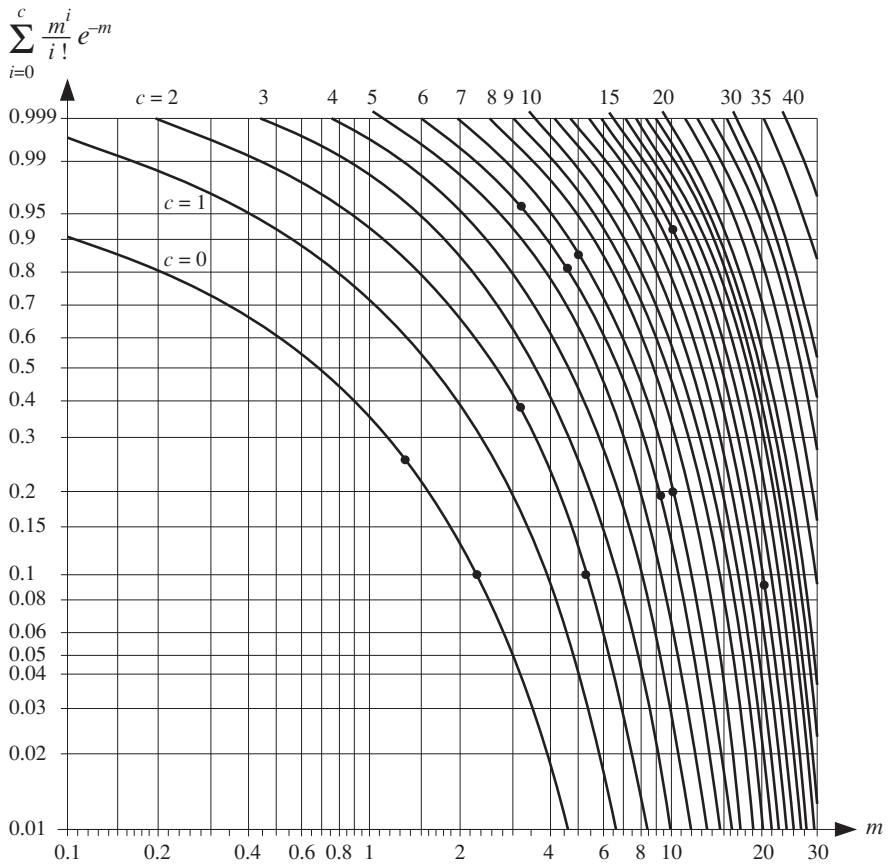


Figure 7.3 Poisson distribution (• results for Examples 7.2 ($c=14$), 7.4 (7), 7.5(0), 7.6(2 & 0), 7.9 (6))

Figure A8.8 shows acceptance and rejection lines for $p_0=1\%$, $p_1=2\%$ & $\alpha=\beta\approx 0.2$. The advantage of the sequential test is that on *average* it requires a smaller sample size than the corresponding simple two-sided sampling plan (Example 7.10 or Fig. 7.8). A disadvantage is that the test duration (sample size) is random.

7.1.3 One-sided Sampling Plans for the Demonstration of a Defective Probability p

The two-sided sampling plans of Section 7.1.2 are fair in the sense that for $\alpha = \beta$, both producer and consumer run the *same risk* of making a false decision. In practical applications however, *one-sided sampling plans* are often used, i.e., only p_0 and α or p_1 and β are specified. In these cases, the operating characteristic curve (acceptance probability curve) is not completely defined. For every value of c ($c = 0, 1, \dots$) a *smallest* n ($n = 1, 2, \dots$) exists which satisfies inequality (7.8) for a given p_0 and α , or a *largest* n exists which satisfies inequality (7.9) for a given p_1 and β . One recognizes that operating characteristic curves become steeper as the value of c increases (see e.g. Figs. 7.4 or A8.9). Hence, for small values of c , the producer (if p_0 and α are given) or the consumer (if p_1 and β are given) *can be favored*. Figure 7.4 (obtained from Fig. 7.3) visualizes the reduction of the consumer risk (from $\beta \approx 0.88$ for $c=0$ or ≈ 0.97 for $c=7$) by increasing values of the defective probability p or values of c , see Fig 7.9 for a counterpart.

When only p_0 and α or p_1 and β are given, it is usual to set in these cases

$$p_0 = AQL \quad \text{and} \quad p_1 = LTPD, \quad (7.13)$$

respectively, where *AQL* is the *Acceptable Quality Level* and *LTPD* is the *Lot Tolerance Percent Defective* (Eqs. (A8.79) to (A8.82)).

A large number of one-sided sampling plans for the demonstration of *AQL* values are given in national and *international standards* (*IEC 60410*, *ISO 2859*, *MIL-STD-105*, *DIN 40080* [7.3]). Many of these plans have been established empirically. The following remarks can be useful when evaluating such plans:

1. *AQL* values are given in %.
2. The values for n and c are in general obtained using the *Poisson approximation*.
3. Not all values of c are listed, the value of α often decreases with increasing c .
4. Sample size is related to lot size, and this relationship is empirical.
5. A distinction is made between reduced tests (level I), normal tests (level II) and tightened tests (level III); level II is normally used; transition from one level to another is often given empirically (e.g. transition from level II to level III is necessary if 2 out of 5 successive independent lots have been rejected and a return to level II follows if 5 successive independent lots are passed).
6. The value of α is not given explicitly (for $c = 0$, for example, α is approximately 0.05 for level I, 0.1 for level II, and 0.2 for level III).

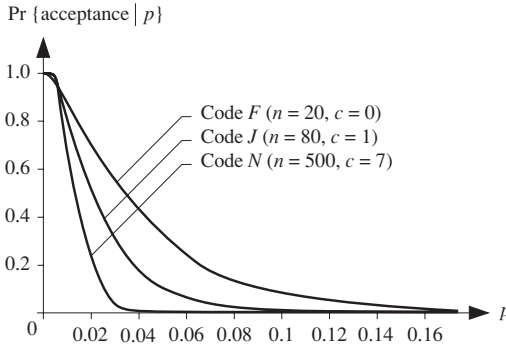


Figure 7.4 Operating characteristic curves (acceptance probability curves) as a function of the defective probability p for $p_0=AQL=0.65\%$ with sample sizes $n=20, 80, 500$ as per Table 7.1 ($\alpha \approx 0.12$ for $c=0$, ≈ 0.09 for $c=1$, ≈ 0.02 for $c=7$ per Fig. 7.3 or Table A9.2)

Table 7.1 presents some test procedures for AQL values from *IEC 60410* [7.3] and Fig. 7.4 shows the corresponding operating characteristic curves for $AQL = 0.65\%$ and sample size $n=20, 80, \text{ and } 500$.

Test procedures for demonstration of $LTPD$ values with given (fixed) customer risk β are for example in [3.12 (S-19500)]. They are often based on the Poisson approximation (p. 304) and can be easily established using a χ^2 -table (Appendix A9.2) or Fig. 7.3. For given β and $LTPD$, the values of n and c can be obtained taking in Fig. 7.3

$$\sum_{i=0}^c \frac{(m)^i}{i!} e^{-m} = \beta$$

and reading $m = np = nLTPD$ for $c = 0, 1, 2, \dots$ (Example: $\beta = 0.1$ & $LTPD = 2\%$ yields $m = 3.9$ for $c = 1$, and from this $n = 3.9/0.02 = 195$; the procedure is thus: test 195 items and reject $LTPD = 2\%$ if more than 1 defect occur).

In addition to the simple one-sided sampling plans described above, *multiple one-sided sampling plans* are often used to demonstrate AQL values. In a *double one-sided sampling plan*, the following procedure is used:

1. Take a first sample of size n_1 and accept definitely if no more than c_1 defects occur, but reject definitely if exactly or more than d_1 defects have occurred.
2. If after the first sample the number of defects is greater than c_1 but less than d_1 , take a second sample of size n_2 and accept if there are totally (in the first and second sample) no more than c_2 defects; elsewhere reject.

The operating characteristic curve (acceptance probability curve) for a *double one-sided sampling plan* can be calculated as

$$\Pr \{ \text{acceptance} \mid p \} = \sum_{i=0}^{c_1} \binom{n_1}{i} p^i (1-p)^{n_1-i} + \sum_{i=c_1+1}^{d_1-1} \left[\binom{n_1}{i} p^i (1-p)^{n_1-i} \sum_{j=0}^{c_2-i} \binom{n_2}{j} p^j (1-p)^{n_2-j} \right]. \quad (7.14)$$

Multiple one-sided sampling plans are also given in national and *international standards*, see for example *IEC 60410* [7.3] for the following double one-sided sampling plan to demonstrate $AQL = 1\%$

Sample Size	n_1	n_2	c_1	d_1	c_2
281 - 500	32	32	0	2	1
501 - 1,200	50	50	0	3	3
1,201 - 3,200	80	80	1	4	4
3,201 - 10,000	125	125	2	5	6

The advantage of multiple one-sided sampling plans is that on average they require smaller sample sizes than would be necessary for simple one-sided sampling plans. A disadvantage is that the test duration is not fixed in advance.

Table 7.1 Test procedures for *AQL demonstration* (test level II, from *IEC 60410* [7.3])

Code	Lot size N	Sam- ple size n	AQL in %											
			0.04	0.065	0.10	0.15	0.25	0.40	0.65	1.0	1.5	2.5	4.0	6.5
			c	c	c	c	c	c	c	c	c	c	c	c
A	2 - 8	2	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	0
B	9 - 15	3	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	0	↑
C	16 - 25	5	↓	↓	↓	↓	↓	↓	↓	↓	↓	0	↑	↓
D	26 - 50	8	↓	↓	↓	↓	↓	↓	↓	↓	0	↑	↓	1
E	51 - 90	13	↓	↓	↓	↓	↓	↓	↓	0	↑	↓	1	2
F	91 - 150	20	↓	↓	↓	↓	↓	↓	0	↑	↓	1	2	3
G	151 - 280	32	↓	↓	↓	↓	↓	0	↑	↓	1	2	3	5
H	281 - 500	50	↓	↓	↓	↓	0	↑	↓	1	2	3	5	7
J	501 - 1200	80	↓	↓	↓	0	↑	↓	1	2	3	5	7	10
K	1.2k - 3.2k	125	↓	↓	0	↑	↓	1	2	3	5	7	10	14
L	3.2k - 10k	200	↓	0	↑	↓	1	2	3	5	7	10	14	21
M	10k - 35k	315	0	↑	↓	1	2	3	5	7	10	14	21	↑
N	35k - 150k	500	↑	↓	1	2	3	5	7	10	14	21	↑	↑
P	150k - 500k	800	↓	1	2	3	5	7	10	14	21	↑	↑	↑
Q	over 500k	1250	1	2	3	5	7	10	14	21	↑	↑	↑	↑

use the first sampling plan above for ↑ or below for ↓, c = number of allowed defects

7.2 Statistical Reliability Tests

Reliability tests are useful to evaluate the reliability *achieved* in a given item. Early initiation of such tests allows quick identification and *cost-effective correction* of weaknesses not discovered by reliability analyses. This supports a learning process, often related to a reliability growth program (Section 7.7). Since reliability tests are generally time-consuming and expensive, they must be coordinated with other tests. Test conditions should be as close as possible to those experienced in the field. As with quality control, a distinction is made between *estimation* and *demonstration* of a specific reliability figure. Section 7.2.1 uses results of Section 7.1 for reliability and availability testing for the case of a *given (fixed) mission*. In section 7.2.2 an unified method for availability estimation and demonstration for the case of continuous operation is introduced. Section 7.2.3 deals carefully with *estimation* and *demonstration* of a constant failure rate λ (or *MTBF* for the case $MTBF = 1/\lambda$). Furthermore, maintainability tests are considered in Section 7.3, accelerated tests in Section 7.4, goodness-of-fit tests in Section 7.5, general reliability data analysis and trend tests in Section 7.6, and reliability growth in Section 7.7. To simplify notations,

the indices S_i are omitted ($R, PA, MTBF, \lambda$ used for $R_{S0}, PA_S, MTBF_{S0}, \lambda_S$).

7.2.1 Reliability & Availability Estimation and Demonstration for the Case of a given fixed Mission

Reliability (R) and availability (asymptotic & steady-state point and average availability $PA = AA$) are often defined as success probability for a given (fixed) mission. Their estimation and demonstration can thus be performed as for an unknown probability p (Section 7.1) by setting, for convenience,

$$p = 1 - R \quad \text{or} \quad p = 1 - PA = 1 - AA.$$

For a demonstration, the null hypothesis $H_0: p < p_0$ is converted to $H_0: R > R_0$ or $H_0: AA > AA_0$, which adheres better to the concept of reliability or availability. The same holds for any other reliability figure expressed as an *unknown probability* p .

The above considerations hold for a given (fixed) mission, repeated as n Bernoulli trials. However, for the case of continuous operation, estimation and demonstration of an availability can lead to a difficulty in defining the time points t_1, t_2, \dots, t_n at which the n observations according to Eqs. (7.2)-(7.4) or (7.8)-(7.10) have to be performed. The case of continuous operation is considered in Section 7.2.2 for availability and Section 7.2.3 for reliability. Examples 7.3-7.6 illustrate some cases of reliability tests for given fixed mission.

Example 7.3

In a reliability test 95 of 100 items pass. Give the confidence interval for R at $\gamma = 0.9$ ($\beta_1 = \beta_2$).

Solution

With $p = 1 - R$ and $\hat{R} = 0.95$ the confidence interval for p follows from Fig. 7.1 as [0.03, 0.10]. The confidence interval for R is then [0.9, 0.97]; Eq. (7.5) leads to [0.901, 0.975] for R .

Example 7.4

The reliability of a given subassembly was $R = 0.9$ and should have been improved through constructive measures. In a test of 100 subassemblies, 94 of them pass the test. Check with a type I error $\alpha = 20\%$ the hypothesis $H_0: R > 0.95$.

Solution

For $p_0 = 1 - R_0 = 0.05$, $\alpha = 20\%$, and $n = 100$, Eq. 7.8 delivers $c = 7$ (see also the graphical solution from Fig. 7.3 with $m = np_0 = 5$ and acceptance probability $\geq 1 - \alpha = 0.8$, yielding $\alpha \approx 0.15$ for $m = 5$ and $c = 7$). As just $k = 6$ subassemblies have failed the test, the hypothesis $H_0: R > 0.95$ can be accepted (must not be rejected) at the level $1 - \alpha \approx 0.85$.

Supplementary result: Assuming as an alternative hypothesis $H_1: R < 0.90$, or $p > p_1 = 0.1$, the type II error β can be calculated from Eq. (7.9) with $c = 7$ & $n = 100$ or graphically from Fig. 7.3 with $m = np_1 = 10$, yielding $\beta \approx 0.2$.

Example 7.5

Determine the minimum number of tests n that must be repeated to verify the hypothesis $H_0: R > R_1 = 0.95$ with a consumer risk $\beta = 0.1$. What is the allowed number of failures c ?

Solution

n and c must satisfy the inequality (7.9) with $p_1 = 1 - R_1 = 0.05$ and $\beta = 0.1$, i. e.,

$$\sum_{i=0}^c \binom{n}{i} 0.05^i \cdot 0.95^{n-i} \leq 0.1.$$

The number of tests n is a minimum for $c = 0$. From $0.95^n \leq 0.1$, it follows that $n = 45$, yielding $\beta \approx 0.099$ (calculation with the Poisson approximation (Eq. (7.12)) yields $n = 46$, a graphical solution with Fig. 7.3 leads to $m \approx 2.3$ and then $n = m/p_1 \approx 46$).

Example 7.6

Continuing with Example 7.5, (i) find n for $c = 2$ and (ii) how large would the producer risk be for $c = 0$ and $c = 2$ if the true reliability were $R = 0.97$?

Solution

(i) From Eq. (7.9),

$$\sum_{i=0}^2 \binom{n}{i} 0.05^i \cdot 0.95^{n-i} \leq 0.1$$

and thus $n = 105$ (Fig. 7.3 yields $m \approx 5.3$ and $n \approx 106$; from Table A9.2, $v = 6$, $t_{6,0.9} = 10.645$ and $n = 107$).

(ii) The producer risk is

$$\alpha = 1 - \sum_{i=0}^c \binom{n}{i} 0.03^i \cdot 0.97^{n-i},$$

hence, $\alpha \approx 0.75$ for $c = 0$ and $n = 45$, $\alpha \approx 0.61$ for $c = 2$ and $n = 105$ (Fig. 7.3, yields $\alpha \approx 0.75$ for $c = 0$ and $m = 1.35$, $\alpha \approx 0.62$ for $c = 2$ and $m = 3.15$; from Table A9.2, $\alpha \approx 0.73$ for $v = 2$ and $t_{2,\alpha} = 2.7$, $\alpha \approx 0.61$ for $v = 6$ and $t_{6,\alpha} = 6.3$ lin. int. (0.74 and 0.61 from [A9.1])).

7.2.2 Availability Estimation & Demonstration for the Case of Continuous Operation (asymptotic & steady-state values)

As refinement on the procedure given in Section 7.2.1, availability estimation and demonstration for a repairable item in continuous operation can be based on results given in Section 6.2 for the one-item repairable structure. Point estimate (with corresponding mean and variance) for the availability can be found for arbitrary distributions of failure-free and repair times (Section 7.2.2.3). However, interval estimation and demonstration tests can lead to some difficulties. An unified approach for estimating & demonstrating the asymptotic and steady-state point and average availability $PA = AA$ for the case of exponentially or Erlangian distributed failure-free and/or repair times is introduced in Appendices A8.2.2.4 & A8.3.1.4 (to simplify the notation, $PA = AA$ is used for $PA_S = AA_S$).

Sections 7.2.2.1 and 7.2.2.2 deal with this approach. The case of exponentially distributed failure-free & repair times, i.e., constant failure & repair rates ($\lambda(x) = \lambda$, $\mu(x) = \mu$) is considered in detail, extension to Erlangian distributions is outlined. Point and average *unavailability* ($1 - PA_{S0}(t)$ and $1 - AA_{S0}(t)$) converge for this case rapidly and exponentially to the asymptotic & steady-state value (Table 6.3)

$$\overline{PA} = 1 - PA = 1 - AA = \lambda / (\lambda + \mu) = (\lambda / \mu) / (1 + \lambda / \mu) \lesssim \lambda / \mu .$$

To simplify considerations, it will be first assumed that the observed time interval $(0, t]$ is $\gg 1/\mu$, *terminates at the conclusion of a repair*, and exactly k (or n) failure-free times τ_i and repair times τ'_i have occurred. Furthermore, considering $\lambda \ll \mu$,

$$\overline{PA}_a = \lambda / \mu \tag{7.15}$$

is estimated instead of $\overline{PA} = \lambda / (\lambda + \mu)$ (absolute error less than $(\lambda / \mu)^2$). λ / μ is a probabilistic value of the asymptotic & steady-state unavailability and has his statistical counterpart in DT / UT , where DT and UT are the observed *down and up times*. The procedures developed in Appendices A8.2.2.4 and A8.3.1.4 are based on the fact that the quantity $\mu \cdot DT / \lambda \cdot UT$ has a *Fisher distribution (F-distribution)* with $\nu_1 = \nu_2 = 2k$ (or $2n$) degrees of freedom. Section 7.2.2.1 deals with estimation of \overline{PA}_a , Section 7.2.2.2 with demonstration of \overline{PA} . Alternative methods are discussed in Section 7.2.2.3.

7.2.2.1 Availability Estimation (Erlangian Failure-Free and/or Repair Times)

Having observed for an item good-as-new at $t=0$ and after each repair (Fig. 6.2), with constant failure & repair rates λ & μ , an operating time $UT = t_1 + \dots + t_k$ and a repair time $DT = t'_1 + \dots + t'_k$, the *maximum likelihood point estimate* for $\overline{PA}_a = \lambda / \mu$ is

$$\widehat{\overline{PA}}_a = (\hat{\lambda} / \hat{\mu}) = DT / UT = (t'_1 + \dots + t'_k) / (t_1 + \dots + t_k) . \tag{7.16}$$

DT / UT is biased, *unbiased* is $(1 - 1/k)DT / UT, k > 1$ (p. 555). $\overline{PA}_a = \lambda / \mu$ is an approximation for $\overline{PA} = \lambda / (\lambda + \mu)$, good for practical applications (abs. error $< (\lambda / \mu)^2$).

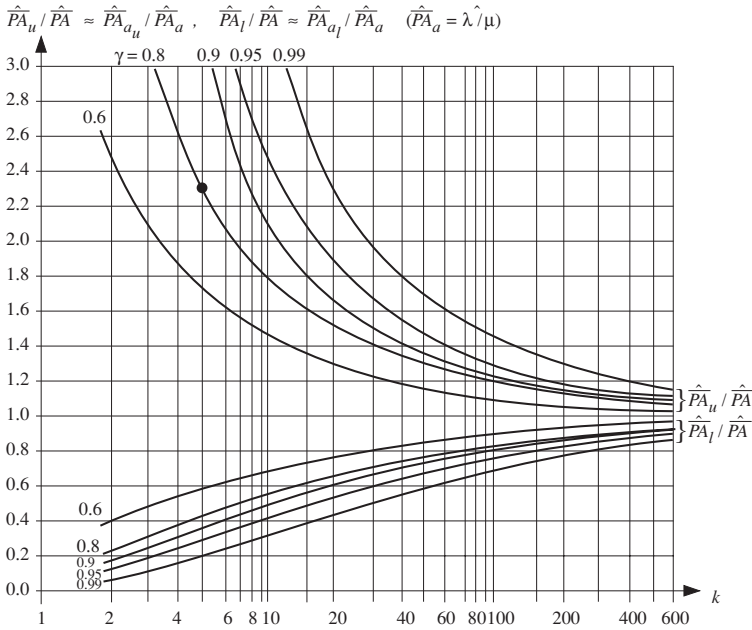


Figure 7.5 Confidence limits $\frac{\hat{P}A_u}{\hat{P}A} \approx \frac{\hat{P}A_{a_u}}{\hat{P}A_a}$ and $\frac{\hat{P}A_l}{\hat{P}A} \approx \frac{\hat{P}A_{a_l}}{\hat{P}A_a}$ per Eq.(7.17) for an unknown asymptotic & steady-state unavailability $\lambda/(\lambda+\mu) = PA = 1 - PA = 1 - AA = \frac{\hat{P}A_a}{(1+\lambda/\mu)}$, $\hat{P}A_a = DT/UT =$ maximum likelihood estimate for λ/μ , $UT = t_1 + \dots + t_k$, $DT = t'_1 + \dots + t'_k$, $\gamma = 1 - \beta_1 - \beta_2 =$ confidence level, here $\beta_1 = \beta_2 = (1 - \gamma)/2$ (• result for Example A8.8)

For given $\beta_1, \beta_2, \gamma = 1 - \beta_1 - \beta_2$ ($0 < \beta_1 < 1 - \beta_2 < 1$), lower $\hat{P}A_{a_l}$ and upper $\hat{P}A_{a_u}$ confidence limits for $\hat{P}A_a$ are given by (Eq. (A8.65))

$$\frac{\hat{P}A_{a_l}}{\hat{P}A_a} = \frac{\hat{P}A_a}{F_{2k, 2k, 1-\beta_2}} \quad \text{and} \quad \frac{\hat{P}A_{a_u}}{\hat{P}A_a} = \frac{\hat{P}A_a}{F_{2k, 2k, 1-\beta_1}}, \tag{7.17}$$

where $F_{2k, 2k, 1-\beta_2}$ and $F_{2k, 2k, 1-\beta_1}$ are the $1-\beta_2$ and $1-\beta_1$ quantiles of the Fisher (F -) distribution with $2k$ degrees of freedom (Appendix A9.4). $\frac{\hat{P}A_{a_l}}{\hat{P}A_a} \approx \frac{\hat{P}A_{a_u}}{\hat{P}A_a} \approx \frac{\hat{P}A_a}{\hat{P}A} = 1 + \lambda/\mu \approx 1$ can often be used. Figure 7.5 gives the confidence limits for $\beta_1 = \beta_2 = (1 - \gamma)/2$, useful for practical applications (Example A8.8). One sided confidence intervals are

$$0 \leq \overline{PA} \leq \frac{\hat{P}A_u}{u}, \quad \text{with } \gamma = 1 - \beta_1 \quad \text{and} \quad \frac{\hat{P}A_l}{l} \leq \overline{PA} < 1, \quad \text{with } \gamma = 1 - \beta_2. \tag{7.18}$$

Corresponding values for the availability can be obtained using $PA = 1 - \overline{PA}$.

If failure free and/or repair times are Erlangian distributed (Eq. (A6.102)) with $\beta_\lambda = n_\lambda$ & $\beta_\mu = n_\mu$, $F_{2k, 2k, 1-\beta_2}$ and $F_{2k, 2k, 1-\beta_1}$ have to be replaced by $F_{2kn_\lambda, 2kn_\mu, 1-\beta_2}$ and $F_{2kn_\lambda, 2kn_\mu, 1-\beta_1}$, for unchanged $MTTF$ & $MTTR$ (Example A8.11). Results based on the distribution of DT (Eq. (7.22)) are not free of parameters (Section 7.2.2.3).

7.2.2.2 Availability Demonstration (Erlangian Failure-Free and/or Repair Times)

In the context of an acceptance testing, *demonstration* of the asymptotic & steady-state point and average availability ($PA=AA$) is often required. The item is assumed as-good-as-new at $t=0$ and after each repair, and for practical applications it is useful to work with the unavailability $\overline{PA}=1-PA$. The main concern of this test is to check a *zero hypothesis* $H_0: \overline{PA} < \overline{PA}_0$ against an *alternative hypothesis* $H_1: \overline{PA} > \overline{PA}_1$ on the basis of the following agreement between producer and consumer:

Items should be accepted with a probability nearly equal to (but not less than) $1-\alpha$ if the true (unknown) unavailability \overline{PA} is lower than \overline{PA}_0 , but rejected with a probability nearly equal to (but not less than) $1-\beta$ if \overline{PA} is greater than \overline{PA}_1 ($\overline{PA}_0, \overline{PA}_1 > \overline{PA}_0, 0 < \alpha < 1-\beta < 1$ are given (fixed) values).

\overline{PA}_0 is the *specified* unavailability and \overline{PA}_1 is the *maximum acceptable* unavailability. α is the allowed *producer's risk* (type I error), i.e., the probability of *rejecting a true hypothesis* $H_0: \overline{PA} < \overline{PA}_0$. β is the allowed *consumer's risk* (type II error), i.e., the probability of *accepting the hypothesis* $H_0: \overline{PA} < \overline{PA}_0$ when the alternative hypothesis $H_1: \overline{PA} > \overline{PA}_1$ is true. Verification of the agreement stated above is a problem of statistical hypothesis testing (Appendix A8.3) and different approach are possible. In the following, the method developed in Appendix A8.3.1.4 is given (comparison with other methods is in Section 7.2.2.3).

Assuming constant failure and repair rates $\lambda(x) = \lambda$ and $\mu(x) = \mu$, the procedure is as follows (Eqs. (A8.91)-(A8.93), see also [A8.29, A2.6 (IEC 61070)]):

1. For given (fixed) $\overline{PA}_0, \overline{PA}_1, \alpha,$ and β ($0 < \alpha < 1-\beta < 1$), find the smallest integer n (1,2, ...) which satisfy (Eq. (A8.91))

$$F_{2n,2n,1-\alpha} \cdot F_{2n,2n,1-\beta} \leq \frac{\overline{PA}_1}{\overline{PA}_0} \cdot \frac{PA_0}{PA_1} = \frac{(1-PA_1)PA_0}{(1-PA_0)PA_1}, \quad (7.19)$$

where $F_{2n,2n,1-\alpha}$ and $F_{2n,2n,1-\beta}$ are the $1-\alpha$ & $1-\beta$ quantiles of the F -distribution with $2n$ degrees of freedom (Appendix A9.4), and compute the limiting value (Eq. (A8.92))

$$\delta = F_{2n,2n,1-\alpha} \overline{PA}_0 / PA_0 = F_{2n,2n,1-\alpha} (1-PA_0) / PA_0. \quad (7.20)$$

2. Observe n failure-free times t_1, \dots, t_n & corresponding repair times t'_1, \dots, t'_n , and
 - reject $H_0: \overline{PA} < \overline{PA}_0$, if $(t'_1 + \dots + t'_n) / (t_1 + \dots + t_n) > \delta$
 - accept $H_0: \overline{PA} < \overline{PA}_0$, if $(t'_1 + \dots + t'_n) / (t_1 + \dots + t_n) \leq \delta$. (7.21)

Table 7.2 gives n and δ for some values of $\overline{PA}_1 / \overline{PA}_0$ used in practical applications (Table A9.4, [A9.2, A9.3]). It must be noted that the test duration is *not fixed in advance*. However, results for fixed time sample plans are not free of parameters (remark to Eq.(7.22)). Values for the *availability* can be obtained using $PA=1-\overline{PA}$.

Table 7.2 Number n of failure-free times τ_1, \dots, τ_n & corresponding repair (restoration) times τ'_1, \dots, τ'_n , and limiting value δ of the observed ratio $(t'_1 + \dots + t'_n) / (t_1 + \dots + t_n)$ to demonstrate $\overline{PA} < \overline{PA}_0$ against $\overline{PA} > \overline{PA}_1$ for various values of α (producer risk), β (consumer risk), and $\overline{PA}_1 / \overline{PA}_0$

	$\overline{PA}_1 / \overline{PA}_0 = 2$ ($PA_0 > 1/2$)***	$\overline{PA}_1 / \overline{PA}_0 = 4$ ($PA_0 > 3/4$)***	$\overline{PA}_1 / \overline{PA}_0 = 6$ ($PA_0 > 5/6$)***
$\alpha \approx \beta \approx 0.1$	$n = 29^*$ $\delta = 1.41 \overline{PA}_0 / PA_0$	$n = 8^*$ $\delta = 1.93 \overline{PA}_0 / PA_0$	$n = 5^{**}$ $\delta = 2.32 \overline{PA}_0 / PA_0$
$\alpha \approx \beta \approx 0.2$	$n = 13^*$ $\delta = 1.39 \overline{PA}_0 / PA_0$	$n = 4^{**}$ $\delta = 1.86 \overline{PA}_0 / PA_0$	$n = 3^*$ $\delta = 2.06 \overline{PA}_0 / PA_0$

* a lower n as per Eq. (7.19) can be given (with corresponding δ per Eq. (7.20)) for $PA_0 \leq 0.99$;
 ** same as * for $PA_0 < 0.98$; *** given by $0 < PA_0, PA_1 < 1$

If failure free and/or repair times are Erlangian distributed (Eq. (A6.102)) with $\beta_\lambda = n_\lambda$ & $\beta_\mu = n_\mu$, $F^{2n, 2n, 1-\alpha}$ and $F^{2n, 2n, 1-\beta}$ have to be replaced by $F^{2n \cdot n_\mu, 2n \cdot n_\lambda, 1-\alpha}$ and $F^{2n \cdot n_\lambda, 2n \cdot n_\mu, 1-\beta}$, for unchanged *MTTF* & *MTTR* (Example A8.11). Results based on the distribution of *DT* (Eq. 7.22) are not parameter free (Section 7.2.2.3).

7.2.2.3 Further Availability Evaluation Methods for Continuous Operation

The approach developed in Appendices A8.2.2.4 & A8.3.1.4 and given in Sections 7.2.2.1 & 7.2.2.2 yields to exact solutions based on the *Fisher distribution* for estimating and demonstrating an availability $PA=AA$, obtained by investigating *DT/UT* for exponentially or Erlangian distributed failure-free and/or repair times. Exponentially distributed failure-free times can be assumed in many practical applications. The distribution of repair (restoration) times can often be approximated by an Erlang distribution (Eq. (A6.102)) with $\beta \geq 3$. Generalization of the distribution of failure-free or repair times can lead to difficulties. In the following some alternative approaches for estimating and demonstrating an availability $PA=AA$ are briefly discussed and compared with the approach given in Sections 7.2.2.1 & 7.2.2.2 (item's behavior still described by an alternating renewal process as per Fig. 6.2)).

A first possibility is to consider only the distribution of the down time *DT* (total repair or restoration time) in a given time interval $(0, t]$. At the given (fixed) time point t the item can be up or down, and Eq. (6.33) with $t-x$ instead of T_0 gives the distribution function of *DT* (Eq. (7.22)). Moments of *DT* have been investigated in [A7.29(1957)], mean and variance of the unavailability $\overline{PA} = 1 - PA = E[DT/t]$ can thus be given for arbitrary distributions of failure-free and repair times. In particular, for the case of constant failure and repair rates ($\lambda(x)=\lambda, \mu(x)=\mu$) it holds that

$$\begin{aligned} & \Pr \{ \text{total down time } DT \text{ in } (0, t] \leq x \mid \text{new at } t=0 \} = \\ & \Pr \{ DT/t \leq x/t \mid \text{new at } t=0 \} = 1 - e^{-(\lambda(t-x)+\mu x)} \sum_{n=1}^{\infty} \left(\frac{\lambda(t-x)^n}{n!} \sum_{k=0}^{n-1} \frac{(\mu x)^k}{k!} \right), \quad 0 < x < t, \\ & \lim_{t \rightarrow \infty} E[DT/t] = \frac{\lambda}{\lambda + \mu} \approx \lambda/\mu, \quad \text{and} \quad \lim_{t \rightarrow \infty} \text{Var}[DT/t] = \frac{2\lambda\mu}{t(\lambda + \mu)^3} \approx 2\lambda/t\mu^2. \quad (7.22) \end{aligned}$$

However, already for the case of constant failure and repair rates, results for interval estimation and demonstration test are not free of parameters (function of μ [A8.29] or λ [A8.18]). The use of the distribution of DT , or DT/t for fixed t , would bring the advantage of a test duration t fixed in advance, but results are not free of parameters and the method is thus of limited utility.

A second possibility is to assign to the state of the item an indicator $\zeta(t)$ taking values 1 for item up and 0 for item down (binary process, Boolean variable). In this case it holds that $PA(t) = \Pr\{\zeta(t)=1\}$, and thus $E[\zeta(t)] = PA(t)$ and $\text{Var}[\zeta(t)] = E[\zeta(t)^2] - E^2[\zeta(t)] = PA(t)(1 - PA(t))$ (Eq. (A6.118)). Investigation on $PA(t)$ reduces to that on $\zeta(t)$, see e. g. [A7.4(1962)]. In particular, estimation and demonstration of $PA(t)$ can be based on observations of $\zeta(t)$ at time points $t_1 < t_2 < \dots$. A basic question here, is the choice of the observation time points (randomly, at constant time intervals $\Delta = t_{i+1} - t_i$, or other). For the case of constant failure & repair rates (λ & μ), $PA(t)$ convergence rapidly to $PA = AA = \mu/(\lambda + \mu) \approx 1 - \lambda/\mu$. (Eq. (6.20)). Furthermore, because of the *constant failure rate*, the joint availability is given by (Eqs. (6.35)) $JA_{S0}(t, t + \Delta) = PA_{S0}(t) \cdot PA_{S0}(\Delta)$, relation which can be extended to an arbitrary number of observation points (Eq. (A6.9)). Estimation and demonstration for the case of observations at constant time intervals Δ can thus be reduced to the case of an *unknown probability* $p = \overline{PA}(\Delta) = 1 - PA(\Delta) \approx (1 - e^{-\mu\Delta})\lambda/\mu$ as per Eq. (6.20), yielding $p \approx \lambda\Delta$ for $\Delta \ll 1/\mu$ or $p \approx \lambda/\mu$ for $\Delta \gg 1/\mu$ (Section 7.1).

A further possibility is to estimate and demonstrate λ & μ *separately* (Eqs. (7.28)-(7.30) and (7.33)-(7.35)), and consider $\overline{PA} = \overline{AA} \approx \lambda/\mu$.

A one-sided interval estimation $\overline{PA} = \overline{AA} \approx \lambda/\mu \leq \hat{PA}_u$ for an item described by Fig. 6.2 and Eq. (7.22), using the Chebyshev's inequality (Eqs. (A6.49)) in the form $\Pr\{|DT/t - \lambda/\mu| > \varepsilon\} \leq 2\lambda/(t\mu^2\varepsilon^2) = \beta_1 = 1 - \gamma$, i.e. for $\varepsilon = \sqrt{2\lambda/t\mu^2(1-\gamma)}$, has been proposed in [7.14]. This leads to $\Pr\{DT/t > \lambda/\mu + \varepsilon\} \leq 1 - \gamma$, or $\Pr\{DT/t \leq \lambda/\mu + \varepsilon\} \geq \gamma$; thus, $\Pr\{\overline{PA} \leq \hat{PA}_u\} \geq \gamma$ with $\hat{PA}_u = \hat{\lambda}/\hat{\mu} + \sqrt{2\hat{\lambda}/t\hat{\mu}^2(1-\gamma)}$, t as test time, and $\hat{\lambda}$ & $\hat{\mu}$ estimates for λ & μ (Eqs. (7.28), (7.23)-(7.25) as appropriate).

The different methods can basically be discussed by comparing Figs. 7.5 & 7.6 and Tables 7.2 & 7.3. Analytical results based on the Fisher distribution yield broader confidence intervals and longer demonstration tests (which can be partly compensated by accepting higher values for $\overline{PA}_u/\overline{PA}_l$ or $\overline{PA}_1/\overline{PA}_0$, considering the low values of \overline{PA} and that λ & μ are unknown); the advantage being an exact knowledge of the involved errors (β_1, β_2) or risks (α, β). However, for some aspects (test duration, possibility to verify maintainability with selected failures) it can become more appropriate to estimate and demonstrate λ & μ separately.

7.2.3 Estimation & Demonstration of a Constant Failure Rate λ (or of *MTBF* for the Case $MTBF = 1/\lambda$)

A constant (time independent) failure rate $\lambda(x)=\lambda$ occurs in many practical applications for nonrepairables items, as well as for *repairable items which are assumed as-good-as-new after repair*, x being the variable starting by $x=0$ at the beginning of the failure-free time considered (as for *interarrival times*, pp.5-6, 41, 378, 380). $\lambda(x)=\lambda$ implies that failure-free times are independent and exponentially distributed with the same parameter λ (Eq.(A6.81)). In this case, the reliability function is given by $R(x) = e^{-\lambda x}$ and for the mean time to failure, $MTTF = 1/\lambda$ holds for all failure-free times (Eq. (A6.84)). If the repair time is not negligible, *MTBF* (mean operating time between failures) is used instead of *MTTF*. However,

*considering that to give a sense to an MTBF, the repaired item must be as-good-as-new after each repair, $\lambda(x)=\lambda$ yields $MTBF=1/\lambda$; also because of the statistical estimate $M\hat{T}BF=T/k$ used in practical applications (p.318), and to avoid misuses, *MTBF* is confined in this book to the case of repairable items with $\lambda(x)=\lambda$.(see also the remarks on pp. 6 & 380).*

A reason for assuming $\lambda(x)=\lambda$ is that by neglecting renewal times (for repair or replacement at failure), i. e. by considering only operating times, *the flow of failures constitute a homogeneous Poisson process* (p. 472). This property characterizes exponentially distributed failure-free times and *highly simplifies investigations*.

This section deals with estimation and demonstration of a constant failure rate λ , or of *MTBF* for the case $MTBF=1/\lambda$ (see Sections 7.5-7.7 for further results). In particular, the case of a *given* (fixed) *cumulative operating time* T , obtained with one or more statistically identical and independent items which are as-good-as-new after each repair or replacement at failure, is considered (footnote on p. 318). Due to the relationship between exponentially distributed failure-free times and the homogeneous Poisson process (Eq. (A7.39)) as well as the additive property of Poisson processes (Example 7.7),

for constant failure rate $\lambda(x)=\lambda$, the fixed cumulative operating time T can be partitioned in an arbitrary way from failure-free times of statistically identical and independent items,

see note to Table 7.3 for a practical rule. Following are two basic situations:

1. Operation of a single item immediately renewed at failure, here $T=t$.
2. Operation of n identical items, each of them being immediately renewed at failure, here, $T = nt$ ($n = 1, 2, \dots$).

As stated above, for constant failure rate $\lambda(x)=\lambda$ and immediate renewal, the failure process is a homogeneous Poisson process with intensity λ for $n=1$, or $n\lambda$ for $n>1$, over the fixed time interval $(0, T]$ for $n=1$, or $(0, T/n]$ for $n>1$. Hence, the probability for k failures within the cumulative operating time T is (Eq. (A7.41))

$$\Pr\{k \text{ failures within } T \mid \lambda\} = \Pr\{k \text{ failures within } T/n \mid n\lambda\} = \frac{(\lambda T)^k}{k!} e^{-\lambda T}, \quad \begin{matrix} k=0,1,\dots, \\ n=1,2,\dots \end{matrix}$$

Statistical procedures for the estimation and demonstration of a failure rate λ can thus be based on the evaluation of the parameter ($m = \lambda T$) of a *Poisson distribution*.

In addition to the case of a given (fixed) cumulative operating time T (with immediate renewal), discussed above and investigated in Sections 7.2.3.1–7.2.3.3, for which the number k of failures in T is a sufficient statistic and $\hat{\lambda} = k/T$ is an unbiased estimate for λ , further possibilities are known. Assuming n identical items at $t=0$ and labeling the *individual failure times* as $t_1 < t_2 < \dots$, measured from $t=0$, also following censoring cases can occur in practical applications ($k > 1$):

1. *Fixed number k of failures*, the test is stopped at the k th failure and failed items are *not renewed*; an unbiased point estimate of the failure rate λ is (Eq (A8.35))

$$\begin{aligned} \hat{\lambda} &= (k-1)/[nt_1 + (n-1)(t_2 - t_1) + \dots + (n-k+1)(t_k - t_{k-1})] \\ &= (k-1)/[t_1 + \dots + t_k + (n-k)t_k]. \end{aligned} \quad (7.23)$$

2. *Fixed number k of failures*, the test is stopped at the k th failure and failed items are *instantaneously renewed*; an unbiased point estimate for λ is

$$\hat{\lambda} = (k-1)/(nt_1 + n(t_2 - t_1) + \dots + n(t_k - t_{k-1})) = (k-1)/nt_k. \quad (7.24)$$

3. *Fixed test time T_{test}* , failed items are *not renewed*; a biased point estimate of the failure rate λ (given k items have failed in $(0, T_{test}]$) is

$$\hat{\lambda} = k/[nt_1 + (n-1)(t_2 - t_1) + \dots + (n-k)(T_{test} - t_k)] = k/[t_1 + \dots + t_k + (n-k)T_{test}]. \quad (7.25)$$

Example 7.7

An item with constant failure rate λ operates first for a fixed time T_1 and then for a fixed time T_2 . Repair times are neglected. Give the probability that k failures will occur in $T = T_1 + T_2$.

Solution

The item's behavior within each of the time periods T_1 and T_2 can be described by a homogeneous Poisson process with intensity λ . From Eq. (A7.39) it follows that

$$\Pr\{i \text{ failures in the time period } T_1 \mid \lambda\} = \frac{(\lambda T_1)^i}{i!} e^{-\lambda T_1}$$

and, because of the *memoryless property* of the homogeneous Poisson process

$$\begin{aligned} \Pr\{k \text{ failures in } T = T_1 + T_2 \mid \lambda\} &= \sum_{i=0}^k \frac{(\lambda T_1)^i}{i!} e^{-\lambda T_1} \cdot \frac{(\lambda T_2)^{k-i}}{(k-i)!} e^{-\lambda T_2} \\ &= e^{-\lambda T} \lambda^k \sum_{i=0}^k \frac{T_1^i}{i!} \cdot \frac{T_2^{k-i}}{(k-i)!} = \frac{(\lambda T)^k}{k!} e^{-\lambda T}. \end{aligned} \quad (7.26)$$

The last part of Eq. (7.26) follows from the binomial expansion of $(T_1 + T_2)^k$. Eq. (7.26) shows that for λ constant, the *cumulative operating time* T can be partitioned in an *arbitrary way from failure-free times of statistically identical and independent items* (see note to Table 7.3 for a rule).

Supplementary result: The same procedure can be used to prove that the *sum of two independent homogeneous Poisson processes* with intensities λ_1 and λ_2 is a homogeneous *Poisson process* with intensity $\lambda_1 + \lambda_2$; in fact,

$$\begin{aligned} & \Pr\{k \text{ failures in } (0, T] \mid \lambda_1, \lambda_2\} \\ &= \sum_{i=0}^k \frac{(\lambda_1 T)^i}{i!} e^{-\lambda_1 T} \frac{(\lambda_2 T)^{k-i}}{(k-i)!} e^{-\lambda_2 T} = \frac{((\lambda_1 + \lambda_2) T)^k}{k!} e^{-(\lambda_1 + \lambda_2) T}. \end{aligned} \tag{7.27}$$

This result can be extended to *nonhomogeneous Poisson processes*.

7.2.3.1 Estimation of a Constant Failure Rate λ (or of MTBF for $MTBF = 1/\lambda$)⁺⁾

Let us consider an item with a constant failure rate $\lambda(x) = \lambda$. If during the *given* (fixed) *cumulative operating time* T ⁺⁾ exactly k failures have occurred, the maximum likelihood *point estimate* for the unknown parameter λ follows as (Eq. (A8.46))

$$\hat{\lambda} = \frac{k}{T}, \quad k = 0, 1, 2, \dots, \quad E[\hat{\lambda}] = \lambda, \quad \text{Var}[\hat{\lambda}] = \lambda / T. \tag{7.28}$$

$\hat{\lambda} = k / T$ is unbiased, i.e. $E[\hat{\lambda}] = \lambda$ and k is a sufficient statistic (Appendix A8.2.1). Furthermore, $\text{Var}[\hat{\lambda}] = \text{Var}[k] / T^2 = \lambda / T$ (Eqs. (A6.128), (A6.40), (A6.46)). For a given *confidence level* $\gamma = 1 - \beta_1 - \beta_2$ ($0 < \beta_1 < 1 - \beta_2 < 1$) and $k > 0$, lower $\hat{\lambda}_l$ and upper $\hat{\lambda}_u$ limits of the *confidence interval* for λ can be obtained from (Eqs. (A8.47) - (A8.51))

$$\sum_{i=k}^{\infty} \frac{(\hat{\lambda}_l T)^i}{i!} e^{-\hat{\lambda}_l T} = \beta_2 \quad \text{and} \quad \sum_{i=0}^k \frac{(\hat{\lambda}_u T)^i}{i!} e^{-\hat{\lambda}_u T} = \beta_1, \tag{7.29}$$

or from

$$\hat{\lambda}_l = \frac{\chi_{2k, \beta_2}^2}{2T} \quad \text{and} \quad \hat{\lambda}_u = \frac{\chi_{2(k+1), 1-\beta_1}^2}{2T}, \tag{7.30}$$

using the quantile of the χ^2 -distribution (Table A9.2). For $k = 0$, Eq. (A8.49) yields

$$\hat{\lambda}_l = 0 \quad \text{and} \quad \hat{\lambda}_u = \ln(1/\beta_1) / T, \quad \text{with } \gamma = 1 - \beta_1. \tag{7.31}$$

Figure 7.6 gives confidence limits $\hat{\lambda}_l / \hat{\lambda}$ & $\hat{\lambda}_u / \hat{\lambda}$ for $\beta_1 = \beta_2 = (1 - \gamma) / 2$, with $\hat{\lambda} = k / T$, useful for practical applications.

For the case $MTBF = 1/\lambda$, $M\hat{T}BF = T / k$, $k \geq 1$, is *biased*; unbiased is, for $\lambda T \gg 1$, $M\hat{T}BF = T / (k + 1)$ ($E[T / (k + 1)] = (1 - e^{-\lambda T}) / \lambda$, Eqs. (A6.40), (A6.39), (A7.41)). For practical applications, $M\hat{T}BF_l \approx 1 / \hat{\lambda}_u$ and $M\hat{T}BF_u \approx 1 / \hat{\lambda}_l$ can often be used.

⁺⁾ The case considered in Sections 7.2.3.1-7.2.3.3 corresponds to a sampling plan with $n \geq 1$ statistically identical & independent items and k failures in the given (fixed, cumulative) operating time T (T is often considered as time interval $(0, t = T/n]$ by assuming *immediate* repair or replacement to as-good-as-new of failed elements, yielding a homogeneous Poisson process (HPP) with intensity $n\lambda$ as flow of failures); fixed T (or $t = T/n$) is known as Type 1 (time) censoring.

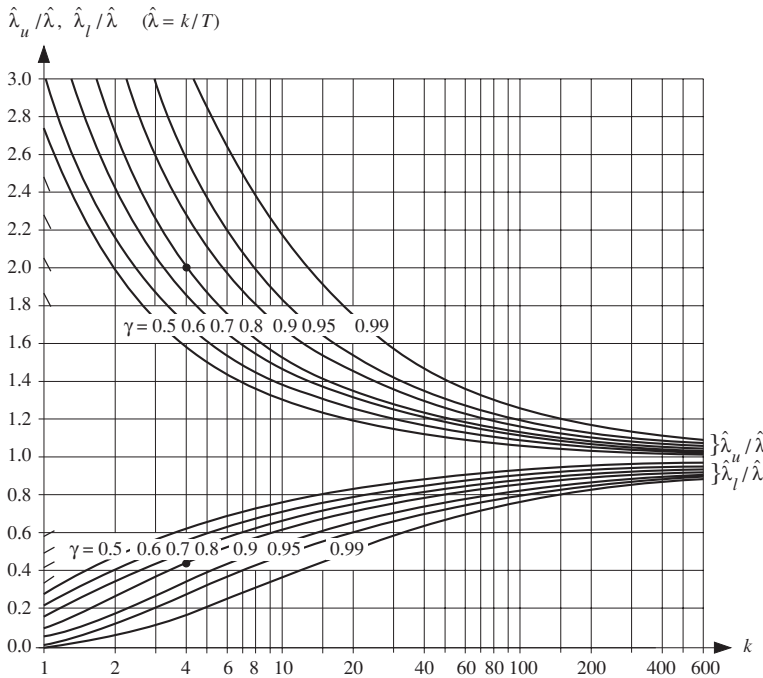


Figure 7.6 Confidence limits $\hat{\lambda}_l / \hat{\lambda}$, $\hat{\lambda}_u / \hat{\lambda}$ for an unknown constant failure rate λ per Eqs. (7.28) & (7.29), T =given (fixed) cumulative operating time (time censoring), k = number of failures during T ($k \geq 1$), $\gamma = 1 - \beta_1 - \beta_2$ = confidence level, here $\beta_1 = \beta_2 = (1 - \gamma) / 2$ (see footnote on p. 318; for $MTBF = 1/\lambda$, $\hat{MTBF}_l \approx 1/\hat{\lambda}_u$ & $\hat{MTBF}_u \approx 1/\hat{\lambda}_l$ can often be used; • result for Examples 7.8, 7.13)

Confidence limits $\hat{\lambda}_l, \hat{\lambda}_u$ can also be used to give one-sided confidence intervals:

or

$$\begin{aligned}
 0 \leq \lambda \leq \hat{\lambda}_u & \quad \text{with } \beta_2 = 0 \quad \text{and } \gamma = 1 - \beta_1, \\
 \lambda \geq \hat{\lambda}_l & \quad \text{with } \beta_1 = 0 \quad \text{and } \gamma = 1 - \beta_2,
 \end{aligned}
 \tag{7.32}$$

For practical applications, $MTBF \geq \hat{MTBF}_l \approx 1/\hat{\lambda}_u$ & $MTBF \leq \hat{MTBF}_u \approx 1/\hat{\lambda}_l$ can often be used, for the case $MTBF = 1/\lambda$.

Example 7.8

In testing a subassembly with constant failure rate λ , 4 failures occur during $T = 10^4$ cumulative operating hours (footnote on p. 318). Find the confidence interval for λ for a confidence level $\gamma = 0.8$ ($\beta_1 = \beta_2 = 0.1$).

Solution

From Fig. 7.6 it follows that for $k=4$ and $\gamma=0.8$, $\hat{\lambda}_l / \hat{\lambda} \approx 0.44$ and $\hat{\lambda}_u / \hat{\lambda} \approx 2.0$. With $T = 10^4$ h, $k = 4$, and $\hat{\lambda} = 4 \cdot 10^{-4} \text{ h}^{-1}$, the confidence limits are $\hat{\lambda}_l \approx 1.7 \cdot 10^{-4} \text{ h}^{-1}$ and $\hat{\lambda}_u \approx 8 \cdot 10^{-4} \text{ h}^{-1}$.

Supplementary result: Corresponding one-sided conf. interval is $\lambda \leq 8 \cdot 10^{-4} \text{ h}^{-1}$ with $\gamma = 0.9$.

In the above considerations (Eqs. (7.28) - (7.32)), the *cumulative operating time* T was given (fixed), independent of the individual failure-free times and the number n of items involved (*Type I* (time) *censoring*, see also the footnote on p. 318). The situation is different when *the number of failures* k is given (fixed), i. e., when the test is stopped at the occurrence of the k h failure (*Type II* (failure) *censoring*). Here, the cumulative operating time is a *random variable* (term $(k-1)/\hat{\lambda}$ of Eqs. (7.23)&(7.24)). Using the memoryless property of homogeneous Poisson processes, it can be shown that the quantities $(t_i - t_{i-1}), i=1, 2, \dots, k, t_0=0$, are independent observations of exponentially distributed random variables with parameters $n\lambda$ for Eq. (7.24) and $(n-i+1)\lambda$ for Eq.(7.23), respectively. This is necessary and sufficient to prove that the $\hat{\lambda}$ given by Eqs.(7.23) and (7.24) are maximum likelihood estimates for λ . For confidence intervals, results of Appendix A8.2.2.3 can be used.

In some practical applications, *system's* failure rate confidence limits as a function of *component's* failure rate confidence limits is asked. Monte Carlo simulation can help. However, for a series system with n elements, *constant failure rates* $\lambda_1, \dots, \lambda_n$, time censoring, and same observation time T , Eqs. (2.19), (7.28) & (7.27) yield $\hat{\lambda}_S = \hat{\lambda}_1 + \dots + \hat{\lambda}_n$. Furthermore, for given fixed T , $2T\lambda_i$ (considered here as random variable, Appendix A8.2.2.2) has a χ^2 -distribution with $2(k_i+1)$ degrees of freedom (Eqs. (A8.48) & (A8.51), Table A9.2); thus, $2T\lambda_S$ has a χ^2 -distribution with $\Sigma 2(k_i+1)$ degrees of freedom (Appendix A9.2, Example A6.15). From this, and considering the shape of the χ^2 -distribution (Tab. A9.2, [A9.2, A9.3]), it holds that $\Pr\{\lambda_S \leq \hat{\lambda}_{1u} + \dots + \hat{\lambda}_{nu}\} \geq \gamma$, with $\hat{\lambda}_{iu}$ (upper limit of the confidence interval for λ_i) obtained from $\Pr\{2T\lambda_i \leq 2T\hat{\lambda}_{iu}\} = \Pr\{\lambda_i \leq \hat{\lambda}_{iu}\} = \gamma > 0.7, i=1, \dots, n$. Extensions to different observation times T_i , series-parallel structures, and Erlangian distributed failure-free times are investigated e. g. in [7.17]. Estimation of λ/μ as approximation for an unavailability $\lambda/(\lambda+\mu)$ is discussed in Section 7.2.2.1.

7.2.3.2 Simple Two-sided Test for the Demonstration of a Constant Failure Rate λ (or of *MTBF* for the case $MTBF = 1/\lambda$)^{†)}

In the context of an *acceptance test*, demonstration of a constant failure rate λ (or of *MTBF* for the case $MTBF = 1/\lambda$) is often required, not merely its estimation as in Section 7.2.3.1. The main concern of this test is to check a zero hypothesis $H_0: \lambda < \lambda_0$ against an alternative hypothesis $H_1: \lambda > \lambda_1$, on the basis of the following agreement between producer and consumer:

Items should be accepted with a probability nearly equal to (but not less than) $1-\alpha$ if the true (unknown) failure rate λ is less than λ_0 , but rejected with a probability nearly equal to (but not less than) $1-\beta$ if λ is greater than λ_1 ($\lambda_0, \lambda_1 > \lambda_0$, and $0 < \alpha < 1-\beta < 1$ are given (fixed) values).

^{†)} See footnote on p. 318.

λ_0 is the *specified* λ and λ_1 is the *maximum acceptable* λ ($1/m_0$ and $1/m_1$ in IEC 61614 [7.19] or $1/\theta_0$ and $1/\theta_1$ in MIL-HDBK-781 [7.23] for the case $MTBF=1/\lambda$). α is the allowed *producer's risk* (type I error), i.e., the probability of rejecting a true hypothesis $H_0: \lambda < \lambda_0$. β is the allowed *consumer's risk* (type II error), i.e., the probability of accepting H_0 when the alternative hypothesis $H_1: \lambda > \lambda_1$ is true. Evaluation of the above agreement is a problem of statistical hypothesis testing (Appendix A8.3), and can be performed e. g. with a *simple two-sided test* or a *sequential test*.

With the *simple two-sided test* (also known as the *fixed length test*), the cumulative operating time T (footnote on p. 318) and the number of allowed failure c during T are fixed quantities. The procedure (test plan) follows in a way similar to that developed in Appendix A8.3.1.1 as:

1. From $\lambda_0, \lambda_1, \alpha, \beta$ determine the smallest integer c and the value T satisfying

$$\sum_{i=0}^c \frac{(\lambda_0 T)^i}{i!} e^{-\lambda_0 T} \geq 1 - \alpha \tag{7.33}$$

and

$$\sum_{i=0}^c \frac{(\lambda_1 T)^i}{i!} e^{-\lambda_1 T} \leq \beta. \tag{7.34}$$

2. Perform a test with a total *cumulative operating time* T (see footnote on p. 318), determine the number of failures k during the test, and

- reject $H_0: \lambda < \lambda_0$, if $k > c$
 - accept $H_0: \lambda < \lambda_0$, if $k \leq c$.
- (7.35)

For the case $MTBF=1/\lambda$, the above procedure can be used to test $H_0: MTBF > MTBF_0$ against $H_1: MTBF < MTBF_1$, by replacing $\lambda_0=1/MTBF_0$ and $\lambda_1=1/MTBF_1$.

Example 7.9

Following conditions have been specified for the demonstration (acceptance test) of the constant (time independent) failure rate λ of an assembly: $\lambda_0 = 1/2000$ h (specified λ), $\lambda_1 = 1/1000$ h (minimum acceptable λ), producer risk $\alpha = 0.2$, consumer risk $\beta = 0.2$. Give: (i) the cumulative test time T and the allowed number of failures c during T ; (ii) the probability of acceptance if the true failure rate λ were $1/3000$ h.

Solution

- (i) From Fig. 7.3, $c = 6$ and $m \approx 4.6$ for $\Pr\{\text{acceptance}\} \approx 0.82$, $c = 6$ and $m \approx 9.2$ for $\Pr\{\text{acceptance}\} \approx 0.19$ (see Example 7.2 for the procedure); thus $c = 6$ and $T \approx 9200$ h. These values agree well with those obtained from Table A9.2 ($v=14$), as given also in Table 7.3.
- (ii) For $\lambda = 1/3000$ h, $T = 9200$ h, $c = 6$

$$\Pr\{\text{acceptance} \mid \lambda = 1/3000 \text{ h}\} = \Pr\{\text{no more than 6 failures in } T = 9200 \text{ h} \mid \lambda = 1/3000 \text{ h}\} = \sum_{i=0}^6 \frac{3.07^i}{i!} e^{-3.07} \approx 0.96,$$

see also Fig. 7.3 for $m = 3.07$ and $c = 6$.

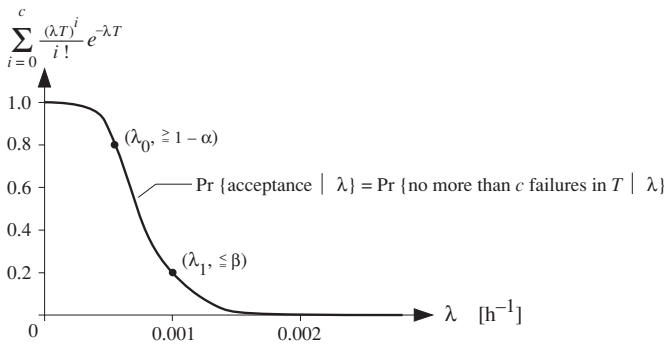


Figure 7.7 Operating characteristic curve (acceptance probability curve) as a function of the constant failure rate λ for $\lambda_0 = 1/2000\text{h}$, $\lambda_1 = 1/1000\text{h}$, $\alpha \approx \beta \approx 0.2$; $T = 9200\text{h}$ and $c = 6$ as per Table 7.3, see also Fig. 7.3 (holds for $MTBF_0 = 2000\text{h}$ and $MTBF_1 = 1000\text{h}$, for the case $MTBF = 1/\lambda$)

The graph of Fig. 7.7 visualizes the validity of the above agreement between producer and consumer (customer). It satisfies the inequalities (7.33) and (7.34), and is known as *operating characteristic curve* (or acceptance probability curve). For each value of λ , it gives the probability of having not more than c failures during a cumulative operating time T . Considering that, for constant failure rate the operating characteristic curve as a function of λ is strictly decreasing, the risk for a false decision decreases for $\lambda < \lambda_0$ and $\lambda > \lambda_1$, respectively. It can be shown that the quantities c and $\lambda_0 T$ only depend on α , β , and the ratio λ_1/λ_0 (*discrimination ratio*).

Table 7.3 gives c and $\lambda_0 T$ for some values of α , β and λ_1/λ_0 useful for practical applications. For the case $MTBF = 1/\lambda$, Table 7.3 holds for testing $H_0: MTBF > MTBF_0$ against $H_1: MTBF < MTBF_1$, by setting $\lambda_0 = 1/MTBF_0$ and $\lambda_1 = 1/MTBF_1$. Table 7.3 can also be used for the demonstration of an *unknown probability p* (Eqs. (7.8) and (7.9)) in the case where the *Poisson approximation* applies. A large number of test plans are in *international standards* [7.19 (61124)].

In addition to the simple two-sided test described above, a *sequential test* is often used (see Appendix A8.3.1.2 & Section 7.1.2.2 for an introduction and Fig. 7.8 for an example). In this test, neither the cumulative operating time T (footnote on p. 318), nor the number c of allowed failures during T are specified before the test begins;

the number of failures is recorded as a function of the (running) cumulative operating time (normalized to $1/\lambda_0$), and the test is stopped as soon as the resulting staircase curve crosses the acceptance line or the rejection line.

Sequential tests offer the advantage that the test duration is on average shorter than with simple two-sided tests. Using Eq. (7.12) with $p_0 = 1 - e^{-\lambda_0 \delta t}$, $p_1 = 1 - e^{-\lambda_1 \delta t}$, $n = T/\delta t$, and $\delta t \rightarrow 0$ (continuous in time), the acceptance and rejection lines are

Table 7.3 Number of allowed failures c during the cumulative operating time T (footnote on p. 318) and value of $\lambda_0 T$ to demonstrate $\lambda < \lambda_0$ against $\lambda > \lambda_1$ for various values of α (producer risk), β (consumer risk), and λ_1 / λ_0 (can be used to test $MTBF < MTBF_0$ against $MTBF > MTBF_1$ for the case $MTBF = 1/\lambda$ or, using $\lambda_0 T = n p_0$, to test $p < p_0$ against $p > p_1$ for an unknown probability $p \ll 1$)

	$\lambda_1 / \lambda_0 = 1.5$	$\lambda_1 / \lambda_0 = 2$	$\lambda_1 / \lambda_0 = 3$
$\alpha \approx \beta \approx 0.1$	$c = 40$ $\lambda_0 T \approx 32.98$ ($\alpha \approx \beta \approx 0.098$)	$c = 14^*$ $\lambda_0 T \approx 32.98$ ($\alpha \approx \beta \approx 0.098$)	$c = 5$ $\lambda_0 T \approx 3.12$ ($\alpha \approx \beta \approx 0.096$)
$\alpha \approx \beta \approx 0.2$	$c = 17$ $\lambda_0 T \approx 14.33$ ($\alpha \approx \beta \approx 0.197$)	$c = 6$ $\lambda_0 T \approx 4.62$ ($\alpha \approx \beta \approx 0.185$)	$c = 2$ $\lambda_0 T \approx 1.47$ ($\alpha \approx \beta \approx 0.184$)
$\alpha \approx \beta \approx 0.3$	$c = 6$ $\lambda_0 T \approx 5.41$ ($\alpha \approx \beta \approx 0.2997$)	$c = 2$ $\lambda_0 T \approx 1.85$ ($\alpha \approx \beta \approx 0.284$)	$c = 1$ $\lambda_0 T \approx 0.92$ ($\alpha \approx \beta \approx 0.236$)

number of items under test $\approx T\lambda_0$, as a rule of thumb; * $c=13$ yields $\lambda_0 T=9.48$ and $\alpha=\beta=0.1003$

• acceptance line : $y_1(x) = ax - b_1$, (7.36)

• rejection line : $y_2(x) = ax + b_2$, (7.37)

with $x = \lambda_0 \delta t \cdot T / \delta t = \lambda_0 T$, T = running cumulative operating time (footnote on p. 318), and

$$a = \frac{(\lambda_1 / \lambda_0) - 1}{\ln(\lambda_1 / \lambda_0)}, \quad b_1 = \frac{\ln(1 - \alpha) / \beta}{\ln(\lambda_1 / \lambda_0)}, \quad b_2 = \frac{\ln(1 - \beta) / \alpha}{\ln(\lambda_1 / \lambda_0)}. \tag{7.38}$$

Sequential tests used in practical applications are given in *international standards* [7.19 (61124)]. To limit testing effort, restrictions are often placed on the test duration and the number of allowed failures. Figure 7.8 shows two *truncated sequential test plans* for $\alpha \approx \beta \approx 0.2$ and $\lambda_1 / \lambda_0 = 1.5$ and 2, respectively. The lines defined by Eqs. (7.36)-(7.38) are shown dashed in Fig. 7.8a.

Example 7.10

Continuing with Example 7.9, give the expected test duration by assuming that the true λ equals λ_0 and a sequential test as per Fig. 7.8 is used.

Solution

From Fig. 7.8 with $\lambda_1 / \lambda_0 = 2$ it follows that $E[\text{test duration} \mid \lambda = \lambda_0] \approx 2.4 / \lambda_0 = 4800 \text{ h}$.

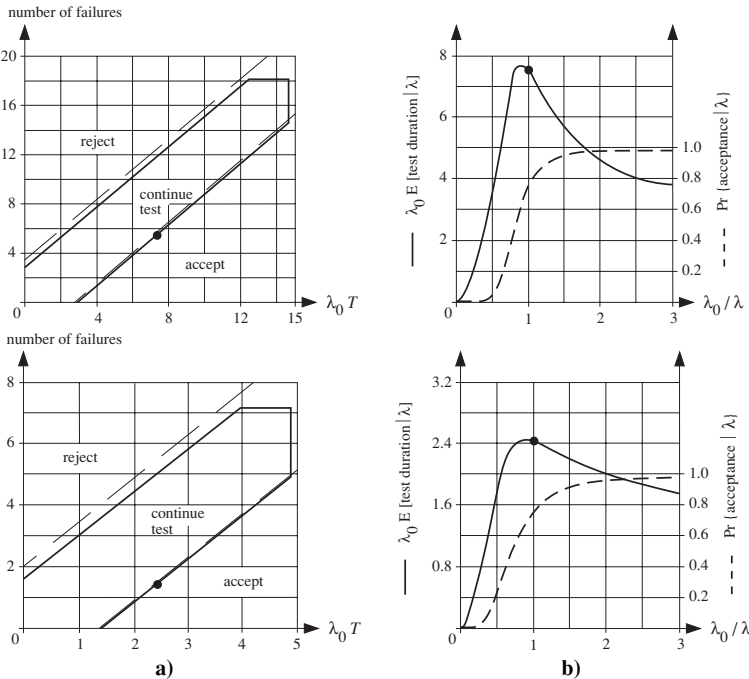


Figure 7.8 a) Sequential test plan to demonstrate $\lambda < \lambda_0$ against $\lambda > \lambda_1$ for $\alpha \approx \beta \approx 0.2$ and $\lambda_1/\lambda_0 = 1.5$ (top), $\lambda_1/\lambda_0 = 2$ (bottom), as per IEC 61124 and MIL-HDBK-781 [7.19, 7.23] (dashed on the left are the lines given by Eqs. (7.36)–(7.38)); b) Expected test duration until acceptance (continuous) and operating characteristic curve (dashed) as a function of λ_0 / λ (can be used to test $MTBF < MTBF_0$ against $MTBF > MTBF_1$, for the case $MTBF = 1/\lambda$)

7.2.3.3 Simple One-sided Test for the Demonstration of a Constant Failure Rate λ (or of $MTBF$ for the case $MTBF = 1/\lambda$)⁺

Simple two-sided tests (Fig. 7.7) and sequential tests (Fig. 7.8) have the advantage that, for $\alpha = \beta$, producer and consumer run the same risk of making a false decision. However, in practical applications often only λ_0 and α or λ_1 and β , i.e. *simple one-sided tests*, are used. The considerations of Section 7.1.3 apply, and care should be taken with small values of c , as operating with λ_0 & α (or λ_1 & β) the producer (or consumer) *can be favored* (see e. g. Problem 7.6 on p. 579). Figure 7.9 shows the operating characteristic curves for various values of c as a function of λ for the demonstration of $\lambda < 1/1000\text{h}$ against $\lambda > 1/1000\text{h}$ with consumer risk $\beta \approx 0.2$ for $\lambda = 1/1000\text{h}$, and visualizes the reduction of producer's risk ($\alpha \approx 0.8$ for $\lambda = 1/1000\text{h}$) by decreasing λ , or increasing c (counterpart of Fig. 7.4).

⁺ See footnote on p. 318.

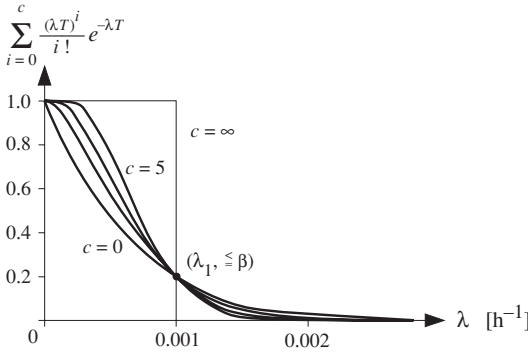


Figure 7.9 Operating characteristic curves (acceptance probability curves) for $\lambda_1=1/1000\text{h}$, ($\cong LTPD$), $\beta=0.2$, and $c=0$ ($T=1610\text{h}$), $c=1$ ($T=2995\text{h}$), $c=2$ ($T=4280\text{h}$), $c=5$ ($T=7905\text{h}$), and $c=\infty$ ($T=\infty$) as per Fig. 7.3 or Table A9.2 (holds for $MTBF_1=1000\text{h}$, for the case $MTBF=1/\lambda$)

7.3 Statistical Maintainability Tests

Maintainability is generally expressed as a *probability*. In this case, results of Sections 7.1 and 7.2.1 can be used to estimate or demonstrate maintainability. However, estimation and demonstration of specific parameters, for instance *MTTR* (mean time to repair, used as a synonym for mean time to *restoration* in this book, see pp. 113 & 381) is important for practical applications. If the underlying random variables are exponentially distributed (constant repair rate μ), the results of Section 7.2.3 for a *constant failure rate* λ can be used. This section deals with the estimation and demonstration of an *MTTR* by assuming that repair time is *lognormally* distributed (for Erlangian distributed repair times, results of Section 7.2.3 can be used, considering Eqs. (A6.102)-(A6.104)).

7.3.1 Estimation of an *MTTR*

Let t'_1, \dots, t'_n be independent observations (realizations) of the repair time τ' of a given item. From Eqs. (A8.6) and (A8.10), the *empirical mean* and *variance* of τ' are given by

$$\hat{E}[\tau'] = \frac{1}{n} \sum_{i=1}^n t'_i, \tag{7.39}$$

and

$$\widehat{\text{Var}}[\tau'] = \frac{1}{n-1} \sum_{i=1}^n (t_i' - \widehat{E}[\tau'])^2 = \frac{1}{n-1} \left[\sum_{i=1}^n t_i'^2 - \frac{1}{n} \left(\sum_{i=1}^n t_i' \right)^2 \right]. \quad (7.40)$$

Both estimates are unbiased, i. e. $E[\widehat{E}[\tau']] = E[\tau'] = MTTR$ & $E[\widehat{\text{Var}}[\tau']] = \text{Var}[\tau']$; furthermore, $\text{Var}[\widehat{E}[\tau']] = \text{Var}[\tau'] / n$ (Appendix A8.1.2). As stated above, the repair time τ' can often be assumed lognormally distributed with distribution function

$$F(t) = \Pr\{\tau' \leq t\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{\ln(\lambda t)}{\sigma}} e^{-x^2/2} dx \quad (7.41)$$

(Eq. (A6.110)), and mean & variance given by (Eqs. (A6.112) and (A6.113))

$$E[\tau'] = MTTR = \frac{e^{\sigma^2/2}}{\lambda}, \quad \text{Var}[\tau'] = \frac{e^{2\sigma^2} - e^{\sigma^2}}{\lambda^2} = MTTR^2 (e^{\sigma^2} - 1). \quad (7.42)$$

From Example A6.18 (p. 448) one recognizes that $\ln \tau'$ is normally distributed with mean $\ln 1/\lambda$ and Variance σ^2 . Using Eqs. (A8.24) and (A8.27), the *maximum likelihood* estimations of λ and σ^2 follow as

$$\widehat{\lambda} = \left[\prod_{i=1}^n \frac{1}{t_i'} \right]^{1/n} \quad \text{and} \quad \widehat{\sigma}^2 = \frac{1}{n} \sum_{i=1}^n [\ln(\widehat{\lambda} t_i')]^2. \quad (7.43)$$

A *point estimate* for λ and σ can also be obtained by the method of quantiles. The idea is to substitute some particular quantiles with the corresponding empirical quantiles to obtain estimates for λ or σ . For $t = 1/\lambda$, $\ln(\lambda t) = 0$ and $F(1/\lambda) = 0.5$, therefore, $1/\lambda$ is the 0.5 quantile (median) $t_{0.5}$ of the distribution function $F(t)$ given by Eq. (7.41). From the empirical 0.5 quantile $\widehat{t}'_{0.5} = \inf\{t' : \widehat{F}_n(t') \geq 0.5\}$ an estimate for λ follows as

$$\widehat{\lambda} = \frac{1}{\widehat{t}'_{0.5}}. \quad (7.44)$$

Moreover, $t = e^\sigma / \lambda$ yields $F(e^\sigma / \lambda) = 0.841$ (Table A9.1); thus $e^\sigma / \lambda = t_{0.841}$ is the 0.841 quantile of $F(t)$ given by Eq. (7.41). Using $\lambda = 1/t_{0.5}$ and $\sigma = \ln(\lambda t_{0.841}) = \ln(t_{0.841} / t_{0.5})$, an estimate for σ is obtained as

$$\widehat{\sigma} = \ln(\widehat{t}'_{0.841} / \widehat{t}'_{0.5}). \quad (7.45)$$

Furthermore, considering $F(e^{-\sigma} / \lambda) = 1 - 0.841 = 0.159$, i. e. $t_{0.159} = e^{-\sigma} / \lambda$, it follows that $e^{2\sigma} = \lambda t_{0.841} / \lambda t_{0.159}$ and thus Eq. (7.45) can be replaced by

$$\widehat{\sigma} = \frac{1}{2} \ln(\widehat{t}'_{0.841} / \widehat{t}'_{0.159}). \quad (7.46)$$

The possibility of representing a lognormal distribution function as a straight line, to simplify interpretation of data, is discussed in Section 7.5.1 (Fig. 7.14, Appendix A9.8.1).

To obtain *interval estimates* for the parameters λ and σ , note that the logarithm of a log normally distributed variable is normally distributed with mean $\ln(1/\lambda)$ and variance σ^2 . Applying the transformation $t'_i \rightarrow \ln t'_i$ to the individual observations t'_1, \dots, t'_n and using the results known for the interval estimation of the parameters of a normal distribution [A6.1, A6.4], the confidence intervals

$$\left[\frac{n \hat{\sigma}^2}{\chi_{n-1, (1+\gamma)/2}^2}, \frac{n \hat{\sigma}^2}{\chi_{n-1, (1-\gamma)/2}^2} \right] \quad (7.47)$$

for σ^2 , and

$$\left[\hat{\lambda} e^{-\varepsilon}, \hat{\lambda} e^{\varepsilon} \right] \quad \text{with} \quad \varepsilon = \frac{\hat{\sigma}}{\sqrt{n-1}} t_{n-1, (1+\gamma)/2} \quad (7.48)$$

for λ can be found with $\hat{\lambda}$ and $\hat{\sigma}$ as in Eq. (7.43). $\chi_{n-1, q}^2$ and $t_{n-1, q}$ are the q quantiles of the χ^2 and t -distribution with $n-1$ degrees of freedom, respectively (Tables A9.2 and A9.3).

Example 7.11

Let 1.1, 1.3, 1.6, 1.9, 2.0, 2.3, 2.4, 2.7, 3.1, and 4.2 h be 10 independent observations (realizations) of a lognormally distributed repair time. Give the maximum likelihood estimate and, for $\gamma = 0.9$, the confidence interval for the parameters λ and σ^2 , as well as the maximum likelihood estimate for *MTTR*.

Solution

Equation (7.43) yields $\hat{\lambda} \approx 0.476 \text{ h}^{-1}$ and $\hat{\sigma}^2 \approx 0.146$ as maximum likelihood estimates for λ and σ^2 . From Eq. (7.42), $\hat{MTTR} \approx e^{0.073} / 0.476 \text{ h}^{-1} \approx 2.26 \text{ h}$. Using Eqs. (7.47) and (7.48), as well as Tables A9.2 and A9.3, the confidence intervals are $[1.46/16.919, 1.46/3.325] \approx [0.086, 0.44]$ for σ^2 and $[0.476 e^{-0.127 \cdot 1.833}, 0.476 e^{0.127 \cdot 1.833}] \text{ h}^{-1} \approx [0.38, 0.60] \text{ h}^{-1}$ for λ , respectively.

7.3.2 Demonstration of an *MTTR*

The demonstration of an *MTTR* (in an acceptance test) will be investigated here by assuming that the repair time τ' is *lognormally* distributed with *known* σ^2 (method 1-A of *MIL-HDBK-470* [7.23]). A rule is asked to test the null hypothesis $H_0: MTTR = MTTR_0$ against the alternative hypothesis $H_1: MTTR = MTTR_1$ for given type I error α and type II error β (Appendix A8.3). The procedure (test plan) is as follows:

1. From α and β ($0 < \alpha < 1 - \beta < 1$), determine the quantiles t_β and $t_{1-\alpha}$ of the standard normal distribution (Table A9.1)

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t_\beta} e^{-x^2/2} dx = \beta \quad \text{and} \quad \frac{1}{\sqrt{2\pi}} \int_{t_{1-\alpha}}^{\infty} e^{-x^2/2} dx = 1 - \alpha. \quad (7.49)$$

From $MTTR_0$ and $MTTR_1$, compute the sample size n (next highest integer)

$$n = \frac{(t_{1-\alpha} MTTR_0 - t_\beta MTTR_1)^2}{(MTTR_1 - MTTR_0)^2} (e^{\sigma^2} - 1). \quad (7.50)$$

2. Perform n independent repairs and record the observed repair times t'_1, \dots, t'_n (representative sample of repair times).
3. Compute $\hat{E}[\tau']$ according to Eq. (7.39) and reject $H_0: MTTR = MTTR_0$ if

$$\hat{E}[\tau'] > c = MTTR_0 (1 + t_{1-\alpha} \sqrt{(e^{\sigma^2} - 1)/n}), \quad (7.51)$$

otherwise accept H_0 .

The proof of the above rule implies a sample size $n > 10$, so that the quantity $\hat{E}[\tau']$ can be assumed to have a normal distribution with mean $MTTR$ and variance $\text{Var}[\tau']/n$ (Eqs. (A6.148), (A8.7), (A8.8)). Considering the type I and type II errors

$$\alpha = \Pr\{\hat{E}[\tau'] > c \mid MTTR = MTTR_0\}, \quad \beta = \Pr\{\hat{E}[\tau'] \leq c \mid MTTR = MTTR_1\},$$

and using Eqs. (A6.105) and (7.49), the relationship

$$c = MTTR_0 + t_{1-\alpha} \sqrt{\text{Var}_0[\tau']/n} = MTTR_1 + t_\beta \sqrt{\text{Var}_1[\tau']/n} \quad (7.52)$$

can be found, with $\text{Var}_0[\tau']$ for $t_{1-\alpha}$ and $\text{Var}_1[\tau']$ for t_β according to Eq. (7.42) ($\text{Var}_i[\tau'] = (e^{\sigma^2} - 1) MTTR_i^2, i = 0, 1$). The sample size n (Eq. (7.50)) follows then from Eq. (7.52). The right hand side of Eq. (7.51) is equal to the constant c as per Eq. (7.52). The operating characteristic curve (OC) can be calculated from

$$\Pr\{\text{acceptance} \mid MTTR\} = \Pr\{\hat{E}[\tau'] \leq c \mid MTTR\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^d e^{-x^2/2} dx, \quad (7.53)$$

with (considering Eqs. (A6.105) and (7.52))

$$d = \frac{MTTR_0}{MTTR} t_{1-\alpha} - \left(1 - \frac{MTTR_0}{MTTR}\right) \sqrt{n/(e^{\sigma^2} - 1)}.$$

Replacing in d the quantity $n/(e^{\sigma^2} - 1)$ from Eq. (7.50) one recognizes that the operating characteristic curve is independent of σ^2 (rounding of n neglected).

Example 7.12

Give the rejection conditions (Eq. (7.51)) and the operating characteristic curve (OC) for the demonstration of $MTTR = MTTR_0 = 2\text{ h}$ against $MTTR = MTTR_1 = 2.5\text{ h}$ with $\alpha = \beta = 0.1$ and $\sigma^2 = 0.2$.

Solution

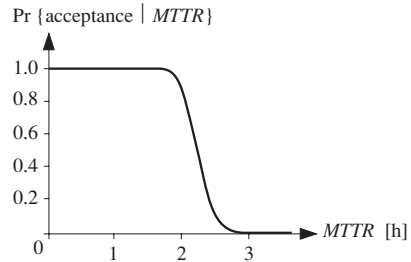
For $\alpha = \beta = 0.1$, Eq. (7.49) and Table A9.1 yield $t_{1-\alpha} = 1.28$, $t_\beta = -1.28$. From Eq. (7.50) it follows $n = 30$. The rejection condition is then given by

$$\sum_{i=1}^{30} t_i' > 2\text{ h} \left(1 + 1.28 \sqrt{\frac{e^{0.2} - 1}{30}} \right) 30 = 66.6\text{ h}.$$

From Eq. (7.53), the OC follows as

$$\Pr\{\text{acceptance} \mid MTTR\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^d e^{-x^2/2} dx,$$

with $d \approx 25.84\text{ h} / MTTR - 11.64$ (see graph).



7.4 Accelerated Testing

The failure rate λ of electronic components lies typically between 10^{-10} and 10^{-7} h^{-1} , and that of assemblies in the range of 10^{-7} to 10^{-5} h^{-1} . With such figures, cost and scheduling considerations demand the use of *accelerated testing* for λ estimation and demonstration, in particular if *reliable field data* are not available. An *accelerated test* is a test in which the applied stress is chosen to exceed that encountered in field operation, but still *below the technological limits*. This in order to shorten the time to failure of the item considered by avoiding an *alteration of the involved failure mechanism* (genuine acceleration). In accelerated tests, failure mechanisms are assumed to be activated selectively by increased stress. The quantitative relationship between degree of activation and extent of stress, i.e. the *acceleration factor A*, is determined via specific tests. Generally,

it is assumed that the stress will not change the type of the failure-free time distribution function of the item under test, but only modify the parameters, this hypothesis is assumed to be valid; however, its verification is mandatory before any statistical evaluation of data from accelerated tests.

Many electronic component *failure mechanisms* are activated through an increase in *temperature*. Calculating the acceleration factor A , the *Arrhenius model* can often be applied over a reasonably large temperature range (about $0\text{--}150^\circ\text{C}$ for ICs). The *Arrhenius model* is based on the Arrhenius rate law [7.10, 3.43], which states that the rate v of a simple (first-order) chemical reaction depends on temperature T as

$$v = v_0 e^{-E_a/kT}. \tag{7.54}$$

E_a and v_0 are parameters, k is the Boltzmann constant ($k = 8.6 \cdot 10^{-5}$ eV / K), and T the absolute temperature in Kelvin degrees. E_a is the *activation energy* and is expressed in eV. Assuming that the event considered (for example the diffusion between two liquids) occurs when the chemical reaction has reached a given threshold, and the reaction time dependence is given by a function $r(t)$, then the relationship between the times t_1 and t_2 necessary to reach at two temperatures T_1 and T_2 a given level of the chemical reaction considered can be expressed as

$$v_1 r(t_1) = v_2 r(t_2).$$

Furthermore, assuming $r(t) \sim t$, i. e. a *linear time dependence*, it follows that

$$v_1 t_1 = v_2 t_2.$$

Substituting in Eq. (7.54) and rearranging, yields

$$\frac{t_1}{t_2} = \frac{v_2}{v_1} = e^{\frac{E_a}{k} \left(\frac{1}{T_1} - \frac{1}{T_2} \right)}.$$

By transferring this *deterministic* model to the mean times to failure $MTTF_1$ and $MTTF_2$ or to the constant failure rates λ_2 and λ_1 (using $MTTF = 1/\lambda$) of a given item at temperatures T_1 and T_2 , it is possible to define an *acceleration factor* A

$$A = MTTF_1 / MTTF_2, \quad \text{or, for time independent failure rate, } A = \lambda_2 / \lambda_1, \quad (7.55)$$

expressed by

$$A = e^{\frac{E_a}{k} \left(\frac{1}{T_1} - \frac{1}{T_2} \right)} \quad (7.56)$$

The right hand sides of Eq. (7.55) applies to the case of a constant (time independent but stress dependent) failure rate $\lambda(t) = \lambda$, for which $E[\tau] = \sqrt{\text{Var}[\tau]} = 1/\lambda$ holds (with τ as time to failure). Assuming that the left hand sides of Eq. (7.55) applies quite general (for time dependent failure rates) to *mean time to failure* ($E[\tau] = MTTF$) and *standard deviation* ($\sqrt{\text{Var}[\tau]}$) as well, and that the *type of the distribution function is the same* at temperatures T_1 and T_2 , it can be shown that for the distribution functions frequently used in reliability engineering (Table A6.1) the following holds for the parameters: $\lambda_2 = A \lambda_1$ for exponential, Gamma, Weibull, and lognormal; $\beta_2 = \beta_1$ for Gamma and Weibull; $\sigma_2 = \sigma_1$ for lognormal; $m_2 = m_1 / A$ & $\sigma_2 = \sigma_1 / A$ for normal distribution.⁺⁺⁾ This yields $F_{\tau_1}(t) = F_{\tau_2}(\frac{t}{A})$ and thus $\tau_1 = A \tau_2$,

^{+) The case $T_2 = T_1 + \Delta T$, yielding a straight line in Fig 7.10 and a lognormal distribution for $\lambda(t)$, is discussed on p. 37.}

^{++) The demonstration is analytical for the exponential, Gamma, lognormal, and normal case; for Weibull, a quasi-analytic demonstration is possible using relations for $\Gamma(z+1)$ & $\Gamma(2z)$ on p.566.}

where τ_1 & τ_2 are the (random) *times to failure* at temperatures T_1 & T_2 , with distribution functions $F_{\tau_1}(t)$ & $F_{\tau_2}(t)$ belonging (per assumption) to the same family (case Vii in Example A6.18 and Eqs. (A6.40), (A6.46) with $C=A$).

Equation (7.56) can be reversed to give an estimate \hat{E}_a for the activation energy E_a based on the mean times to failure \hat{MTTF}_1 and \hat{MTTF}_2 (or the failure rates $\hat{\lambda}_1$ and $\hat{\lambda}_2$) obtained empirically from two life tests at temperatures T_1 and T_2 . However, at *least three tests* at $T_1, T_2,$ and T_3 are necessary to verify the model.

The activation energy is highly dependent upon the particular *failure mechanism* involved (see Table 3.5 for some indicative figures). High E_a values lead to high acceleration factors. For ICs, global values of E_a lie between 0.3 and 0.7eV, values which could basically be obtained empirically from the curves of the failure rate as a function of the junction temperature. However, it must be noted that the Arrhenius model does not hold for all electronic devices and for any temperature range, see e.g. also [7.13, 7.15, 7.22] for further critical remarks on accelerated tests.

Figure 7.10 shows the acceleration factor A from Eq. (7.56) as a function of θ_2 in $^{\circ}\text{C}$, for $\theta_1 = 35$ and 55°C and with E_a as parameter ($\theta_i = T_i - 273$).

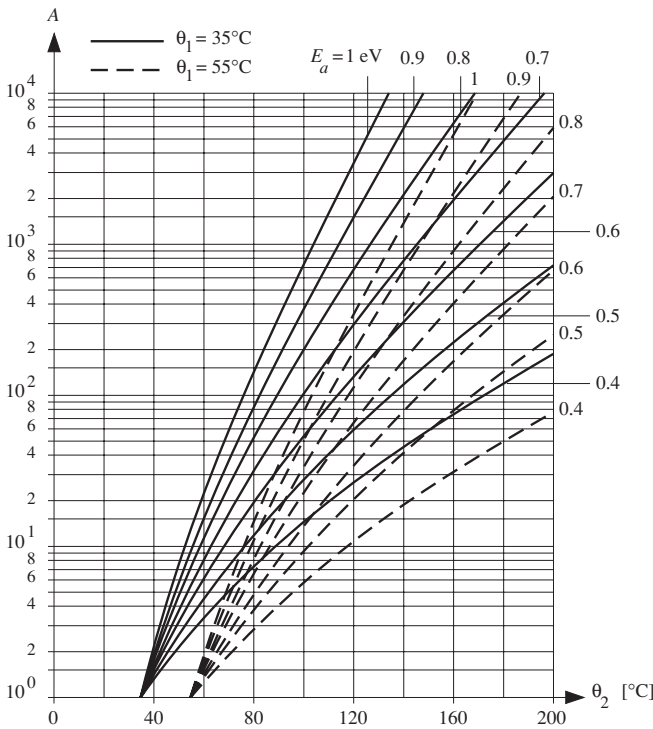


Figure 7.10 Acceleration factor A according to the Arrhenius model (Eq. (7.56)) as a function of θ_2 for $\theta_1 = 35$ and 55°C , and with E_a in eV as parameter ($\theta_i = T_i - 273$)

In particular for the case of a *constant* (time independent) *failure rate*, the acceleration factor A can be used as a *multiplicative factor* in the conversion of the *cumulative operating time* from stress T_2 to stress T_1 (Example 7.13, see also the remark to Eq. (7.55)). In practical applications, the acceleration factor A lies between 10 and some few hundreds, seldom > 1000 (Examples 7.13 & 7.14).

If the item under consideration exhibits *more than one dominant failure mechanism* or consists of series elements E_1, \dots, E_n having different failure mechanisms, the series reliability model (Sections 2.2.6.1 and 2.3.6) can often be used to calculate the *compound failure rate* $\lambda_S(T_2)$ at temperature T_2 by considering the failure rates $\lambda_i(T_1)$ and the acceleration factors A_i of the individual elements ^{*)}

$$\lambda_S(T_2) = \sum_{i=1}^n A_i \lambda_i(T_1). \quad (7.57)$$

Equation (7.57) applies for series structures, see p. 364 for further considerations.

Example 7.13

Four failures have occurred during 10^7 cumulative operating hours (footnote on p. 318) of a digital CMOS IC at a chip temperature of 130°C . Assuming $\theta_1 = 35^\circ\text{C}$, a constant failure rate λ , and an activation energy $E_a = 0.4\text{ eV}$, give the interval estimation of λ for $\gamma = 0.8$.

Solution

For $\theta_1 = 35^\circ\text{C}$, $\theta_2 = 130^\circ\text{C}$, and $E_a = 0.4\text{ eV}$ it follows from Fig. 7.10 or Eq. (7.56) that $A \approx 35$. The cumulative operating time at 35°C is thus $T = 0.35 \cdot 10^9\text{ h}$ and the point estimate for λ is $\hat{\lambda} = k/T \approx 11.4 \cdot 10^{-9}\text{ h}^{-1}$. With $k = 4$ and $\gamma = 0.8$, it follows from Fig. 7.6 that $\hat{\lambda}_l / \hat{\lambda} \approx 0.44$ and $\hat{\lambda}_u / \hat{\lambda} \approx 2$; the confidence interval for λ is therefore $[5, 22.8] \cdot 10^{-9}\text{ h}^{-1}$.

Example 7.14

A PCB contains 10 metal film resistors with stress factor $S = 0.1$ and $\lambda(25^\circ\text{C}) = 0.2 \cdot 10^{-9}\text{ h}^{-1}$, 5 ceramic capacitors (class 1) with $S = 0.4$ and $\lambda(25^\circ\text{C}) = 0.8 \cdot 10^{-9}\text{ h}^{-1}$, 2 electrolytic capacitors (Al wet) with $S = 0.6$ and $\lambda(25^\circ\text{C}) = 6 \cdot 10^{-9}\text{ h}^{-1}$, and 4 ceramic-packaged linear ICs with $\Delta\theta_{JA} = 10^\circ\text{C}$ and $\lambda(35^\circ\text{C}) = 20 \cdot 10^{-9}\text{ h}^{-1}$. Neglecting the contribution of printed wiring and solder joints, give the failure rate of the PCB at a burn-in temperature θ_A of 80°C on the basis of failure rate relationships given in Figs. 2.4 & 2.5.

Solution

The resistor and capacitor acceleration factors can be obtained from Fig. 2.4 as

resistor:	$A \approx 2.5/0.7 \approx 3.6$
ceramic capacitor (class 1):	$A \approx 3.8/0.45 \approx 8.4$
electrolytic capacitor (Al wet):	$A \approx 13.6/0.35 \approx 38.9$.

Using Eq. (2.4) for the ICs, it follows that $\lambda \sim \Pi_T$. With $\theta_J = 35^\circ\text{C}$ and 90°C , the acceleration factor for the linear ICs can then be obtained from Fig. 2.5 as $A \approx 10/0.9 \approx 11$. From Eqs. (2.19) & (7.57), the failure rate of the PCB follows as

$$\lambda(25^\circ\text{C}) \approx (10 \cdot 0.2 + 5 \cdot 0.8 + 2 \cdot 6 + 4 \cdot 20) 10^{-9}\text{ h}^{-1} \approx 100 \cdot 10^{-9}\text{ h}^{-1}$$

$$\lambda(80^\circ\text{C}) \approx (10 \cdot 0.2 \cdot 3.6 + 5 \cdot 0.8 \cdot 8.4 + 2 \cdot 6 \cdot 38.9 + 4 \cdot 20 \cdot 11) 10^{-9}\text{ h}^{-1} \approx 1.4 \cdot 10^{-6}\text{ h}^{-1} \approx 14 \cdot \lambda(25^\circ\text{C}).$$

^{*)} Elements with similar failure mechanisms can be grouped in one element, as per Eqs. (2.18), (2.19).

A further model for investigating the time scale reduction (time compression) resulting from an increase in temperature has been proposed by H. Eyring [3.43, 7.25]. The *Eyring model* defines the acceleration factor as

$$A = (T_2/T_1) e^{\frac{B}{k} \left(\frac{1}{T_1} - \frac{1}{T_2} \right)}, \quad (7.58)$$

where B is not necessarily an activation energy. Eyring also suggests the following model, which considers the influences of temperature T and of a further stress X

$$A = (T_2/T_1)^m e^{\frac{B}{k} \left(\frac{1}{T_1} - \frac{1}{T_2} \right)} e^{[X_1 \left(C + \frac{D}{kT_1} \right) - X_2 \left(C + \frac{D}{kT_2} \right)]}. \quad (7.59)$$

Equation (7.59) is known as the *generalized Eyring model*. In this multiplicative model, a function of the normalized variable $x = X/X_0$ can also be used instead of the quantity X itself (for example x^n , $1/x^n$, $\ln x^n$, $\ln(1/x^n)$). B is not necessarily an activation energy, C & D constants. The generalized Eyring model led to accepted models, for *electromigration* (Black, $m=0$, $X_1 = \ln(j_2/j_1)^n$, $B=E_a$, $C=1$, $D=X_2=0$ in Eq. (7.59)), *corrosion* (Peck), and *voltage stress* (Kemeny) [3.33, 3.56, 3.67]

$$A = \left(\frac{j_2}{j_1} \right)^n e^{\frac{E_a}{k} \left(\frac{1}{T_1} - \frac{1}{T_2} \right)}, \quad A = \left(\frac{RH_2}{RH_1} \right)^n e^{\frac{E_a}{k} \left(\frac{1}{T_1} - \frac{1}{T_2} \right)}, \quad A = e^{(C_0 + \frac{E_a}{kT} + C_1 V/V_{\max})}, \quad (7.60)$$

where j = current density, RH = relative humidity, and V = voltage, respectively (see also Eqs. (3.2)–(3.6) and Table 3.5). For voltage stress, a refined model of the form $A = e^{\gamma(V_a - V_0)}$ is discussed e. g. in [3.67].

For failure mechanisms related to *mechanical fatigue*, Coffin-Manson simplified models [2.61, 2.72] (based on the inverse power law) can often be used, yielding for the number of *cycles to failure*

$$A = \frac{N_1}{N_2} = \left(\frac{\Delta T_2}{\Delta T_1} \right)^{\beta_T} \quad \text{or} \quad A = \frac{N_1}{N_2} = \left(\frac{G_2}{G_1} \right)^{\beta_M}, \quad (7.61)$$

where ΔT refers to thermal cycles, G to vibration tests ($0.5 < \beta_T < 0.8$, $0.7 < \beta_M < 0.9$ often occur in practical applications). For damage accumulation, Miner's hypothesis of *independent damage increments* [3.52] can be used in some applications. Known for conductive-filament formation is the Rudra's model [3.62]. Models for solder joints are discussed e. g. in [3.79 (2011), 3.90], see also Section 3.4 for some considerations.

Refinement of the above models is in progress in the context of *physics of failures* (PoF) [2.15, 3.49, 3.66, 3.67], in particular for ULSI ICs and considering stress dependent parameters and time dependent failure rates, with emphasis on:

1. New failure mechanisms in oxide and package, as well as new externally induced failure mechanisms.
2. Identification and analysis of causes for early failures or premature wear-out.
3. Development of *physical models* for *failure mechanisms* and of *simplified models* for *reliability predictions* in practical applications.

Such efforts will give better *physical understanding* on components failure rates.

In addition to the accelerated tests discussed above, a rough estimate of component life time can often be obtained through *short-term tests* under extreme stresses (HALT, HAST, etc.). Examples are humidity testing of plastic-packaged ICs at high pressure and nearly 100% RH, or tests of ceramic-packaged ICs at up to 350°C. Experience shows that under high stress, life time is often lognormally distributed, thus with *strong time dependence* of the failure rate (Table A6.1). *Highly accelerated stress tests* (HAST) and *highly accelerated life tests* (HALT) can activate failure mechanisms which would not occur during normal operation, so care is necessary in extrapolating results to situations exhibiting lower stresses. Often, the purpose of such tests is to *force* (not only to activate) *failures*. They belong thus to the class of semi-destructive or destructive tests, often used at the qualification of prototype to investigate possible failure modes, mechanisms and/or technological limits. The same holds for *step-stress accelerated tests* (often used as life tests or in screening procedures), for which, accumulation of damage can be more complex as given e. g. by the Miner's hypothesis or in [7.20, 7.28]. A *case-by-case investigation* is mandatory for all this kind of tests.

7.5 Goodness-of-fit Tests

Let t_1, \dots, t_n be n independent observations of a random variable τ distributed according to $F(t)$, a rule is asked to test the null hypothesis $H_0: F(t) = F_0(t)$, for a given type I error α (probability of *rejecting* a true hypothesis H_0), against a general alternative hypothesis $H_1: F(t) \neq F_0(t)$. *Goodness-of-fit tests* deal with such testing of hypothesis and are often based on the *empirical distribution function* (EDF), see Appendices A8.3 for an introduction. This section shows the use of Kolmogorov-Smirnov and chi-square tests (see p. 556 for Cramér-von Mises tests). Trend tests are discussed in Section 7.6.

7.5.1 Kolmogorov-Smirnov Test

The *Kolmogorov-Smirnov test* (p. 556) is based on the convergence for $n \rightarrow \infty$ of the empirical distribution function (Eq. (A8.1))

$$\hat{F}_n(t) = \begin{cases} 0 & \text{for } t < t_{(1)} \\ \frac{i}{n} & \text{for } t_{(i)} \leq t < t_{(i+1)}, \\ 1 & \text{for } t \geq t_{(n)} \end{cases} \quad i = 1, 2, \dots, n-1, \quad (7.62)$$

to the true distribution function, and compares the experimentally obtained $\hat{F}_n(t)$ with the given (postulated) $F_0(t)$. $F_0(t)$ is assumed here to be known and continuous, $t_{(1)} < \dots < t_{(n)}$ are the *ordered observations*. The procedure is as follows:

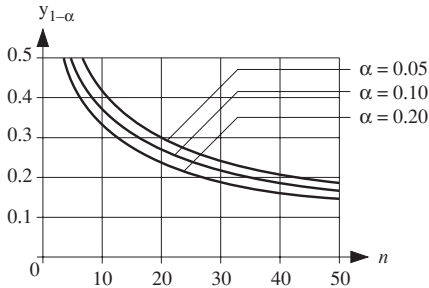


Figure 7.11 Largest deviation $y_{1-\alpha}$ between a postulated distribution function $F_0(t)$ and the corresponding empirical distribution function $\hat{F}_n(t)$ at the level $1-\alpha$ ($\Pr\{D_n \leq y_{1-\alpha} \mid F_0(t) \text{ true}\} = 1-\alpha$)

1. Determine the largest deviation D_n between $\hat{F}_n(t)$ and $F_0(t)$

$$D_n = \sup_{-\infty < t < \infty} |\hat{F}_n(t) - F_0(t)|. \tag{7.63}$$

2. From the given type I error α and the sample size n , use Table A9.5 or Fig. 7.11 to determine the critical value $y_{1-\alpha}$.
3. Reject $H_0: F(t) = F_0(t)$ if $D_n > y_{1-\alpha}$; otherwise accept H_0 .

This procedure can be easily combined with a *graphical evaluation of data*. For this purpose, $\hat{F}_n(t)$ and the band $F_0(t) \pm y_{1-\alpha}$ are drawn using a *probability chart* on which $F_0(t)$ can be represented by a straight line. If $\hat{F}_n(t)$ leaves the band $F_0(t) \pm y_{1-\alpha}$, the hypothesis $H_0: F(t) = F_0(t)$ is to be rejected (note that the band width is not constant when using a probability chart). Probability charts are discussed in Appendix A.8.1.3, examples are in Appendix A9.8 and Figs. 7.12-7.14. Example 7.15 (Fig. 7.12) shows a graphical evaluation of data for the case of a Weibull distribution, Example 7.16 (Fig. 7.13) investigates the distribution function of a population with *early failures* and a constant failure rate using a *Weibull probability chart*, and Example 7.17 (Fig. 7.14) uses the Kolmogorov-Smirnov test to check agreement with a lognormal distribution. If $F_0(t)$ is not completely known, a modification is necessary (Appendix A8.3.3).

Example 7.15

Accelerated life testing of a wet Al electrolytic capacitor leads following 13 ordered observations of lifetime: 59, 71, 153, 235, 347, 589, 837, 913, 1185, 1273, 1399, 1713, and 2567 h. (i) Draw the empirical distribution function of data on a Weibull probability chart. (ii) Assuming that the underlying distribution function is Weibull, determine $\hat{\lambda}$ and $\hat{\beta}$ graphically (p.531). (iii) The maximum likelihood estimation of λ & β yields $\hat{\beta} = 1.12$, calculate $\hat{\lambda}$ and compare with (ii).

Solution

- (i) Figure 7.12 presents the empirical distribution function $\hat{F}_n(t)$ on Weibull probability paper.
- (ii) The graphical determination of λ and β leads to (straight line (ii)) $\hat{\lambda} \approx 1/840$ h and $\hat{\beta} \approx 1.05$.
- (iii) With $\hat{\beta} \approx 1.12$, Eq. (A8.31) yields $\hat{\lambda} \approx 1/908$ h (straight line (iii)) (see also Example A8.12).

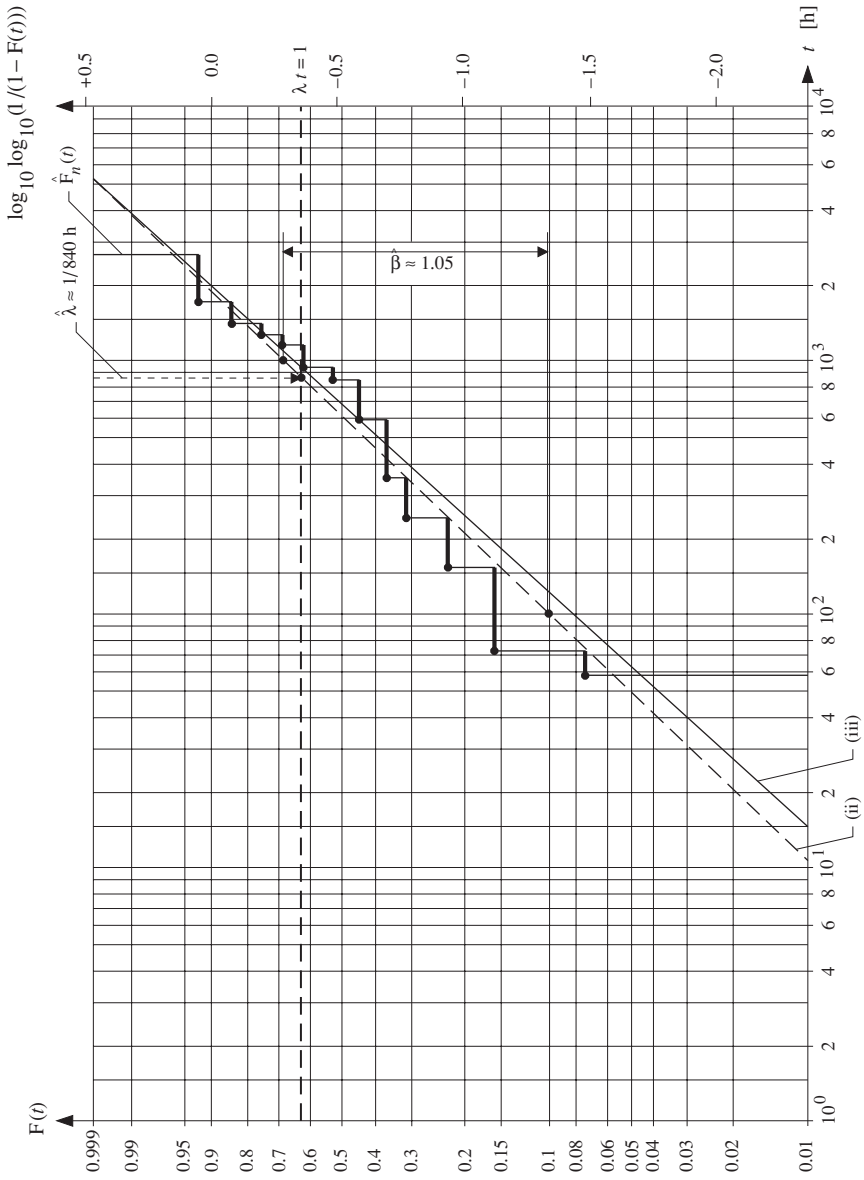


Figure 7.12 Empirical distribution function $\hat{F}_n(t)$ and estimated Weibull distribution functions (ii) and (iii) as per Example 7.15 (see Appendix A8.1.3, in particular the remark on p. 531)

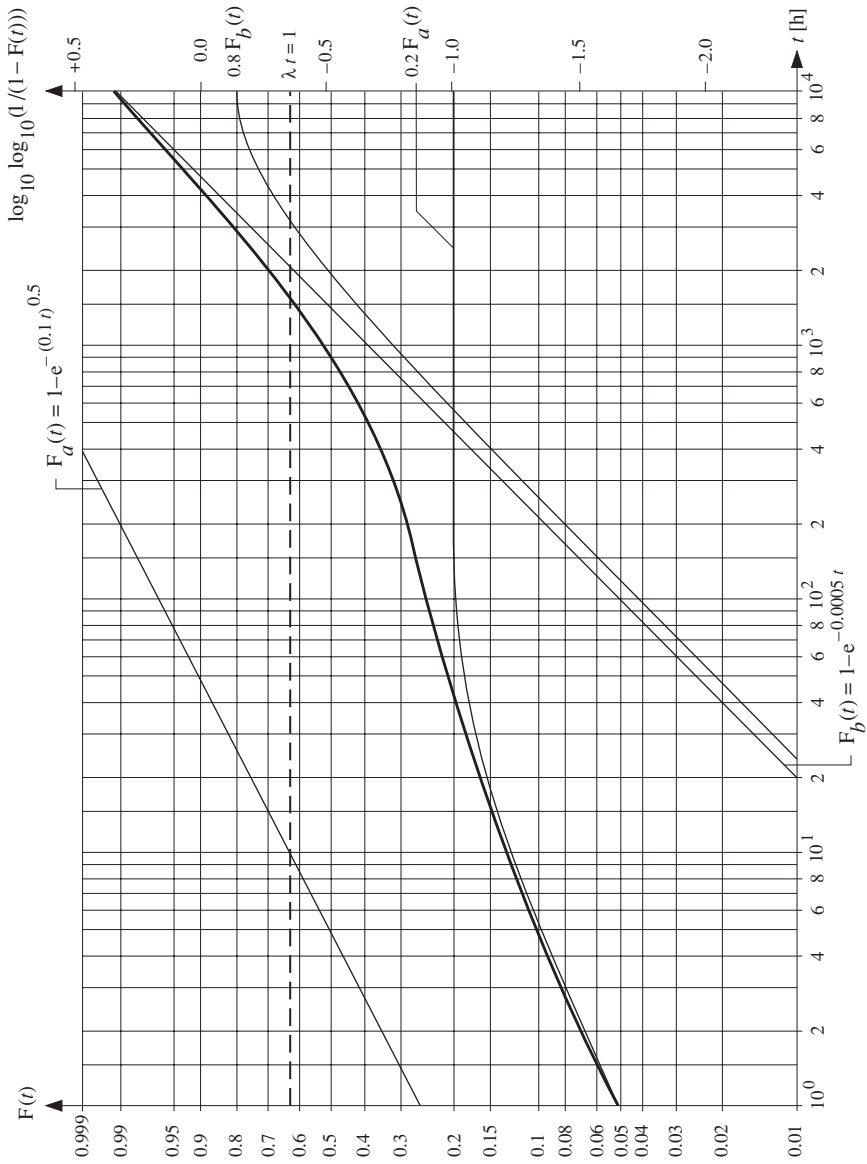


Figure 7.13 S-shape of a weighted sum $F(t) = pF_a(t) + (1-p)F_b(t)$ of a Weibull distribution $F_a(t)$ and an exponential distribution $F_b(t)$ per Example 7.16, useful to detect (describe) *early failures* (wear-out failures for slope 1 at the beginning and >1 at the end, see also pp. 7, 355 & 467 for alternative possibilities and pp. 7 & 444 when early failures and wear-out can occur)

Example 7.16

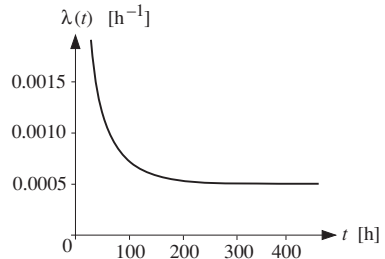
Investigate the *mixed* distribution function $F(t) = 0.2[1 - e^{-(0.1t)^{0.5}}] + 0.8[1 - e^{-0.0005t}]$ on a Weibull probability chart (describing a possible *early failure period*).

Solution

The weighted sum of a Weibull distribution (with $\beta = 0.5$, $\lambda = 0.1 \text{ h}^{-1}$, and $MTTF = 20 \text{ h}$) and an exponential distribution (with $\lambda = 0.0005 \text{ h}^{-1}$ and $MTTF = 1/\lambda = 2000 \text{ h}$) represents the

distribution function of a population of items with early failures up to about $t \approx 300 \text{ h}$, see graph; $\lambda(t) = [0.01(0.1t)^{-0.5}e^{-(0.1t)^{0.5}} + 0.0004e^{-0.0005t}] / [0.2e^{-(0.1t)^{0.5}} + 0.8e^{-0.0005t}]$ is nearly constant at 0.0005 h^{-1} for t between 300 and 300.000h, so that for $t > 300 \text{ h}$ a constant failure rate can be assumed ($1 - F(300) \approx 0.69$, $\lambda(300) \approx 0.00051 \text{ h}^{-1}$; $1 - F(300.000) \approx 6 \cdot 10^{-66}$, $\lambda(300.000) \approx 0.0005 \text{ h}^{-1}$).

Figure 7.13 gives the function $F(t)$ on a Weibull probability chart, showing the typical *s-shape*.



Example 7.17

Use the Kolmogorov-Smirnov test to verify with a type I error $\alpha = 0.2$, whether the repair time defined by the observations t_1, \dots, t_{10} of Example 7.11 are distributed according to a lognormal distribution function with parameters $\lambda = 0.5 \text{ h}^{-1}$ and $\sigma = 0.4$ (hypothesis H_0).

Solution

The lognormal distribution (Eq. (7.41)) with $\lambda = 0.5 \text{ h}^{-1}$ and $\sigma = 0.4$ is represented by a straight line on Fig. 7.14 ($F_0(t)$). With $\alpha = 0.2$ and $n = 10$, Table A9.5 or Fig. 7.11 yields $y_{1-\alpha} = 0.323$ and thus the band $F_0(t) \pm 0.323$. Since the empirical distribution function $\hat{F}_n(t)$ does not leave the band $F_0(t) \pm y_{1-\alpha}$, the hypothesis H_0 can be accepted.

7.5.2 Chi-square Test

The *chi-square test* (χ^2 -test, pp. 557 - 560) can be used for *continuous* or *noncontinuous* $F_0(t)$. Furthermore, $F_0(t)$ need not to be completely known.

For $F_0(t)$ *completely known*, the procedure is as follows:

1. Partition the definition range of the random variable τ into k intervals (classes) $(a_1, a_2], (a_2, a_3], \dots, (a_k, a_{k+1}]$; the choice of the classes must be made independently of the observations t_1, \dots, t_n (made before test begin) and based on the rule: $n p_i \geq 5$, with p_i as per Eq. (7.64).
2. Determine the number of observations k_i in each class $(a_i, a_{i+1}]$, $i = 1, \dots, k$ ($k_i =$ number of t_j with $a_i < t_j \leq a_{i+1}$, $k_1 + \dots + k_k = n$).
3. Assuming the hypothesis H_0 , compute the expected number of observations for each class $(a_i, a_{i+1}]$

$$n p_i = n(F_0(a_{i+1}) - F_0(a_i)), \quad i = 1, \dots, k, \quad p_1 + \dots + p_k = 1. \quad (7.64)$$

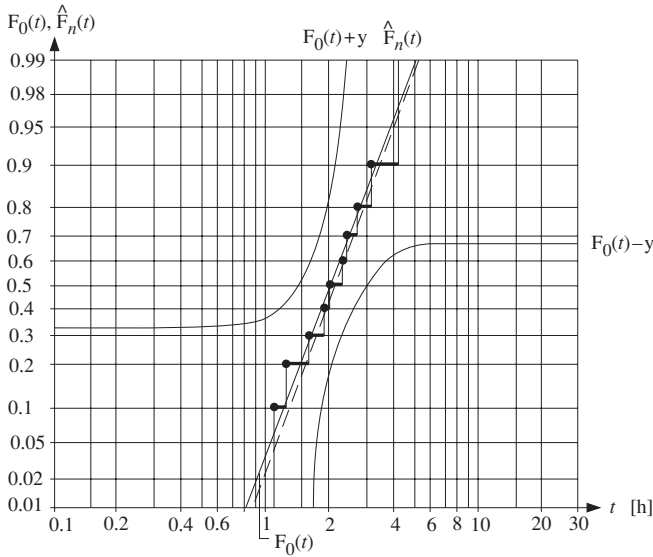


Figure 7.14 Kolmogorov-Smirnov test to check the repair time distribution as per Example 7.17 (the distribution function with $\hat{\lambda}$ and $\hat{\sigma}$ from Example 7.11 is shown dashed for information only)

4. Compute the statistic

$$X_n^2 = \sum_{i=1}^k \frac{(k_i - n p_i)^2}{n p_i} = \sum_{i=1}^k \frac{k_i^2}{n p_i} - n. \tag{7.65}$$

5. For a given type I error α , use Table A9.2 or Fig. 7.15 to determine the $(1-\alpha)$ quantile of the chi-square distribution with $k-1$ degrees of freedom $\chi_{k-1, 1-\alpha}^2$.
6. Reject $H_0: F(t) = F_0(t)$ if $X_n^2 > \chi_{k-1, 1-\alpha}^2$; otherwise accept H_0 .

If $F_0(t)$ is not completely known ($F_0(t) = F_0(t, \theta_1, \dots, \theta_r)$), where $\theta_1, \dots, \theta_r$ are unknown parameters, $r < k-1$), modify the above procedure after step 2 as follows:

- 3'. On the basis of the observations k_i in each class $(a_i, a_{i+1}]$, $i = 1, \dots, k$ determine the maximum likelihood estimates for the parameters $\theta_1, \dots, \theta_r$ from the following system of (r) algebraic equations

$$\sum_{i=1}^k \frac{k_i}{p_i(\theta_1, \dots, \theta_r)} \cdot \frac{\partial p_i(\theta_1, \dots, \theta_r)}{\partial \theta_j} \Big|_{\theta_j = \hat{\theta}_j} = 0, \quad j = 1, \dots, r \tag{7.66}$$

with $p_i = F_0(a_{i+1}, \theta_1, \dots, \theta_r) - F_0(a_i, \theta_1, \dots, \theta_r) > 0$, $p_1 + \dots + p_k = 1$, and for each class $(a_i, a_{i+1}]$ compute the expected number of observations

$$n \hat{p}_i = n [F_0(a_{i+1}, \hat{\theta}_1, \dots, \hat{\theta}_r) - F_0(a_i, \hat{\theta}_1, \dots, \hat{\theta}_r)], \quad i = 1, \dots, k. \tag{7.67}$$

4'. Calculate the statistic

$$\hat{X}_n^2 = \sum_{i=1}^k \frac{(k_i - n\hat{p}_i)^2}{n\hat{p}_i} = \sum_{i=1}^k \frac{k_i^2}{n\hat{p}_i} - n. \tag{7.68}$$

5'. For given type I error α , use Table A9.2 or Fig. 7.15 to determine the $(1-\alpha)$ quantile of the χ^2 distribution with $k-1-r$ degrees of freedom.

6'. Reject H_0 : $F(t) = F_0(t)$ if $\hat{X}_n^2 > \chi_{k-1-r, 1-\alpha}^2$; otherwise accept H_0 .

Comparing the above two procedures, it can be noted that the number of degrees of freedom has been reduced from $k-1$ to $k-1-r$, where r is the number of parameters of $F_0(t)$ which have been estimated from the observations t_1, \dots, t_n using the *multinomial distribution* (Example A8.13, see Example 7.18 for an application).

Example 7.18

Let 160, 380, 620, 650, 680, 730, 750, 920, 1000, 1100, 1400, 1450, 1700, 2000, 2200, 2800, 3000, 4600, 4700, and 5000 h be 20 independent observations (realizations) of the failure-free time τ for a given assembly. Using the chi-square test for $\alpha = 0.1$ and the 4 classes (0, 500], (500, 1000], (1000, 2000], (2000, ∞), determine whether or not τ is exponentially distributed (hypothesis H_0 : $F(t) = 1 - e^{-\lambda t}$, λ unknown).

Solution

The given classes yield number of observations of $k_1 = 2$, $k_2 = 7$, $k_3 = 5$, and $k_4 = 6$. The point estimate of λ is then given by Eq. (7.66) with $p_i = e^{-\lambda a_i} - e^{-\lambda a_{i+1}}$, yielding for $\hat{\lambda}$ the numerical solution $\hat{\lambda} \approx 0.562 \cdot 10^{-3} \text{ h}^{-1}$. Thus, the numbers of expected observations in each of the 4 classes are according to Eq. (7.67) $n\hat{p}_1 = 4.899$, $n\hat{p}_2 = 3.699$, $n\hat{p}_3 = 4.90$, and $n\hat{p}_4 = 6.499$. From Eq. (7.68) it follows that $\hat{X}_{20}^2 = 4.70$ and from Table A9.2, $\chi_{20, 0.9}^2 = 4.605$. The hypothesis H_0 : $F(t) = 1 - e^{-\lambda t}$ must be rejected since $\hat{X}_n^2 > \chi_{k-1-r, 1-\alpha}^2$.

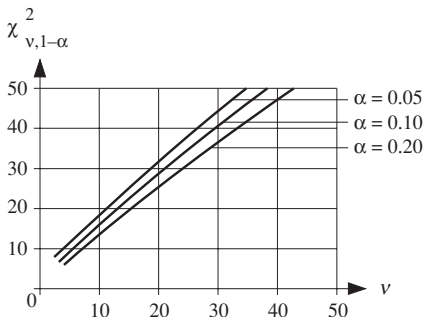


Figure 7.15 $(1-\alpha)$ quantile (α percentage point) of the *chi-square distribution* with v degrees of freedom ($\chi_{v, 1-\alpha}^2$, see also Table A9.2)

7.6 Statistical Analysis of General Reliability Data

7.6.1 General considerations

In Sections 7.2-7.5, data were issued from a sample of a random variable τ , i.e., they were n independent realizations (observations) t_1, \dots, t_n of a random variable $\tau > 0$ distributed according to (a postulated) $F(t) = \Pr\{\tau \leq t\}$ with $F(0) = 0$, and belonging to one of the following equivalent situations:

1. *Life times* t_1, \dots, t_n of n statistically identical and independent items, all starting at $t=0$ when plotted on the time axis (Figs. 1.1, 7.12, 7.14, A8.1).
2. Failure-free times separating successive failure occurrences of a repairable item (system) with negligible repair times and repaired (restored) *as a whole to as-good-as-new at each repair*; i.e., statistically identical & independent *interarrival times* with a common distribution function, yielding a *renewal process*.

To this data structure belongs also the case considered in Example 7.19.

A basically different situation arises when the observations are arbitrary points on the time axis (i.e. a *general point process*). To distinguish this case, the involved random variables are labeled $\tau_1^*, \tau_2^*, \dots$, with t_1^*, t_2^*, \dots for the corresponding realizations ($t_1^* < t_2^* < \dots$ tacitly assumed). This situation often occurs in reliability tests;

for instance, when *only the failed element* in a system is repaired to as-good-as-new, and *at least one element in the system has a time dependent failure rate*; in this case, *failure-free times (interarrival times, by assuming negligible repair times) are neither independent nor equally distributed*.

Except for very large systems, for which the flow of failures can be supposed to converge to a homogeneous Poisson process (p. 521), and case 2 above, only the case of a system with *constant failure rates for all elements* ($\lambda_1, \dots, \lambda_n$) leads (if failed elements are quickly repaired to as-good-as-new in a negligible time) to *interarrival times which are independent random variables with a common distribution function* $F(x)$, i.e. to a *renewal process* (a homogeneous Poisson process with $F(x) = 1 - e^{-\lambda_s x}$ for a series system). Shortcomings are known [6.1, 7.11, A7.30].

Example 7.19

Let $F(t)$ be the distribution function of the failure-free time of a given item. Suppose that at $t=0$ an unknown number n of items are put into operation and that at the time t_k exactly k items are failed (no replacement or repair has been done). Give a point estimate for n .

Solution

Setting $p = F(t_k)$, the number k of failures in $(0, t_k]$ is binomially distributed (Eq. (A6.120))

$$\Pr\{k \text{ failures in } (0, t_k]\} = p_k = \binom{n}{k} p^k (1-p)^{n-k}, \quad \text{with } p = F(t_k). \quad (7.69)$$

An estimate for n using the maximum likelihood method, $L = \binom{n}{k} p^k (1-p)^{n-k}$ as per Eq. (A8.23) and $\partial \ln L / \partial n = 0$ for $n = \hat{n}$, yields $\left(\binom{n}{k} \approx (e^{-k}/k!)(n^n/(n-k)^{(n-k)})\right)$, Stirling's formula p. 566)

$$\hat{n} = k/p = k/F(t_k). \quad (p_k \approx e^{-np} (np)^k / k! \text{ yields also } \hat{n} = k/p.) \quad (7.70)$$

Supplementary results: If $F(t)$ is unknown, $\hat{F}_k(t)$ can be obtained using t_1, \dots, t_k and Eq. (A8.1).

Easy to investigate, when observing data on the time axis, are also cases involving *nonhomogeneous Poisson processes* (Sections 7.6.2, 7.6.3, 7.7, Appendix A7.8.2). However, more general situations, can lead to difficulties, except for some general results valid for stationary point processes (Appendices A7.8.3-A7.8.5).

From all the above considerations, the following basic rule should apply:

If neither a Poisson process (homogeneous or nonhomogeneous) nor a renewal process can be assumed for the underlying point process, care is necessary in identifying possible models; in any case, validation of model assumptions (physical & statistical aspects) should precede data analysis.

The *homogeneous Poisson process* (HPP), introduced in Appendix A7.2.5 as a particular renewal process, is the simplest point process. It is *memoryless*, and tools for a statistical investigation are well known. *Nonhomogeneous Poisson processes* (NHPPs) are *without aftereffect* (Appendix A7.8.2), and for investigation purposes they can be transformed into an HPP (Eq. (A7.200)). Investigations on renewal processes (Appendix A7.2) can be reduced to that of independent random variables with a common distribution function (cases 1 and 2 on p.341). However, disregarding the last part of the above general rule can lead to mistakes, even in the presence of renewal processes or independent realizations of a random variable τ . As an example, let us consider an item with *two independent failure mechanisms*, one appearing with constant failure rate $\lambda_0 = 10^{-3} \text{h}^{-1}$ and the second (wear-out) with a shifted Weibull distribution $F(t) = 1 - e^{-(\lambda(t-\psi))^\beta}$ with $\lambda = 10^{-2} \text{h}^{-1}$, $\psi = 10^4 \text{h}$, and $\beta = 3$ ($t > \psi$, $F(t) = 0$ for $t \leq \psi$). The failure-free time τ has the distribution function $F(t) = 1 - e^{-\lambda_0 t}$ for $0 < t \leq \psi$ and, as for case 2 in Eq. (A6.34), $F(t) = 1 - e^{-\lambda_0 t} \cdot e^{-(\lambda(t-\psi))^\beta}$ for $t > \psi$ (failure rate $\lambda(t) = \lambda_0$ for $t \leq \psi$ and $\lambda(t) = \lambda_0 + \beta \lambda^\beta (t-\psi)^{\beta-1}$ for $t > \psi$, similar to a *series model with independent elements* (Eq. (2.18)). If the presence of the above two failure mechanisms is not known, neither suspected, and the test is stopped (censored) at 10^4h , the wrong conclusion can be drawn that the item has a constant failure rate of 10^{-3}h^{-1} .

Investigation of cases involving general point processes is beyond the scope of this book (only some general results are given in Appendices A7.8.3- A7.8.5). A large number of ad hoc procedures are known in the literature, but they often only apply to specific situations and their use needs a careful validation of the assumptions stated with the model.

After some considerations on tests for *nonhomogeneous Poisson processes* in Section 7.6.2, Sections 7.6.3.1 and 7.6.3.2 deal with *trend tests* to check the assumption *homogeneous Poisson process* versus *nonhomogeneous Poisson process with increasing or decreasing intensity*. A heuristic test to distinguish a homogeneous Poisson process from a general monotonic trend is discussed in Section 7.6.3.3; however, as stated in the above general rule, the validity of a model should be checked also on the basis of physical considerations on the item considered, in particular for the property *without aftereffect*, characterizing Poisson processes.

7.6.2 Tests for Nonhomogeneous Poisson Processes

A nonhomogeneous Poisson process (NHPP) is a point processes which count function $v(t)$ has unit jumps, *independent increments* (in nonoverlapping intervals), and satisfies for any $b > a \geq 0$ (Appendix A7.8.2)

$$\Pr\{k \text{ events in } (a, b]\} = \frac{(M(b)-M(a))^k}{k!} e^{-(M(b)-M(a))}, \quad \begin{matrix} k=0,1,2,\dots \\ \leq a < b, M(0)=0. \end{matrix} \quad (7.71)$$

For $a=0$ & $b=t$ it holds that $\Pr\{v(t)=k\} = (M(t))^k e^{-M(t)}/k!$. $M(t)$ is the *mean value function* of the NHPP, giving the expected number of points (events) in $(0, t]$

$$M(t) = E[v(t)], \quad t > 0, \quad M(t) = 0 \text{ for } t \leq 0. \quad (7.72)$$

$M(t) = \lambda t$ yields a *homogeneous Poisson process* (HPP). Assuming $M(t)$ derivable,

$$m(t) = dM(t)/dt \geq 0, \quad t > 0, \quad m(t) = 0 \text{ for } t \leq 0, \quad (7.73)$$

is the *intensity* of the NHPP and has for $\delta t \downarrow 0$ following interpretation (Eq. (A7.194))

$$\Pr\{\text{one event in } (t, t+\delta t]\} = m(t)\delta t + o(\delta t). \quad (7.74)$$

Because of independent increments (in nonoverlapping intervals), the number of events (failures) in a time interval $(t, t+\theta]$ (Eq. (7.71) with $a=t$ & $b=t+\theta$) and the rest waiting time to the next event from an arbitrary time point t (Eqs. (A7.196))

$$\Pr\{\tau_R(t) > x\} = \Pr\{\text{no event in } (t, t+x]\} = e^{-(M(t+x)-M(t))}, \quad x \geq 0, \quad (7.75)$$

are *independent of the process development up to time t*; i.e., the Poisson process is a process *without aftereffect* (*memoryless* if homogeneous). The mean $E[\tau_R(t)]$ is thus also independent of the process development up to time t (Eq. (A7.197))

$$E[\tau_R(t)] = \int_0^{\infty} e^{-(M(t+x)-M(t))} dx.$$

Furthermore, if $0 < \tau_1^* < \tau_2^* < \dots$ are the occurrence times (arrival times) of the event considered (e.g. failures of a repairable system), measured from $t=0$, it holds for $m(t) > 0$ ($M(t)$ derivable and strictly increasing) that the quantities

$$\psi_1^* = M(\tau_1^*) < \psi_2^* = M(\tau_2^*) < \dots \quad (7.76)$$

are the occurrence times in a homogeneous Poisson processes with *intensity one* (Eq. (A7.200)). Moreover, for given (fixed) $t=T$ and $v(T)=n$, the occurrence times $0 < \tau_1^* < \dots < \tau_n^* < T$ have the same distribution as if they were the *order statistic* of n independent identically distributed random variables with *density*

$$m(t)/M(T), \quad 0 < t < T, \quad (7.77)$$

and distribution function $M(t)/M(T)$ on $(0, T)$ (Eq. (A7.205)).

Equation (7.74) gives the *unconditional* probability for *one event* in $(t, t + \delta t]$. Thus, $m(t)$ refers to the occurrence of *any one* of the events considered. It corresponds to the *renewal density* $h(t)$ and the *failure intensity* $z(t)$, but *differs basically* from the *failure rate* $\lambda(t)$ (see remarks on pp. 7, 378, 426, 466, 524).

Nonhomogeneous Poisson processes (NHPPs) are introduced in Appendix A7.8.2. Some examples are discussed in Section 7.7 with applications to reliability growth. Assuming that the underlying process is an NHPP, estimation of the model parameters (parameters θ of $m(t, \theta)$) can be performed using the maximum likelihood method on the basis of observed data $0 < t_1^* < t_2^* < \dots < t_n^* < T$ (time censoring; t_1^*, t_2^*, \dots are the observed values (realizations) of $\tau_1^*, \tau_2^*, \dots$ and $*$ is used to explicitly indicate that t_1^*, t_2^*, \dots are points on the time axis and not independent realizations of a random variable τ (e. g. as in Figs. 1.1, 7.12, 7.14)). Considering Eqs. (7.71) and (7.74), the likelihood function follows as (Eq. (7.102))

$$L = e^{-M(T)} \prod_{i=1}^n m(t_i^*), \tag{7.78}$$

and delivers the maximum likelihood estimate $\hat{\theta}$ for the parameters θ of $m(t, \theta)$ by solving $\partial L / \partial \theta = 0$ for $\theta = \hat{\theta}$, where θ can be a vector (see e. g. Eq. (7.104) for the parameters α and β of the NHPP with $m(t) = \alpha \beta t^{\beta-1}$). Using the property stated by Eq. (7.76), statistical tests for exponential distribution or for homogeneous Poisson processes (Appendix A8.2.2.2 and Section 7.2.3) can be applied to NHPPs as well. Furthermore, using the property stated by Eq. (7.77), the goodness-of-fit tests introduced in Appendix A8.3.2 & Section 7.5 (Kolmogorov-Smirnov, chi-square, Cramér-von Mises) can be used to verify agreement of observed data $t_1^*, \dots, t_n^* < T$ with a *postulated* $M_0(t)$. For the Kolmogorov-Smirnov test, the procedure given in Section 7.5.1 applies with

$$\hat{F}_n(t) = v(t) / v(T) \tag{7.79}$$

and

$$F_0(t) = M_0(t) / M_0(T), \tag{7.80}$$

where $v(t)$ is the observed number of events in $(0, t]$ (p. 520).

More difficult is the situation when the assumption that the underlying model is an NHPP *must also be verified by a statistical data analysis*, for instance with a goodness-of-fit test. The problem is not completely solved. However, the property given by Eqs. (7.76) and (7.77) can be used for goodness-of-fit of the NHPP with incompletely specified (up to the parameters) mean function $M_0(t)$. The chi-square test holds with the procedure given in Section 7.5.2 and Appendix A8.3.3. For a first evaluation, the Kolmogorov-Smirnov test (and tests based on a quadratic statistics) can be used, taking half (randomly selected) of the observations t_1^*, \dots, t_n^* to estimate the parameters and continuing with the whole sample the procedure given in Section 7.5.1 for the goodness-of-fit test [A8.11, A8.32].

7.6.3 Trend Tests

In reliability engineering one is often interested to test if there is a *monotonic trend* in the times between successive failures (interarrival times) of a repairable system with negligible repair (restoration) times. For instance, in order to detect *the end of an early failure period or the beginning of a wear-out period*. Such tests extend the tests for exponentiality or for homogeneous Poisson processes introduced in Section 7.2.3 (see also Sections 7.5, A8.2.1, A8.2.2, A8.3.2, A8.3.3). If the underlying point process can be approximated by a *renewal process*, a *graphical approach* can be used in detecting the presence of trends, see e.g. Fig. 7.13 for the case of early failures. In the case of a nonhomogeneous Poisson process (NHPP), a trend is given by an increasing or decreasing intensity $m(t)$, e. g. $\beta > 1$ or $\beta < 1$ in Eq. (7.99). Trend tests can also be useful in investigating what kind of alternative hypothesis should be considered when an assumption is to be made about the statistical properties of a given data set. However,

trend tests check, in general, a postulated hypothesis against a more or less broad alternative hypothesis; care is therefore necessary in drawing conclusions from this tests, and the basic rule given on p. 342 applies.

In the following, some trend tests used in reliability data analysis are discussed, among them the Laplace test (see e. g. [A8.1] for greater details).

7.6.3.1 Tests of an HPP versus an NHPP with increasing intensity

The homogeneous Poisson process (HPP) is a point process which count function $v(t)$ has stationary and independent Poisson distributed increments in nonoverlapping intervals (Eqs. (A7.41)). *Interarrival times in an HPP are independent and distributed according to the same exponential distribution $F(x) = 1 - e^{-\lambda x}$ (occurrence times are Erlangian distributed, Eqs. (A7.39), (A6.102)).* The parameter λ characterizes completely the HPP. λ is at the same time *the intensity of the HPP and the failure rate $\lambda(x)$ for all interarrival times, x starting by 0 at each occurrence time of the event considered (e.g. failure of a repairable system with negligible repair (restoration) times).* This *numerical equality* has been the cause for misinterpretations and misuses in practical applications, see e.g. [6.1, 7.11, A7.30]. The homogeneous Poisson process has been introduced in Appendix A7.2.5 as a particular renewal process. Considering $v(t)$ as the count function giving the number of events (failures) in $(0, t]$, Example A7.13 (Eq. (A7.213)) shows that:

For given (fixed) T and $v(T) = n$ (time censoring), the normalized arrival times $0 < \tau_1^/T < \dots < \tau_n^*/T < 1$ of a homogeneous Poisson process (HPP) have the same distribution as if they were the order statistic of n independent identically uniformly distributed random variables on $(0, 1)$* (7.81)

Similar results hold for an NHPP (Eq. (A7.206)):

For given (fixed) T and $v(T) = n$ (time censoring), the normalized arrival times $0 < M(\tau_1^*) / M(T) < \dots < M(\tau_n^*) / M(T) < 1$ of a nonhomogeneous Poisson process (NHPP) with mean value function $M(t)$ have the same distribution as if they were the order statistic of n independent identically uniformly distributed random variables on $(0,1)$. (7.82)

With the above transformations, properties of the uniform distribution can be used to support statistical tests on homogeneous and nonhomogeneous Poisson processes.

Let ω be a continuous uniformly distributed random variable with density

$$f_\omega(x) = 1 \quad \text{on } (0,1), \quad f_\omega(x) = 0 \quad \text{outside } (0,1), \quad (7.83)$$

and distribution function $F_\omega(x) = x$ on $(0,1)$. Mean and variance of ω are given by (Eqs. (A6.37) and (A6.44))

$$E[\omega] = 1/2 \quad \text{and} \quad \text{Var}[\omega] = 1/12. \quad (7.84)$$

The sum of n independent random variables ω has mean $n/2$ and variance $n/12$. The distribution function $F_{\omega_n}(x)$ of $\omega_1 + \dots + \omega_n$ is defined on $(0,n)$ and can be computed using Eq. (A7.12). $F_{\omega_n}(x)$ has been investigated in [A8.8], yielding to the conclusion that $F_{\omega_n}(x)$ rapidly approach a normal distribution as n increases. For practical applications one can assume that for given (fixed) T and $v(T) = n \geq 5$, the sum of the normalized arrival times $0 < \tau_1^*/T < \dots < \tau_n^*/T < 1$ of an HPP is distributed as

$$\Pr\left\{ \left[\left(\sum_{i=1}^n \tau_i^*/T \right) - n/2 \right] / \sqrt{n/12} \leq x \right\} \approx \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-y^2/2} dy, \quad -\infty < x < \infty, \quad (7.85)$$

(Eq. (A6.148)). Equation (7.85) can be used to test an HPP ($m(t) = \lambda$) versus an NHPP with increasing intensity $m(t) = dM(t)/dt$. Considering the observations (realizations) $0 < t_1^* < t_2^* < \dots < t_n^* < T$, the corresponding test procedure is:

1. Compute the statistic

$$\left[\left(\sum_{i=1}^n t_i^*/T \right) - n/2 \right] / \sqrt{n/12}, \quad t_i^* = i \text{ th arrival time.} \quad (7.86)$$

2. For given type I error α determine the critical value $t_{1-\alpha}$ ($1-\alpha$ quantile of the standard normal distribution, e.g. $t_{1-\alpha} \approx 1.64$ for $\alpha = 0.05$ (Tab. A9.1)).

3. Reject the hypothesis H_0 : the underlying point process is an HPP, against H_1 : the underlying process is an NHPP with increasing intensity, at $1-\alpha$ confidence, if $[(\sum_{i=1}^n t_i^*/T) - n/2] / \sqrt{n/12} > t_{1-\alpha}$; otherwise accept H_0 . (7.87)

A test based on Eqs. (7.86)-(7.87) is called *Laplace test* and was introduced by Laplace as a test of randomness. From Eq. (7.87) one recognizes that $\sum_{i=1}^n t_i^*/T$ is a sufficient statistic (Appendix A8.2.1). It can be noted that for H_1 true ($m(t)$ increasing), most of the arrival times (failures) tend to occur after $T/2$, increasing the term $[(\sum_{i=1}^n t_i^*/T) - n/2] / \sqrt{n/12}$. Example 7.20 gives an application. For failure censoring, Eq. (7.86) holds by summing over $n-1$ and taking $T = t_n^*$ (see e.g. [A8.1]).

A further possibility to test an HPP ($m(t) = \lambda$) versus an NHPP with increasing intensity $m(t) = dM(t)/dt$ is to use the statistic

$$\sum_{i=1}^n \ln(T/t_i^*). \quad (7.88)$$

Considering (Eq. (A7.213)) that for given (fixed) T and $v(T) = n$, the normalized arrival times $0 < \omega_1 = \tau_1^*/T < \dots < \omega_n = \tau_n^*/T < 1$ of an HPP have the same distribution as if they were the order statistic of n independent identically uniformly distributed random variables on $(0, 1)$, and that (Example 7.21) $2 \sum_{i=1}^n \ln(T/t_i^*) = 2 \sum_{i=1}^n \ln \omega_i$ has a χ^2 -distribution (Eq. (A6.103)) with $2n$ degrees of freedom

$$F(x) = \Pr\left\{ 2 \sum_{i=1}^n \ln(T/t_i^*) \leq x \right\} = \frac{1}{2^n (n-1)!} \int_0^x y^{n-1} e^{-y/2} dy, \quad (7.89)$$

the statistic given by Eq. (7.88) can be used to test an HPP ($m(t) = \lambda$) versus an NHPP with increasing intensity $m(t) = dM(t)/dt$. The corresponding test procedure is:

1. Compute the statistic

$$2 \sum_{i=1}^n \ln(T/t_i^*), \quad t_i^* = i \text{ th arrival time.} \quad (7.90)$$

2. For given type I error α determine the critical value $\chi_{2n, \alpha}^2$ (α quantile of the χ^2 -distribution, e. g. $\chi_{2n, \alpha}^2 \approx 7.96$ for $n=8$ & $\alpha=0.05$ (Table A9.2)).
3. Reject the hypothesis H_0 : the underlying point process is an HPP, against H_1 : the underlying process is an NHPP with increasing intensity, at $1-\alpha$ confidence, if $2 \sum_{i=1}^n \ln(T/t_i^*) < \chi_{2n, \alpha}^2$; otherwise accept H_0 . (7.91)

From Eq. (7.91) one recognizes that $2 \sum_{i=1}^n \ln(T/t_i^*)$ is a sufficient statistic (Appendix A8.2.1). It can be noted that for H_1 true ($m(t)$ increasing), $2 \sum_{i=1}^n \ln(T/t_i^*)$ tends to assume small values. Example 7.22 gives an application. For failure censoring, Eq. (7.90) holds by summing over $n-1$ and taking $T = t_n^*$ (see e. g. [A8.1]).

Example 7.20

In a reliability test, 8 failures have occurred in $T=10,000$ h and $t_1^* + \dots + t_8^* = 43,000$ h has been observed. Test with a risk $\alpha = 5\%$ (at 95% confidence), using the rule (7.87), the hypothesis H_0 : the underlying point process is an HPP, against H_1 : the underlying process is an NHPP with increasing intensity.

Solution

From Table A9.1 $t_{0.95} = 1.64 > (4.3-4)/0.816 = 0.367$ and H_0 can not be rejected.

Example 7.21

Let the random variable ω be uniformly distributed on $(0,1)$. Show that $\eta = -\ln(\omega)$ is distributed according to $F_\eta(t) = 1 - e^{-t}$ on $(0, \infty)$, and thus $2 \sum_{i=1}^n -\ln(\omega_i) = 2 \sum_{i=1}^n \eta_i = \chi_{2n}^2$.

Solution

Considering that for $0 < \omega < 1$, $-\ln(\omega)$ is a decreasing function defined on $(0, \infty)$, it follows that the events $\{\omega \leq x\}$ and $\{\eta = -\ln(\omega) > -\ln(x)\}$ are equivalent. From this (see also Eq. (A6.31)), $x = \Pr\{\omega \leq x\} = \Pr\{\eta > -\ln(x)\}$ and thus, using $-\ln(x) = t$, one obtains $\Pr\{\eta > t\} = e^{-t}$ and thus

$$F_\eta(t) = \Pr\{\eta \leq t\} = 1 - e^{-t}. \tag{7.92}$$

From Eqs. (A6.102)-(A6.104), $2 \sum_{i=1}^n -\ln(\omega_i) = 2 \sum_{i=1}^n \eta_i$ has a χ^2 -distribution with $2n$ degrees of freedom.

Example 7.22

In a reliability test, 8 failures have occurred in $T = 10,000$ h at 850, 1200, 2100, 3900, 4950, 5100, 8300, 9050 h. Test with a risk $\alpha = 5\%$ (at 95% confidence), using the rule (7.91), the hypothesis H_0 : the underlying point process is an HPP, against the alternative hypothesis H_1 : the underlying process is an NHPP with increasing intensity.

Solution

From Table A9.2, $\chi_{16, 0.05}^2 \approx 7.96 < 2(\ln(T/t_1^*) + \dots + \ln(T/t_8^*)) = 17.5$ and H_0 can not be rejected.

7.6.3.2 Tests of an HPP versus an NHPP with decreasing intensity

Tests of a homogeneous Poisson process (HPP) versus a nonhomogeneous Poisson process (NHPP) with a *decreasing intensity* $m(t) = dM(t)/dt$ can be deduced from those for increasing intensity given in section 7.6.3.1. Equations (7.85) and (7.89) remain true. However, if the intensity is decreasing, most of the failures tend to occur before $T/2$ and test procedure for the Laplace test has to be changed in:

1. Compute the statistic

$$\left[\left(\sum_{i=1}^n t_i^*/T \right) - n/2 \right] / \sqrt{n/12}, \quad t_i^* = i \text{ th arrival time.} \tag{7.93}$$

2. For given type I error α determine the critical value t_α (α quantile of the standard normal distribution, e. g. $t_\alpha \approx -1.64$ for $\alpha = 0.05$ (Tab. A9.1)).
3. Reject the hypothesis H_0 : the underlying point process is an HPP, against H_1 : the underlying process is an NHPP with *decreasing intensity*, at $1-\alpha$ confidence, if $[(\sum_{i=1}^n t_i^*/T) - n/2] / \sqrt{n/12} < t_\alpha$; otherwise accept H_0 . (7.94)

From Eq. (7.94) one recognizes that $\sum_{i=1}^n t_i^*/T$ is a sufficient statistic (Appendix A8.2.1). It can be noted that for H_1 true ($m(t)$ decreasing), most of the arrival times (failures) tend to occur before $T/2$, decreasing $[(\sum_{i=1}^n t_i^*/T) - n/2] / \sqrt{n/12}$. Example 7.23 gives an application. For *failure censoring*, Eq. (7.93) holds by summing over $n-1$ and taking $T = t_n^*$ (see e. g. [A8.1]).

For the test according to the statistic (7.88), the test procedure is:

1. Compute the statistic

$$2 \sum_{i=1}^n \ln(T/t_i^*), \quad t_i^* = i \text{ th arrival time.} \quad (7.95)$$

2. For given type I error α determine the critical value $\chi_{2n,1-\alpha}^2$ ($1-\alpha$ quantile of the χ^2 distribution, e. g. $\chi_{2n,1-\alpha}^2 \approx 26.3$ for $n=8$ & $\alpha=0.05$ (Table A9.2)).
3. Reject the hypothesis H_0 : the underlying point process is an HPP, against H_1 : the underlying process is an NHPP with *decreasing intensity*, at $1-\alpha$ confidence, if $2 \sum_{i=1}^n \ln(T/t_i^*) > \chi_{2n,1-\alpha}^2$; otherwise accept H_0 . (7.96)

From Eq. (7.96) one recognizes that $2 \sum_{i=1}^n \ln(T/t_i^*)$ is a sufficient statistic (Appendix A8.2.1). It can be noted that for H_1 true ($m(t)$ decreasing), $2 \sum_{i=1}^n \ln(T/t_i^*)$ tends to assume large values. Example 7.24 gives an application. For *failure censoring*, Eq. (7.95) holds by summing over $n-1$ and taking $T = t_n^*$ (see e.g. [A8.1]).

7.6.3.3 Heuristic Tests to distinguish between HPP and General Monotonic Trend

In some applications, only little information is available about the underlying point process describing failures occurrence of a complex repairable system. As in the previous sections, it will be assumed that repair times are neglected. Asked is a test to identify a monotonic trend of the failure intensity against a constant failure intensity given by a homogeneous Poisson process (HPP).

Consider first, investigations based on successive *interarrival times*. Such an investigation should be performed at the beginning of data analysis, also because

Example 7.23

Continuing Example 7.20, test using the rule (7.94) and the data of Example 7.20, with a risk $\alpha=5\%$ (at 95% confidence), the hypothesis H_0 : the underlying point process is an HPP, against the alternative hypothesis H_1 : the underlying process is an NHPP with decreasing intensity.

Solution

From Table A9.1, $t_{0,05} \approx -1.64 < 0.367$ and H_0 can not be rejected.

Example 7.24

Continuing Example 7.22, test using the rule (7.96) and the data of Example 7.22, with a risk $\alpha=5\%$ (at 95% confidence), the hypothesis H_0 : the underlying point process is an HPP, against the alternative hypothesis H_1 : the underlying process is an NHPP with decreasing intensity.

Solution

From Table A9.2, $\chi_{16,0.95}^2 \approx 26.3 > 2(\ln(T/t_1^*) + \dots + \ln(T/t_8^*)) = 17.5$ and H_0 can not be rejected.

it can quickly deliver a first information about a possible monotonic trend (e. g. interarrival times become more and more long or short). Moreover, if the underlying point process describing failures occurrence can be approximated by a *renewal process* (interarrival times are independent and identically distributed), procedures of Section 7.5 based on the empirical distribution function (EDF) have a *great intuitive appeal* and can be useful in testing for monotonic trends of the failure rate as well, see Examples 7.15-7.17 (Figs. 7.12-7.14). In particular, the *graphical approaches* given in Example 7.16 (Fig. 7.13) would allow the detection and quantification of an *early failure period*. The same would be for a *wear-out period*. Similar considerations hold if the involved point process can be approximated by a nonhomogeneous Poisson process (NHPP), see Sections 7.6.1 -7.6.3.2 and 7.7.

If a trend in successive interarrival times is recognized, but the underlying point process can not be approximated by a renewal process (including the homogeneous Poisson process (HPP)) or an NHPP, a further possibility is to consider the *observed failure time points* $t_1^* < t_2^* < \dots$ directly. As shown in Appendix A7.8.5, a mean value function $Z(t) = E[v(t)]$ can be associated to each point process, where $v(t)$ is the count function giving the number of failures occurred in $(0, t]$ ($Z_S(t)$ and $v_S(t)$ should be used for considerations at system level). From the observed failure time points (observed occurrence times) $t_1^* < t_2^* < \dots$, the empirical mean value function $\hat{Z}(t) = \hat{E}[v(t)]$ follows as

$$\hat{Z}(t) = \hat{E}[v(t)] = \begin{cases} 0 & \text{for } t < t_1^* \\ i & \text{for } t_i^* \leq t < t_{i+1}^*, \quad i = 1, 2, \dots \end{cases} \quad (7.97)$$

The mean value function $Z(t)$ corresponds to the renewal function $H(t)$ in a renewal process (Eq. (A7.15)); $z(t) = dZ(t)/dt$ is the *failure intensity* and correspond to the *renewal density* $h(t)$ in a renewal process (Eqs. (A7.18) & A7.24)). For a *homogeneous Poisson process* (HPP), $Z(t)$ takes the form (Eq. (A7.42))

$$Z(t) = E[v(t)] = \lambda t. \quad (7.98)$$

Each deviation from a straight line $Z(t) = a \cdot t$ is thus an indication for a possible trend (besides statistical deviations). As shown in Example A7.1 (Fig. A7.2) for a renewal process, early failures or wear-out gives a basically different shape of the underlying renewal function, a *convex shape* for the case of *early failures* and a *concave shape* for the case of *wear-out*. This property can be used to recognize the presence of trends in a point process, by considering the shape of the associated empirical mean value function $\hat{Z}(t)$ given by Eq. (7.97), see e. g. [7.24]. However,

such a procedure remains a very rough evaluation (see Fig. A7.2 for the case of a renewal process); care is thus necessary when extrapolating results, e. g. about the failure rate value after the early failure period or the percentage of early failures.

7.7 Reliability Growth

At the prototype qualification tests, the reliability of complex equipment & systems can be less than expected. Disregarding any imprecision of data or model used in calculating the predicted reliability (Chapter 2), such a discrepancy is often the consequence of *weaknesses* (errors, flaws, mistakes) during design or manufacturing. For instance, use of components or materials at their technological limits or with internal weaknesses, cooling, interface or EMC problems, transient phenomena, interference between hardware and software, assembling or soldering problems, damage during handling, transportation or testing, etc. Errors and flaws cause *defects* and *systematic failures*. Superimposed to these are *early failures* and failures with *constant failure rate* (wear-out should not be present at this stage). However,

a distinction between deterministic faults (defect & systematic failures) and random faults (early failures & failures with constant failure rate) is only possible with a cause analysis; such an analysis is necessary to identify and eliminate causes of observed faults (redesign for defects and systematic failures, screening for early failures, and repair for failures with constant failure rate), and initiates a learning process improving the reliability of the equipment or system considered.

Of course, *defects and systematic failures* can also be randomly distributed on the time axis, e.g. caused by a mission dependent time-limited overload, by software defects, or simply because of the system complexity. However, they still differ from failures, as they are *basically independent of operating time* (disregarding systematic failures which can appear only after a certain operating time, e.g. as for some cooling or software problems).

The aim of a *reliability growth program* is the *cost-effective* improvement of the item's reliability through successful correction/elimination of the *causes* of design or production weaknesses. Early failures should be precipitated with an appropriate screening (*environmental stress screening* (ESS)), see Section 8.2 for electronic components, Section 8.3 for electronic assemblies, and Section 8.4 for cost aspects. Considering that flaws found during reliability growth are in general *deterministic* (defects and systematic failures), reliability growth is performed during prototype qualification tests and *pilot production*, seldom for series-produced items (Fig. 7.16). Stresses during reliability growth are often higher than those expected in the field (as for ESS). Furthermore, the statistical methods used to *investigate reliability growth* are in general *basically different* from those given in Section 7.2 for standard reliability tests (e. g. to estimate or demonstrate a constant failure rate λ). This is because during the reliability growth program, design and/or production changes or modifications are introduced in the item(s) considered and statistical evaluation is *not restarted* after a change or modification.

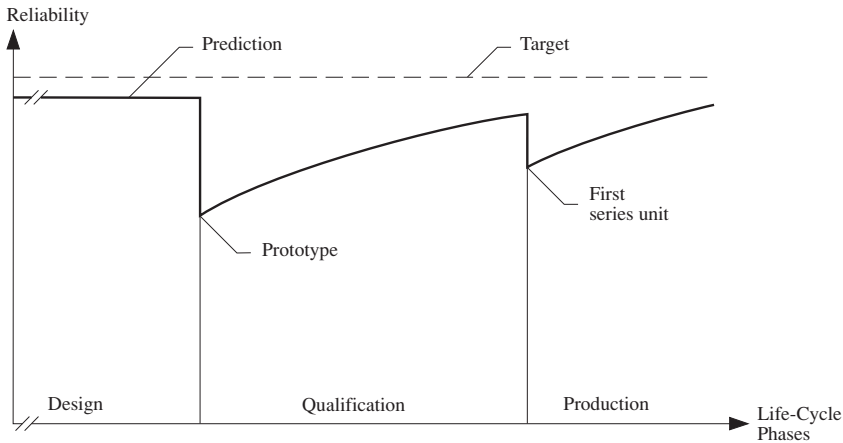


Figure 7.16 Qualitative visualization of a possible *reliability growth*

A large number of models have been proposed to describe reliability growth for hardware and software, see e.g. [5.68, 5.71, 7.31-7.49, A2.6(61014 & 61164)], some of them on the basis of theoretical considerations. A practice oriented model, proposed by J.T. Duane [7.36], refined in [7.35 (1975)], and carefully investigated in [A8.1], known also as the *AMSAA model*, assumes that the *flow of events* (system failures) constitutes a *nonhomogeneous Poisson process* (NHPP) with *intensity*

$$m(t) = \frac{dM(t)}{dt} = \alpha\beta t^{\beta-1}, \quad \alpha > 0, 0 < \beta < 1, t > 0, m(t)=0 \text{ for } t \leq 0, \quad (7.99)$$

and *mean value function*

$$M(t) = \alpha t^\beta, \quad \alpha > 0, 0 < \beta < 1, t > 0, M(t)=0 \text{ for } t \leq 0. \quad (7.100)$$

$M(t)$ gives the expected number of failures in $(0, t]$. $m(t)\delta t$ is the probability for one failure (any one) in $(t, t+\delta t]$ (Eq. (7.74)). It can be shown that for an NHPP, $m(t)$ is equal to the failure rate $\lambda(t)$ of the *first occurrence time* (Eq. (A7.209)). Thus, comparing Eqs. (7.99) & (A6.91) one recognizes that for the NHPP described by Eq. (7.99), the *first occurrence time* has a Weibull distribution; however,

$m(t)$ and $\lambda(t)$ are fundamentally different (see remarks on pp. 7, 344, 378, 426, 466, 524), and all others interarrival times do not follow a Weibull distribution and are neither independent nor identically distributed.

Because of the distribution of the *first occurrence time*, the NHPP process described by Eq. (7.99) is often (improperly) called *Weibull process*, causing great confusion. Also used is the term *power law process*. Nonhomogeneous Poisson processes are

investigated in Appendix A7.8.2.

In the following, an NHPP will be *assumed* as underlying model;

verification of this assumption is mandatory, and should be based also on physical considerations on the nature / causes of the defects and systematic failures involved (not only on statistical aspects).

If the underlying process is an NHPP, estimation of the model parameters (α and β in the case of Eq. (7.99)) can easily be performed using observed data.

Let us consider first the *time censored* case (Type I censoring) and assume that up to the given (fixed) time T , n events have occurred at times $0 < t_1^* < t_2^* < \dots < t_n^* < T$. t_1^*, t_2^*, \dots are the realizations (observations) of the arrival times $\tau_1^*, \tau_2^*, \dots$ and * indicates that t_1^*, t_2^*, \dots are points on the time axis and not independent realizations of a random variable τ with a given (fixed) distribution function (e.g. as in Figs. 1.1, 7.12, 7.14). Considering the main property of an NHPP, i. e., that the number of events in nonoverlapping intervals are *independent* and distributed according to (Eq. (A7.195))

$$\Pr\{k \text{ events in } (a, b]\} = \frac{(M(b) - M(a))^k}{k!} e^{-(M(b) - M(a))}, \quad \begin{matrix} k=0,1,2,\dots \\ 0 \leq a < b, M(0)=0. \end{matrix} \quad (7.101)$$

and the interpretation of the intensity $m(t)$ given by Eq. (7.74) or Eq. (A7.194), the following *likelihood function* (Eq. (A8.24)) can be found for the parameter estimation of the intensity $m(t)$

$$\begin{aligned} L &= m(t_1^*)e^{-M(t_1^*)}m(t_2^*)e^{-(M(t_2^*)-M(t_1^*))}\dots m(t_n^*)e^{-(M(t_n^*)-M(t_{n-1}^*))}e^{-(M(T)-M(t_n^*))} \\ &= e^{-M(T)} \prod_{i=1}^n m(t_i^*) . \end{aligned} \quad (7.102)$$

Equation (7.102) considers no event ($k=0$ in Eq. (7.101)) in each of the non-overlapping intervals $(0, t_1^*), (t_1^*, t_2^*), \dots, (t_n^*, T)$ and applies to an arbitrary NHPP. For the Duane model it follows that

$$L = e^{-M(T)} \prod_{i=1}^n m(t_i^*) = \alpha^n \beta^n e^{-\alpha T} \beta \prod_{i=1}^n t_i^{*\beta-1}, \quad (7.103)$$

or

$$\ln L = n \ln(\alpha\beta) - \alpha T + (\beta - 1) \sum_{i=1}^n \ln(t_i^*) .$$

The *maximum likelihood estimates* $\hat{\alpha}$ and $\hat{\beta}$ of the parameters α and β are then obtained from

$$\left. \frac{\partial \ln L}{\partial \alpha} \right|_{\alpha=\hat{\alpha}} = 0 \quad \text{and} \quad \left. \frac{\partial \ln L}{\partial \beta} \right|_{\beta=\hat{\beta}} = 0,$$

yielding

$$\hat{\beta} = \frac{n}{\sum_{i=1}^n \ln(T/t_i^*)} \quad \text{and} \quad \hat{\alpha} = \frac{n}{T\hat{\beta}}. \quad (7.104)$$

An estimate for the *intensity* of the underlying nonhomogeneous Poisson process is

$$\hat{m}(t) = \hat{\alpha} \hat{\beta} t^{\hat{\beta}-1}, \quad 0 < t < T. \quad (7.105)$$

With known values for $\hat{\alpha}$ and $\hat{\beta}$, Eq. (7.105) can be used to extrapolate the *attainable intensity* if the reliability growth process were to be continued with the *same statistical properties* for a further time span Δ after T , yielding

$$\hat{m}(T+\Delta) = \hat{\alpha} \hat{\beta} (T+\Delta)^{\hat{\beta}-1}, \quad \Delta > 0. \quad (7.106)$$

see Example 7.25 for a practical application.

In the case of *event censoring*, i.e., when the test is stopped at the occurrence of the n th event (Type II censoring), Eq. (7.104) holds by summing over $n-1$ and taking $T = t_n^*$, see e.g. [A8.1].

Interval estimation for the parameters α and β can be found, see for instance [A8.1].

For *goodness-of-fit-tests* one can consider the property of nonhomogeneous Poisson processes that, for *given* (fixed) T and knowing that n events have been observed in $(0, T)$, i.e. for given T & $v(T) = n$, the occurrence times $0 < \tau_1^* < \dots < \tau_n^* < T$ have the same distribution as if they were the *order statistic* of n independent and identically distributed random variables with density $m(t)/M(T)$, on $(0, T)$ (Eq. (A7.205)). For example, the *Kolmogorov-Smirnov test* (Section 7.5) can be used with $\hat{F}_n(t) = v(t)/v(T)$ (Eq. (7.79)) and $F_0(t) = M_0(t)/M_0(T)$ (Eq. (7.80)), see also Appendices A7.8.2 and A8.3.2. Furthermore, it holds that if $\tau_1^* < \tau_2^* < \dots$ are the occurrence times of an NHPP, then $\psi_1^* = M(\tau_1^*) < \psi_2^* = M(\tau_2^*) < \dots$ are the occurrence times in a *homogeneous Poisson process* (HPP) with *intensity one* (Eq. (A7.200)). Results for independent and identically distributed random variables, for HPP or for

Example 7.25

During the reliability growth program of a complex equipment, the following data was gathered: $T = 1200$ h, $n = 8$ and $\sum \ln(T/t_i^*) = 20$. Assuming that the underlying process can be described by a Duane model, estimate the intensity at $t = 1200$ h and the value attainable at $t + \Delta = 3000$ h if the reliability growth *would continue with the same statistical properties*.

Solution

With $T = 1200$ h, $n = 8$ and $\sum \ln(T/t_i^*) = 20$, it follows from Eq. (7.104) that $\hat{\beta} = 0.4$ and $\hat{\alpha} \approx 0.47$. From Eq. (7.105), the estimate for the intensity leads to $\hat{m}(1200) \approx 2.67 \cdot 10^{-3} \text{ h}^{-1}$ ($\hat{M}(1200) \approx 8$). The attainable intensity after an extension of the program for reliability growth by 1800 h is given by Eq. (7.106) as $\hat{m}(3000) \approx 1.54 \cdot 10^{-3} \text{ h}^{-1}$.

exponential distribution function can thus be used.

Important is also to note that for an NHPP, distribution and mean value of the random time $\tau_R(t)$ from an arbitrary (fixed) time point $t \geq 0$ to the next event (failure) are *independent of the process development up to the time t*. For $E[\tau_R(t)]$ it holds, in particular (Eq. (A7.197)),

$$E[\tau_R(t)] = \int_0^{\infty} \Pr\{\text{no event in } (t, t+x)\} dx = \int_0^{\infty} e^{-(M(t+x) - M(t))} dx. \quad (7.107)$$

Assuming thus, to have for a given (fixed) $t = t_0 > 0$

$$M(t_0+x) = M(t_0) + \lambda x \quad \text{or} \quad m(t_0+x) = \lambda, \quad t_0 \text{ given (fixed), } x > 0, \quad (7.108)$$

i. e. a constant failure rate λ after an *early failure period of length* t_0 , it follows that

$$E[\tau_R(t_0+x)] = 1/\lambda. \quad t_0 \text{ given (fixed), } x > 0. \quad (7.109)$$

Similarly, for

$$M(t_0+x) = M(t_0) + \alpha x^\beta \quad \text{or} \quad m(t_0+x) = \alpha \beta x^{\beta-1}, \quad t_0 \text{ given (fixed), } x > 0, \quad (7.110)$$

it follows that

$$E[\tau_R(t_0+0)] = \Gamma(1+1/\beta) / \alpha^{1/\beta}, \quad t_0 \text{ given (fixed),} \quad (7.111)$$

(Appendix A9.6 or Eq. (A6.92) with $\lambda = \alpha^{1/\beta}$). For repairable items (systems) with negligible repair (restoration) times, equations (7.108)-(7.111) give

a possibility, for modeling an early failures period followed by constant failure rate (Eqs.(7.108),(7.109)) or a period of constant failure rate followed by wear-out (7.110),(7.111)); this, in addition to the remarks on pp. 7, 428, 467, and Figs. 7.13 or A7.2 for non-repairable items (combination of models is also possible).

The *Duane model* often applies to electronic, electromechanical, and mechanical equipment and systems. It can also be used to describe the occurrence of *software defects (dynamic defects)*. However, other models have been discussed in the literature especially for software (Section 5.3.4). Among these, the *logarithmic Poisson model*, which assumes a *nonhomogeneous Poisson process* with intensity

$$m(t) = \frac{1}{\delta + \gamma t} \quad \text{or} \quad m(t) = \frac{\alpha + 1}{\beta + t}, \quad 0 < \alpha, \beta, \delta, \gamma < \infty, \quad t \geq 0. \quad (7.112)$$

For the logarithmic Poisson model, $m(t)$ is monotonically decreasing with $m(0) < \infty$ and $m(\infty) = 0$. Considering $M(0) = 0$, it follows that

$$M(t) = \frac{\ln(1 + \gamma t / \delta)}{\gamma} \quad \text{or} \quad M(t) = \ln(1 + t / \beta)^{\alpha+1}. \quad (7.113)$$

Models combining in a multiplicative way two possible mean value functions $M(t)$ have been investigated in [7.33] by assuming

$$M(t) = a \ln(1 + t / b) \cdot (1 - e^{-t/b}) \quad \text{and} \quad M(t) = \alpha t^\beta \cdot [1 - (1 + t / \gamma) e^{-t/\gamma}], \quad (7.114)$$

with $a, b, \alpha, \gamma > 0$, $0 < \beta < 1$, $t \geq 0$. In both cases, the intensity $m(t)$ grows from 0 to a maximum, from which it goes to 0 with a shape similar to that of the models given by Eq. (7.112).

The models described by Eqs. (7.100), (7.113) & (7.114) are based on *nonhomogeneous Poisson processes*, satisfying thus the properties discussed in Appendix A7.8.2. However,

although appealing, nonhomogeneous Poisson processes (NHPP) can not solve all reliability growth modeling problems, basically because of their intrinsic simplicity related to the assumption of independent increments (in nonoverlapping intervals).

The consequence of this assumption, is that the involved process (NHPP) is a process *without aftereffect* for which the waiting time to the next event from an arbitrary (fixed) time point t is independent of the process development up to time t (Eq. (7.75)). Furthermore, the failure rate referred to the first occurrence time τ_1^* is the intensity of the underlying NHPP, and τ_1^* characterizes thus the NHPP (follows from Eq. (A7.209))

$$\Pr\{\tau_1^* \leq t\} = 1 - e^{-M(t)} = 1 - e^{-\int_0^t m(x) dx},$$

or by comparing Eq. (7.75) for $t=0$ with Eq. (2.11), considering Eq. (2.7) & $M(0)=0$; see Point 2 on p.519 for the extension to the n th interarrival time $\eta_n = \tau_n^* - \tau_{n-1}^*$, $n > 1$). From the above considerations,

an NHPP (even less an HPP) can not be used to estimate the number of defects present in a software package (e.g. at $t=0$), see also [A7.30] for further comments.

In general, it is not possible to *fix a priori the model* to be used in a given situation. For hardware as well as for software, a *physical* motivation of the model, based on failure or defect (fault) *mechanisms / causes*, can help in such a choice. Having a suitable model, the next step should be to verify that assumptions made are compatibles with the model and, after that, to check the compatibility with data. Misuses or misinterpretations can occur, often because of dependencies between the involved random variables.

8 Quality & Reliability (RAMS) Assurance During the Production Phase (Basic Considerations)

Reliability (RAMS) assurance has to be continued during the *production phase*, coordinated with other quality assurance activities. In particular, for monitoring and controlling *production processes, item configuration, in-process and final tests, screening procedures, and collection, analysis & correction of defects and failures*. The last measure yields to a *learning process* whose purpose is to *optimize the quality of manufacture*, taking into account cost and time schedule limitations. This chapter introduces some basic aspects of quality and reliability (RAMS) assurance during production, discusses test and *screening procedures* for electronic components and assemblies, introduces the concept of *cost optimization* related to a test strategy and develops it for a cost optimized test and screening strategy at the *incoming inspection*. For greater details on qualification & monitoring of production processes one may refer to [7.1 - 7.5, 8.1 - 8.14]. Models for reliability growth are discussed in Section 7.7.

8.1 Basic Activities

The quality and reliability (RAMS) level achieved during the design and development phase must be retained during production (pilot and series production). The following basic activities support this purpose (see also Table A3.2, points 7-16).

1. Management of the *item's configuration* (review and release of the production documentation, control and accounting of changes and modifications).
2. Selection and *qualification of production facilities and processes*.
3. Monitoring and control of the *production procedures* (assembling, testing, transportation, storage, etc.).
4. *Protection against damage* during production (electrostatic discharge (ESD), mechanical, thermal, electrical stresses).
5. Systematic collection, analysis, and correction of *defects and failures* occurring during the item's production or testing (back to the *root cause*).
6. Quality and reliability (RAMS) assurance during *procurement* (documentation, incoming inspection, supplier audits).

7. *Calibration* of measurement and testing equipment.
8. Performance of *in-process and final tests* (functional and environmental).
9. *Screening* of critical components and assemblies. ⁺⁾
10. Optimization of the cost and time schedule for testing and screening (realization of a *test and screening strategy*).

Configuration management, monitoring of *corrective actions*, and some important aspects of *statistical quality control* and *reliability tests* have been considered in Section 1.3, Chapter 7, and Appendices A3–A5. The following sections present test and screening procedures for electronic components and assemblies, introduce the concept of test and screening strategy, and develop it for a cost optimized test and screening strategy at the *incoming inspection*. Although focused on electronic systems, many of the considerations given below applies to mechanical systems as well. For greater details on qualification & monitoring of production processes one may refer to [7.1-7.5, 8.1-8.14], see also Section 7.7 for reliability growth.

8.2 Testing and Screening of Electronic Components

8.2.1 Testing of Electronic Components

Most electronic components are tested today by the end user only on a *sampling basis*. To be cost effective, sampling plans should also consider the *quality assurance effort of the component's manufacturer*, in particular the confidence which can be given to the data furnished by him. In critical cases, the sample should be large enough to allow acceptance of more than 2 defective components (Sections 7.1.3, 3.1.4). *100% incoming inspection* can be necessary for components used in high reliability and/ or safety equipment and systems, new components, components with important changes in design or manufacturing, or for some critical components like power semiconductors, mixed-signal ICs, and complex logic ICs used at the limits of their *dynamic parameters*. This, so long as the fraction of defective remains over a certain limit, fixed by technical and cost considerations. Advantages of a 100% incoming inspection of electronic components are:

1. Quick detection of all relevant defects.
2. Reduction of the number of defective populated printed circuit boards (PCBs).
3. Simplification of the tests at PCB level.
4. Replacement of the defective components by the supplier.
5. Protection against *quality changes from lot to lot*, or within the same lot.

⁺⁾ Highly accelerated stress screening (HASS) must be critically evaluated before use.

Despite such advantages, different kinds of *damage* (overstress during testing, assembling, soldering) can cause problems at PCB level. *Defective probability* p (fraction of defective items) lies for today's established components in the range of a few ppm (part per million) for passive components up to some thousands of ppm for complex active components. In defining a *test strategy*, a possible *change* of p from lot to lot or within the same lot should also be considered. An example of test procedure for electronic components is given in Section 3.2.1 for VLSI ICs. Test strategies with cost consideration are developed in Section 8.4.

8.2.2 Screening of Electronic Components

Electronic components new on the market, produced in small series, subjected to an important redesign, or manufactured with insufficiently stable process parameters can exhibit *early failures*, i. e., failures during the first operating hours (seldom over thousand hours). Because of high replacement cost at equipment level or in the field, components exhibiting early failures should be eliminated before they are mounted on printed circuit boards. Defining a cost-effective *screening strategy* is difficult for at least following two reasons:

1. It may activate *failure mechanisms* that would not appear in field operation.
2. It could introduce *damage* (ESD, transients) which may be the cause of further *early failures*.

Ideally, screening should be performed by skilled personnel, be focused on the *failure mechanisms* which have to be activated, and *not cause damage or alteration*. Experience on a large number of components [3.2, 3.6, 8.22] shows that for *established technologies* and *stable process parameters*, *thermal cycles* for discrete (in particular power) devices and *burn-in* for ICs are the most effective steps to precipitate *early failures*. Table 8.1 gives *possible* screening procedures for electronic components used in *high reliability and/or safety* equipment and systems.

Screening procedures and sequences are in national and *international standards* [8.27, 8.28, 8.32]. The following is an example of a *screening procedure* for ICs in *hermetic packages for high reliability or safety applications*:

1. *High-temperature storage*: The purpose of high temperature storage is the stabilization of the thermodynamic equilibrium and thus of the IC electrical parameters. Failure mechanisms related to surface problems (contamination, oxidation, contacts) are activated. The ICs are placed on a metal tray (pins on the tray to avoid thermal voltage stresses) in an oven at 150°C for 24h. Should solderability be a problem, a protective atmosphere (N_2) can be used.
2. *Thermal cycles*: The purpose of thermal cycles is to test the ICs ability to endure rapid temperature changes, this activates failure mechanisms related to mechanical stresses caused by mismatch in *expansion coefficients* of the

Table 8.1 Example of test and screening procedures for electronic components used in *high reliability and/or safety* equipment & systems (apply in part also to SMD; see Section 7.1 for sampling plans)

Component	Sequence
Resistors	Visual inspection, 20 thermal cycles for resistor networks ($-40/+125^{\circ}\text{C}$)*, 48 h steady-state burn-in at 100°C and $0.6 P_N^*$, el. test at 25°C *
Capacitors	<ul style="list-style-type: none"> • Film: Visual inspection, 48 h steady-state burn-in at $0.9\theta_{\max}$ and U_N^*, el. test at 25°C ($C, \tan \delta, R_{IS}$)*, measurement of R_{IS} at 70°C* • Ceramic: Visual inspection, 20 thermal cycles (θ_{extr}^*), 48 h steady-state burn-in at U_N and $0.9\theta_{\max}^*$, el. test at 25°C ($C, \tan \delta, R_{IS}$)*, measurement of R_{IS} at 70°C* • Tantalum (solid): Visual inspection, 10 thermal cycles (θ_{extr}^*), 48 h steady-state burn-in at U_N and $0.9\theta_{\max}$ (low ZQ)*, el. test at 25°C ($C, \tan \delta, I_r$)*, meas. of I_r at 70°C* • Aluminum (wet): Visual inspection, forming (as necessary), 48 h steady-state burn-in at U_N and $0.9\theta_{\max}^*$, el. test at 25°C ($C, \tan \delta, I_r$)*, measurement of I_r at 70°C*
Diodes (Si)	Visual inspection, 30 thermal cycles ($-40/+125^{\circ}\text{C}$)*, 48 h reverse bias burn-in at 125°C *, el. test at 25°C ($I_r, U_F, U_{R\min}$)*, seal test (fine/gross leak)**
Transistors (Si)	Visual inspection, 20 thermal cycles ($-40/+125^{\circ}\text{C}$)*, 50 power cycles ($25/125^{\circ}\text{C}$, ca. 1 min on / 2 min off) for power elements*, el. test at 25°C ($\beta, I_{CEO}, U_{CEO\min}$)*, seal test (fine/gross leak)**
Optoelectronic	<ul style="list-style-type: none"> • LED, IRED: Visual inspection, 72 h high temp. storage at 100°C*, 20 thermal cycles ($-20/+80^{\circ}\text{C}$)*, el. test at 25°C ($U_F, U_{R\min}$)*, seal test (fine/gross leak)** • Optocoupler: Visual inspection, 20 thermal cycles ($-25/100^{\circ}\text{C}$), 72 h reverse bias burn-in (HTRB) at 85°C*, el. test at 25°C ($I_C / I_F, U_F, U_{R\min}, U_{CEsat}, I_{CEO}$), seal test (fine/gross leak)**
Digital ICs	<ul style="list-style-type: none"> • BiCMOS: Visual inspection, reduced el. test at 25°C, 48 h dyn. burn-in at 125°C*, el. test at 70°C*, seal test (fine/gross leak)** • MOS (VLSI): Visual inspection, reduced el. test at 25°C (rough functional test, I_{DD}), 72 h dyn. burn-in at 125°C*, el. test at 70°C*, seal test (fine/gross leak)** • CMOS (VLSI): Visual inspection, reduced el. test at 25°C (rough functional test, I_{DD}), 48 h dyn. burn-in at 125°C*, el. test at 70°C*, seal test (fine/gross leak)** • EPROM, EEPROM (>1M): Visual inspection, programming (CHB), high temp. storage ($48\text{ h}/125^{\circ}\text{C}$), erase, programming (inv. CHB), high temp. storage ($48\text{ h}/125^{\circ}\text{C}$), erase, el. test at 70°C, seal test (fine/gross leak)**
Linear ICs	Visual inspection, reduced el. test at 25°C (rough functional test, I_{CC} , offsets), 20 thermal cycles ($-40/+125^{\circ}\text{C}$)*, 96 h reverse bias burn-in (HTRB) at 125°C with red. el. test at 25°C *, el. test at 70°C *, seal test (fine/gross leak)**
Hybrid ICs	Visual inspection, high temp. storage ($24\text{ h}/125^{\circ}\text{C}$), 20 thermal cycles ($-40/+125^{\circ}\text{C}$), constant acceleration ($2,000$ to $20,000 g_n/60\text{ s}$)*, red. el. test at 25°C , 96 h dynamic burn-in at 85 to 125°C , el. test at 25°C , seal test (fine/gross leak)**

* sampling basis; + hermetic packages; el. = electrical, red. = reduced, N = rated value, CHB = checkerboard

material used. Thermal cycles are generally performed air to air in a two-chamber oven (transfer from low to high temperature chamber and vice versa using a lift). The ICs are placed on a metal tray (pins on the tray to avoid thermal voltage stresses) and subjected to at least 10 thermal cycles from -65 to $+150^{\circ}\text{C}$ (transfer time $\leq 1\text{min}$, time to reach the specified temperature $\leq 15\text{min}$, dwell time at the temperature extremes $\geq 10\text{min}$). Should solderability be a problem, a protective atmosphere (N_2) can be used.

3. *Constant acceleration*: The purpose of the constant acceleration is to check the mechanical stability of die-attach, bonding, and package. This step is only performed for ICs in hermetic packages, when used in critical applications. The ICs are placed in a centrifuge and subjected to an acceleration of $30,000g_n$ ($300,000\text{m/s}^2$) for 60 seconds (generally z-axis only).
4. *Burn-in*: Burn-in is a relatively expensive, but efficient screening step that provokes for ICs up to 80% of the chip-related and 30% of the package-related *early failures*. The ICs are placed in an oven at 125°C for 24 to 168h and are operated statically or dynamically at this temperature (cooling under power at the end of burn-in is often required). Ideally, ICs should operate with electrical signals as in the field. The consequence of the high burn-in temperature is a *time acceleration factor* A often given by the Arrhenius model (Eq. (7.56))

$$A = \frac{\lambda_2}{\lambda_1} \approx e^{\frac{E_a}{k} \left(\frac{1}{T_1} - \frac{1}{T_2} \right)},$$

where E_a is the *activation energy*, k the Boltzmann's const. ($8.6 \cdot 10^{-5} \text{eV/K}$), and λ_1 and λ_2 are the failure rates at chip temperatures T_1 and T_2 (in K), respectively, see Fig. 7.10 for a graphical representation. The *activation energy* E_a varies according to the *failure mechanisms* involved. *Global average values* for ICs lie between 0.3 and 0.7eV. Using Eq. (7.56), the burn-in duration can be calculated for a given application. For instance, if the period of early failures is 3,000h, $\theta_1 = 55^{\circ}\text{C}$, and $\theta_2 = 130^{\circ}\text{C}$ (junction temp. in $^{\circ}\text{C}$), the effective burn-in duration would be of about 50h for $E_a \approx 0.65\text{eV}$ and 200h for $E_a \approx 0.4\text{eV}$ (Fig. 7.10). It is often difficult to decide whether a *static* or a *dynamic burn-in* is more effective. Should surface, oxide, and metallization problems be dominant, a static burn-in is better. On the other hand, a dynamic burn-in activates practically all failure mechanisms. It is therefore important to make such a choice on the basis of practical experience.

5. *Seal*: A seal test is performed to check the seal integrity of the cavity around the chip in hermetically-packaged ICs. It begins with the *fine leak test*: ICs are placed in a vacuum (1h at 0.5mmHg) and then stored in a helium atmosphere under pressure (ca. 4h at 5atm); after a waiting period in open air (30min), helium leakage is measured with the help of a specially

calibrated mass spectrometer (required sensitivity approx. $10^{-8}\text{atm cm}^3/\text{s}$, depending on the cavity volume). After the fine leak test, ICs are tested for *gross leak*: ICs are placed in a vacuum (1 h at 5 mmHg) and then stored under pressure (2 h at 5 atm) in fluorocarbon FC-72; after a short waiting period in open air (2 min), the ICs are immersed in a fluorocarbon indicator bath (FC-40) at 125°C ; a continuous stream of small bubbles or two large bubbles from the same place within 30 s indicates a defect.

8.3 Testing and Screening of Electronic Assemblies

Electrical testing of electronic assemblies, for instance populated printed circuit boards (PCBs), can be basically performed in one of the following ways:

1. Functional test within the assembly or unit in which the PCB is used.
2. Functional test with help of a functional test equipment.
3. In-circuit test followed by a functional test with the assembly or unit in which the PCB is used.

The first method is useful for small series production. It assumes that components have been tested (or are of sufficient quality) and that automatic or semi-automatic *localization* of defects on the PCB is possible. The second method is suitable for large series production, in particular from the point of view of protection against *damage* (ESD, backdriving, mechanical stresses), but can be expensive. The third and most commonly used method assumes the availability of an appropriate *in-circuit test equipment*. With such an equipment, each component is electrically isolated and tested statically or quasi-statically. This can be sufficient for passive components and discrete semiconductors, as well as for SSI and MSI ICs, but it cannot replace an electrical test at the incoming inspection for LSI and VLSI ICs (functional tests on in-circuit test equipment are limited to some few 100kHz and dynamic tests (Fig. 3.4) are not possible). Thus, even if in-circuit testing is used, incoming inspection of critical components should not be omitted. A further disadvantage of in-circuit testing is that the outputs of an IC can be forced to a LOW or a HIGH state. This stress (*backdriving*) is generally short (50ns), but may be sufficient to cause damage to the IC in question. In spite of this, and of some other problems (polarity of electrolytic capacitors, paralleled components, tolerance of analog devices), in-circuit testing is today the most effective means to test populated printed circuit boards (PCBs), on account of its good *defect localization* capability.

Because of the large number of components & solder joints involved, the *defective probability* of a PCB can be relatively high in stable production conditions too. Experience shows that for a PCB with about 500 components and 3,000 solder joints,

the following *indicative values* can be expected (see Table 1.3 for fault report forms):

- 0.5 to 2% defective PCBs (often for 3/4 assembling and 1/4 components),
- 1.5 defects per defective PCB (mean value).

Considering such figures, it is important to remember that defective PCBs are often *reworked* and that a repair or rework can have a negative influence on the quality and reliability of a PCB.

Screening populated printed circuit boards (PCBs) or assemblies with higher integration level is generally a difficult task, because of the many different technologies involved. Experience on a large number of PCBs [8.22(1989), 3.76] leads to the following *screening procedure* which can be recommended for PCBs used in *high reliability and/or safety applications* (SMT and mixed technology):

1. Visual inspection and reduced electrical test.
2. 100 thermal cycles ($0^{\circ}\text{C}/+80^{\circ}\text{C}$) with temperature gradient $\leq 5^{\circ}\text{C}/\text{min}$ (within the components), dwell time ≥ 10 min after the thermal equilibrium has been reached within $\pm 5^{\circ}\text{C}$, power off during cooling (gradient $\geq 20^{\circ}\text{C}/\text{min}$ only if this also occurs in the field and is compatible with the PCB technology).
3. 15 min random vibration at $2 g_{\text{rms}}$, 20 - 500Hz (to be performed if significant vibrations occur in the field).
4. 48 h *run-in* at ambient temperature, with periodic power on/off switching.
5. Final electrical and functional test.

Extensive investigations on *SMT assemblies* [3.92, 3.81, 3.79(96,02,05,0.8,11), 3.90], show that basically two different deformation mechanisms can be present in solder joints (Section 3.4), *grain boundary sliding* at rather low temperature gradients and low stiffness of the structure component – PCB, and *dislocation climbing* at higher temperature gradients and high stiffness (e.g. for leadless ceramic components);

for this reason, screening of populated PCBs in SMT should be avoided if the temperature gradient occurring in the field is not known.

Preventive actions, to build in quality and reliability during manufacturing, have to be preferred. This holds in particular for lead-free solder joints, which are more sensitive than Sn-Pb solder joints to manufacturing flaws or defects, mechanical vibrations, and fast thermal cycles (see also Sections 3.4 & 5.1.5.4).

The above procedure can be considered as an *environmental stress screening* (ESS), often performed on a 100% basis in a series production of PCBs used in *high reliability and/or safety applications* to provoke *early failures*. It can serve as a basis for screening at higher integration levels.

Thermal cycles can be combined with power on / off switching or vibration to increase effectiveness. However, in general a *screening strategy* for PCBs (or at higher integration level) should be established on a case-by-case basis, and be periodically reconsidered (reduced or even canceled if the percentage of early failures drops below a given value, 1% for instance).

Burn-in at assembly level is often used as an accelerated reliability test to validate a predicted assembly's failure rate λ_S . Assuming that the assembly consists of elements E_1, \dots, E_n in series, with failure rates $\lambda_1(T_1), \dots, \lambda_n(T_1)$ at temperature T_1 and activation factors A_1, \dots, A_n for a stress at temperature T_2 , the assembly failure rate $\lambda_S(T_2)$ at temperature T_2 can be calculated from Eqs. (2.19) & (7.57) as

$$\lambda_S(T_2) = \sum_{i=1}^n A_i \lambda_i(T_1).$$

Evaluation of the experimentally obtained failure rate $\lambda_S(T_2)$ can follow as given in Section 7.2.3. However, because of the many different technologies often used in an assembly (e.g. populated PCB), T_2 is generally chosen $< 100^\circ\text{C}$. Equation (7.57) basically holds for series structures. In the presence of *redundancy*, distinction should be made if the assembly is repairable or not during burn-in. However,

in both cases, assuming $\lambda_i(t) = \lambda_i$, the contribution of redundancies to λ_S can often be neglected for a burn-in duration $\ll 1/\lambda_m$, where $\lambda_m = \max\{\lambda_1, \dots, \lambda_n\}$ (Eq. (6.157) and Fig. 2.7).

8.4 Test and Screening Strategies, Economic Aspects

8.4.1 Basic Considerations

In view of the optimization of cost associated with testing and screening during production, each manufacturer of high-performance equipment and systems is confronted with the following question:

What is the most cost-effective approach to eliminate all defects, systematic failures, and early failures prior to shipment to the customer?

The answer to this question depends essentially on the level of quality, reliability, and safety required for the item considered, the consequence of a defect or a failure, the effectiveness of each test or screening step, as well as on the direct and *deferred cost* involved (warranty cost for instance). A *test and screening strategy* should thus be *tailored* to the item considered, in particular to its complexity, technology, and production procedures, but also to the facilities and skill of the manufacturer. In setting up such a strategy, the following aspects must be considered:

1. *Cost equations* should include deferred cost (for instance, *warranty cost* and *cost for loss of image*).

2. Testing and screening should begin at the lowest level of integration and be *selective*, i. e., consider the effectiveness of each test or screening step.
3. *Qualification tests* on prototypes are important to eliminate *defects* and *systematic failures*, they should include performance, environmental & reliability tests.
4. Testing and screening should be carefully planned to allow *high interpretability* of the results, and be supported by a *quality data reporting system* (Fig. 1.8).
5. Testing and screening strategy should be discussed early in the design phase, during *design reviews*.

Figure 8.1 can be used as start point for the development of a *test and screening strategy* at the assembly level.

A basic relationship between *test strategy and cost* is illustrated in the example of Fig. 8.2, in which two different strategies are compared. Both cases in Fig. 8.2 deal with the production of a stated quantity of equipment or systems for which a total of 100,000 ICs of a given type are necessary. The ICs are delivered with a *defective probability* $p = 0.5\%$. During production, additional defects occur

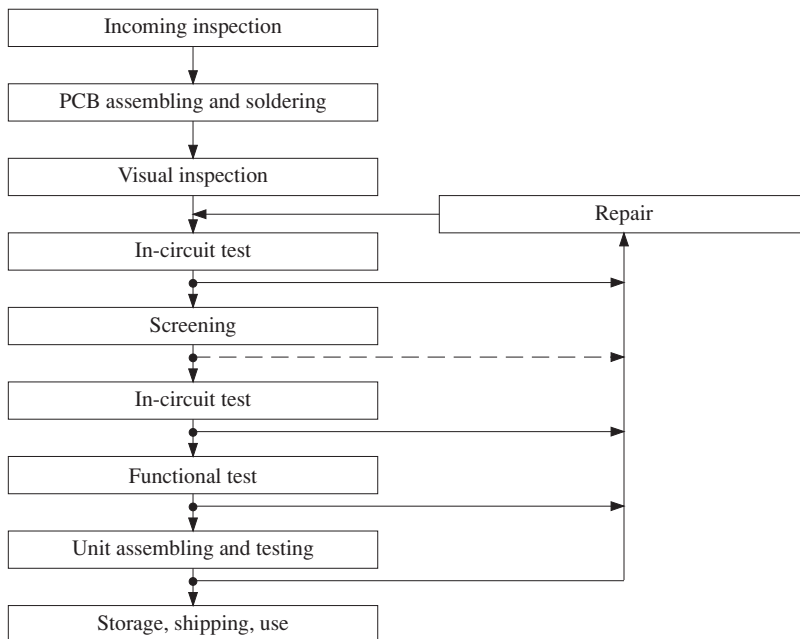
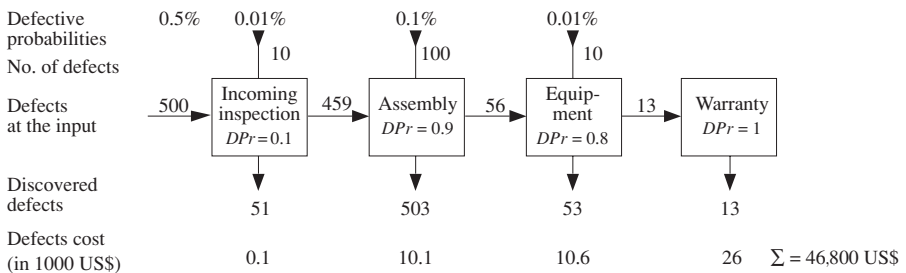


Figure 8.1 Flow chart as a basis for the *development of a test and screening strategy* for electronic assemblies (e. g. populated printed circuit boards (PCBs))

as a result of incorrect handling, mounting, etc., with probabilities of 0.01% at the incoming inspection, 0.1% at assembly level, and 0.01% at equipment level. The cost of eliminating a defective IC is assumed to be \$2 (US\$) at the incoming inspection, \$20 at assembly level, \$200 at equipment level, and \$2,000 during warranty. The two test strategies differ in the probability (*DPr*) of detecting and eliminating a defect. This probability is for the four levels 0.1, 0.9, 0.8, 1.0 in the first strategy and 0.95, 0.9, 0.8, 1.0 in the second strategy. It is assumed, in this example, that the additional cost to improve the detection probability at incoming inspection (+ \$20,000) are partly compensated by the savings in the test at the assembly level (− \$10,000). As Fig. 8.2 shows, total cost of the second test strategy are (for this example) lower (\$21,900) than those of the first one.

Number of defects and cost are *in all* this kind of considerations *expected values* (means of random variables). The use of arithmetic means in the example of Fig. 8.2, on the basis of 100,000 ICs at the input, is for convenience only.

Strategy a



Strategy b

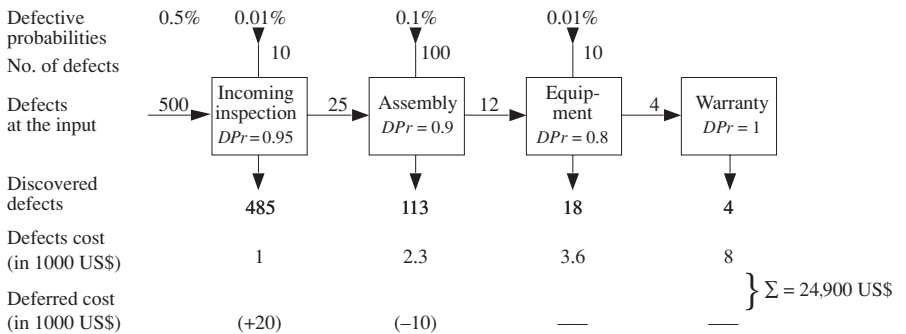


Figure 8.2 Comparison between two possible test strategies (figures for defects and cost have to be considered as *expected values*, number of defects on the basis of 100,000 ICs at the input): a) Emphasis on assembly test; b) Emphasis on incoming inspection (*DPr* = detection probability)

Models like that of Fig. 8.2 can be used to identify *weak points* in the production process (e. g. with respect to the defective probabilities at the different production steps) or to evaluate the effectiveness of additional measures introduced to decrease quality cost.

8.4.2 Quality Cost Optimization at Incoming Inspection Level

In this section, *optimization of quality cost* in the context of a *testing and screening strategy* is solved for the case of the choice between a *100% incoming inspection* and an incoming inspection on a sampling basis. Two cases will be distinguished, incoming inspection without screening (test only, illustrated by Fig. 8.3 and Fig. 8.4) and incoming inspection with screening (test and screening, illustrated by Fig. 8.5 and Fig. 8.6).^{+) The following notation is used:}

A_t = probability of acceptance at the sampling test (i. e., probability of having no more than c defective components in a sample of size n (function of p_d , given by Eq. (A6.121) with $p=p_d$ and $k=c$, see also Fig. 7.3 for a graphical solution using the Poisson approximation)

A_s = same as A_t , but for screening (screening with test)

c_d = deferred cost per defective component

c_f = deferred cost per component with early failure

c_r = replacement cost per component at the incoming inspection (c_r includes component cost and cost for test and/or screening, as appropriate)

c_t = testing cost per component (test only)

c_s = screening cost per component (c_s includes cost for screening and test)

C_t = expected value (mean) of the total cost (direct and deferred) for incoming inspection without screening (test only) of a lot of N components

C_s = expected value (mean) of the total cost (direct and deferred) for incoming inspection with screening (screening with test) of a lot of N components

n = sample size

N = lot size

p_d = defective probability (defects are recognized at the test)

p_f = probability for an early failure (early failures are precipitated by the screening)

^{+) The concept of average outgoing quality (Eq. (7.11)) can be used to compute the mean percentage of components with defects or early failures (as function of p_d or p_f) that reach the assembly line in the case of a sampling test at the incoming inspection.}

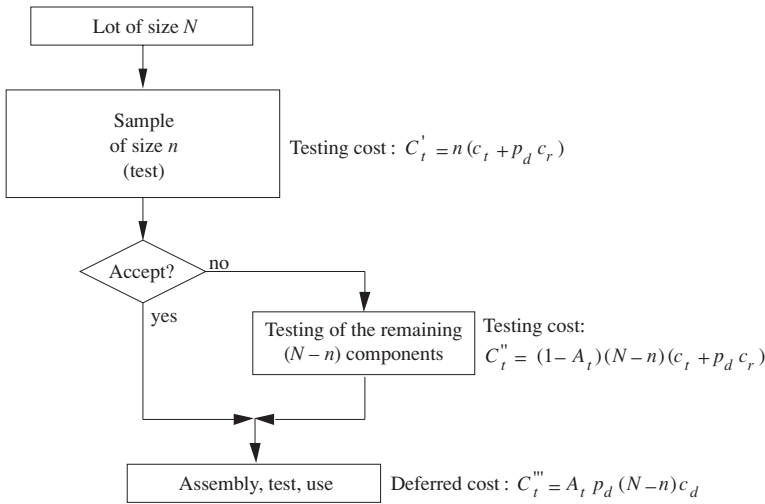


Figure 8.3 Model for quality cost optimization (direct and deferred cost) at the *incoming inspection without screening* of a lot of N components (all cost are expected values, see Fig. 8.5 for screening)

Consider first the *incoming inspection without screening* (test only). The corresponding model is shown in Fig. 8.3. From Fig. 8.3, the following *cost equation* can be established for the *expected value* (mean) of the total cost C_t

$$\begin{aligned}
 C_t &= C_t' + C_t'' + C_t''' \\
 &= n(c_t + p_d c_r) + (N - n)(1 - A_t)(c_t + p_d c_r) + (N - n)A_t p_d c_d \\
 &= N(c_t + p_d c_r) + (N - n)A_t [p_d c_d - (c_t + p_d c_r)].
 \end{aligned} \tag{8.1}$$

Investigating Eq. (8.1) leads to the following cases:

1. For $p_d = 0$, $A_t = 1$ and thus

$$C_t = n c_t. \tag{8.2}$$

2. For a 100% incoming inspection, $n = N$ and thus

$$C_t = N(c_t + p_d c_r). \tag{8.3}$$

3. Considering the term related to $(N - n)A_t$, it follows that

$$c_d < c_r + \frac{c_t}{p_d} \tag{8.4}$$

yields

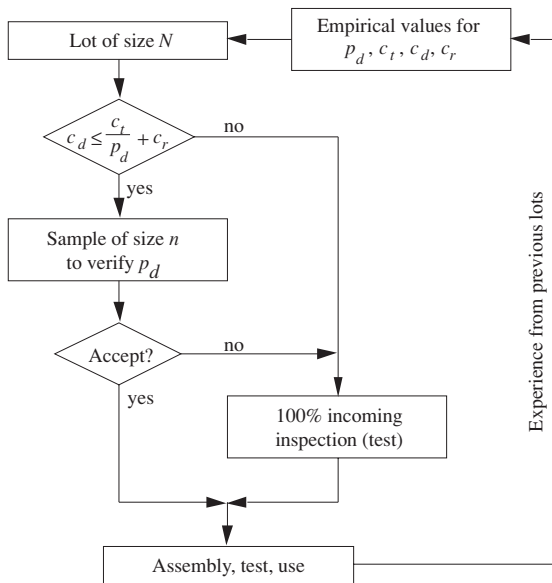


Figure 8.4 Practical realization of the procedure described by the model of Fig. 8.3

$$C_t < N(c_t + p_d c_r),$$

and thus a *sampling test is more cost effective.*

4. On the other hand,

$$c_d > c_r + \frac{c_t}{p_d} \tag{8.5}$$

yields

$$C_t > N(c_t + p_d c_r)$$

and thus, a 100% incoming inspection is more cost effective.

A practical realization of the procedure according to the model of Fig. 8.3 is given in Fig. 8.4. The sample of size n , to be tested instead of the 100% incoming inspection if the inequality (8.4) is fulfilled, is used to verify the value of p_d , which for the actual lot can differ from the assumed one (estimation of p_d using results of Section 7.1.1, or demonstration of $p_{dactual} < c_t / (c_d - c_r)$ for given c_d, c_r, c_t , e.g. using one-sided sampling plan with $AQL = c_t / (c_d - c_r)$, $AQL < c_t / (c_d - c_r)$ or $LTPD = c_t / (c_d - c_r)$, see the considerations on pp. 306-307 to fix the values for n and c).

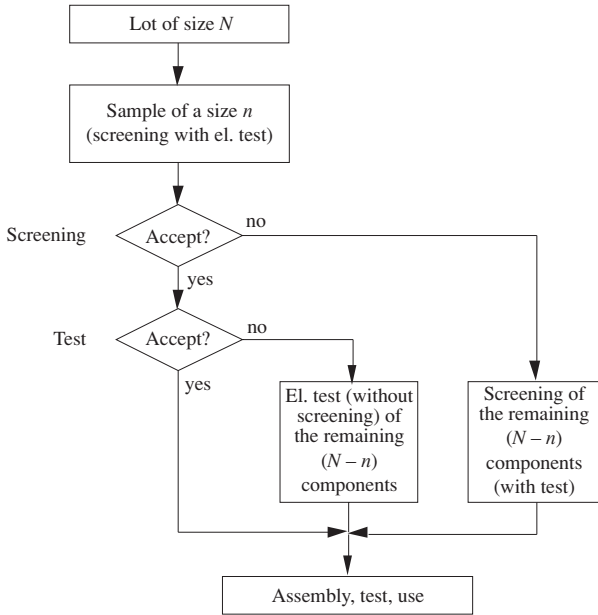


Figure 8.5 Model for quality cost optimization (direct and deferred cost) at the *incoming inspection with screening* of a lot of N components (all cost are expected values; screening includes test)

As a second case, let us consider the situation of an *incoming inspection with screening* (Section 8.2). Figure 8.5 gives the corresponding model and leads to the following *cost equation* for the expected value (mean) of the total cost C_s ⁺

$$\begin{aligned}
 C_s &= n[c_s + (p_f + p_d)c_r] + (N-n)A_s[p_f c_f + A_t p_d c_d + (1 - A_t)(c_t + p_d c_r)] \\
 &\quad + (N-n)(1 - A_s)[c_s + (p_f + p_d)c_r] \\
 &= N[c_s + (p_f + p_d)c_r] + (N-n)A_s[p_f c_f + A_t p_d c_d \\
 &\quad + (1 - A_t)(c_t + p_d c_r) - (c_s + (p_f + p_d)c_r)].
 \end{aligned}
 \tag{8.6}$$

Considering the term related to $(N-n)A_s$, it follows that for

$$p_f c_f + A_t p_d c_d + (1 - A_t)(c_t + p_d c_r) < c_s + (p_f + p_d)c_r
 \tag{8.7}$$

a sampling screening (with test) is *more cost effective* than a 100% screening (with test). A practical realization of the procedure according to the model of Fig. 8.5 is given in Fig. 8.6. As in Fig. 8.4, the sample of size n to be screened instead of the 100% screening if the inequality (8.7) is fulfilled, is used to verify the values of p_d and p_f , which for the actual lot can differ from the assumed ones (see the

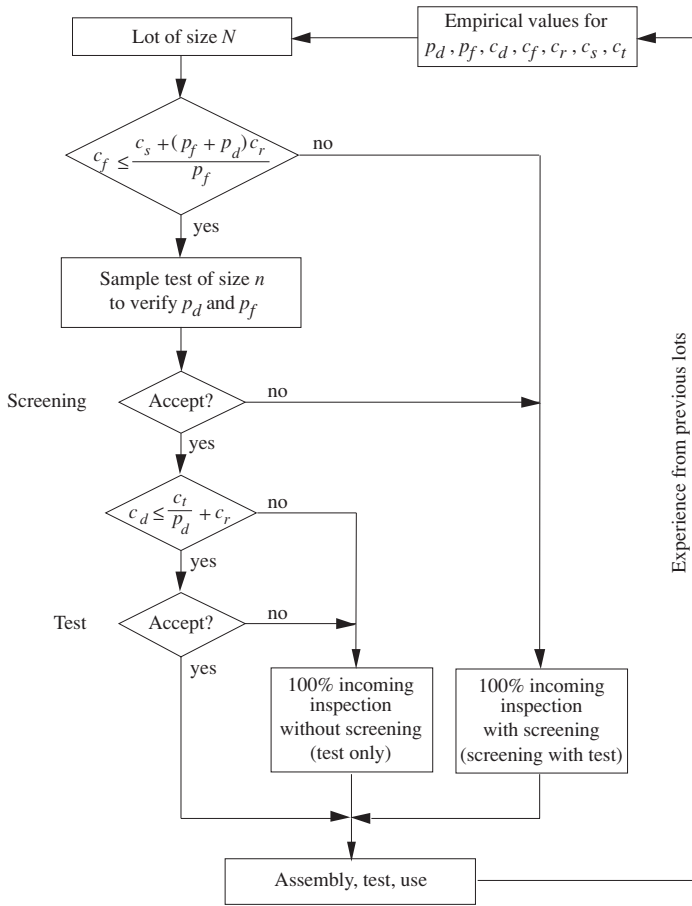


Figure 8.6 Practical realization of the procedure described by Fig. 8.5 (screening includes test)

considerations on p. 369 to fix the values for n and c). The first inequality in Fig. 8.6 is valid for

$$p_f c_f \gg A_t p_d c_d + (1 - A_t)(c_t + p_d c_r),$$

i. e. for $p_f c_f \gg p_d c_d$, by assuming $A_t \rightarrow 1$ and considering that early failures generally appear in the field; it can be refined to better satisfy the inequality (8.7), as necessary. The second inequality in Fig. 8.6 refers to the cost for incoming inspection without screening (inequality (8.4)), and uses the actual p_d , obtained from the sample test of size n .

8.4.3 Procedure to handle first deliveries

Components, materials, and externally manufactured subassemblies or assemblies should be submitted at the *first delivery* to an appropriate selection procedure. Part of this procedure can be performed in cooperation with the manufacturer to avoid duplication of efforts. Figure 8.7 gives the basic structure of such a procedure, see Sections 3.2 and 3.4 for some examples of qualification tests for components and assemblies.

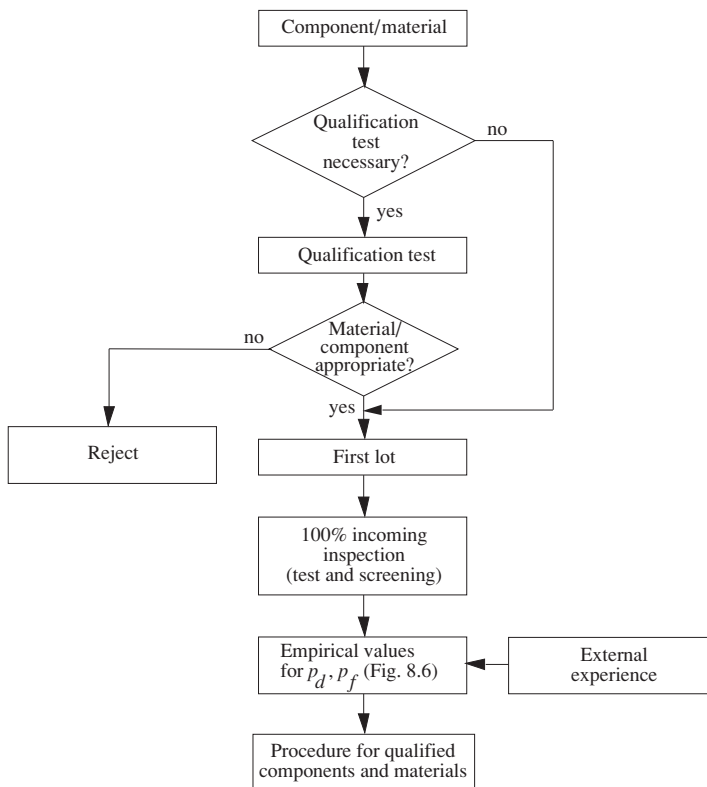


Figure 8.7 Selection procedure for non qualified components and materials

Appendices (A1 - A11)

A1 Terms and Definitions

Appendix A1 *defines and comments* on the terms most commonly used in reliability engineering (Fig. A1.1). Table 5.4 (p. 162) extends this appendix to software quality (see also [A1.5, A1.6]). Attention has been paid to the adherence to relevant international standards [A1.1 - A.1.7] and recent trends [A1.4], respecting coherence (in particular in the definition/discussion on Fault, *MTBF*, *MTTF*, *MTTR*, $R(t)$, $\lambda(t)$).

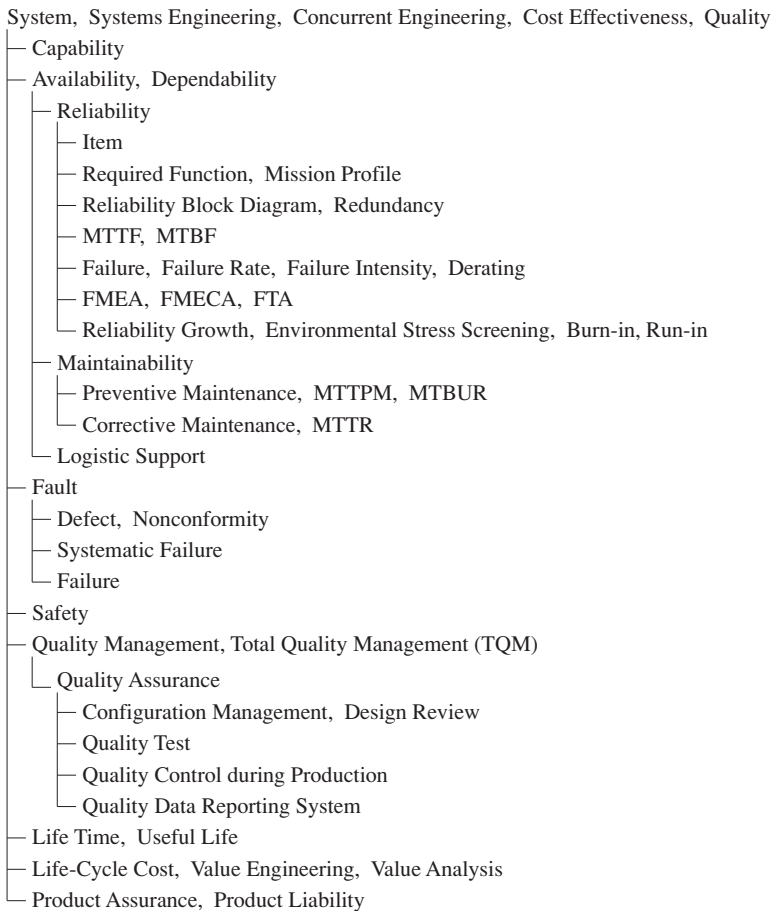


Figure A1.1 Terms most commonly used in reliability (RAMS) engineering

Availability, Instantaneous Availability, Point Availability (PA(t)) [A1.4]

Probability that the item is in a state to perform as required at a given instant.

Perform as required means *perform the required function under stated conditions*. At system level, $PA_S(t)$ is used (system refers in this book, and often in practical applications, to the highest integration level of the item considered). *Instantaneous availability* is often used. The use of $A(t)$ should be avoided, to elude confusion with other kind of availability (e. g. average availability $AA(t)$, mission availability $MA(T_0, t_0)$, and work-mission availability $WMA(T_0, x)$ as given in Section 6.2). A qualitative definition, focused on *ability*, is also possible and belongs to the concept of *dependability*. The term *item* stands for a structural unit of arbitrary complexity. *Stated conditions* generally refer to given environmental conditions, continuous operation (item down only for repair), renewal at failure (as-good-as-new after repair), and ideal human factors & logistic support. For an item with more than one element, *as-good-as-new* after repair refers in this book to the *repaired element in the reliability block diagram*. This assumption is valid for the whole item (system), *only in the case of constant failure rates for all not renewed elements*. Assuming *renewal for the whole item*, the asymptotic & steady-state value of the point availability can be expressed by $PA = MTF / (MTF + MTTR)$ ($PA_S = MUT_S / (MUT_S + MDT_S)$ at system level). PA is also the asymptotic & steady-state value of the *average availability* AA (often given as *availability* A). The convergence of $PA(t)$ to $PA = AA$ is discussed in Section 6.2 (in particular on pp. 178, 186-7, 188).

Burn-in (nonrepairable items)

Type of screening test while the item is in operation.

For electronic devices, stresses during burn-in are often constant higher ambient temperature (e. g. 125°C for ICs) and constant higher supply voltage. Burn-in can be considered as a part of a *screening procedure*, performed on a 100% basis to *provoke early failures* and to stabilize characteristics of the item. Often it can be used as an *accelerated reliability test* to investigate item's failure rate.

Burn-in, Run-in (repairable items)

Process of increasing the reliability of hardware by employing functional operation of all items in a prescribed environment, with corrective maintenance during the early failure period.

The term *run-in* is often used instead of *burn-in*. The stress conditions have to be chosen as near as possible to those expected in *field operation*. Faults detected during burn-in/run-in can be deterministic (defects or systematic failures) during the pilot production, but should be attributable only to *early failures* (randomly distributed) during the series production (see also **Reliability Growth**).

Capability [A1.4]

Ability to meet stated quantitative dependability characteristics under given internal conditions.

Performance (technical performance) is often used instead of *capability*.

Concurrent Engineering

Systematic approach to reduce the time to develop, manufacture, and market the item, essentially by integrating production activities into the design & development phase.

Concurrent engineering is achieved through intensive *teamwork* between all engineers involved in the design, production, and marketing of the item. It has a positive influence on the optimization of *life-cycle cost*.

Configuration Management

Procedure to specify, describe, audit, and release the configuration of the item, as well as to control it during modifications or changes.

Configuration includes all of the item's *functional and physical* characteristics as given in the documentation (to specify, produce, test, accept, operate, maintain, and logistically support the item) and as present in the hardware and / or software. In practical applications, it is useful to subdivide configuration management into *configuration identification, auditing, control* (design reviews), and *accounting*. Configuration management is of *great importance* during the design & development phase.

Corrective Maintenance

Maintenance carried out after fault detection to restore the item to a specified state.

A *fault* is a state, and can result from a defect or a failure. Corrective maintenance is also known as *repair* and can include any or all of the following steps: *detection* (recognition), *localization* (isolation), *correction* (disassemble, remove, replace, reassemble, adjust), and *function checkout*. In this book, fault detection time as well as *administrative, logistic & technical delays* are neglected, *repair* is thus used as a synonym for *restoration*. To simplify calculations, it is generally assumed that the *repaired element in the reliability block diagram is as-good-as-new* after each repair (including a possible environmental stress screening (ESS) of the corresponding spare parts). This assumption applies to the *whole item (system) only* if all nonrepaired elements have *constant failure rates* (see **Failure rate** for further comments).

Cost Effectiveness

Measure of the ability of the item to meet a service demand of stated quantitative characteristics, with the best possible usefulness to life-cycle cost ratio.

System effectiveness is often used instead of *cost effectiveness*.

Defect

Nonfulfillment of a requirement related to an intended or specified use.

From a technical point of view, a *defect* is similar to a *nonconformity*; however, not necessarily from a legal point of view (in relation to product liability, nonconformity should be preferred). Defects do not need to influence the item's functionality. They are caused by errors or mistakes during design, development, production, or installation. The term *defect* should be preferred to that of *error*, which is a *cause*. Unlike *failures*, which *always appear in time* (randomly distributed), *defects are present at $t = 0$* . However, some defects can only be recognized when the item is operating and are referred to as *dynamic defects* (e. g. in software). Similar to defects, with regard to causes, are **Systematic failures** (e. g. caused by a cooling problem); however, they must not be present at $t=0$.

Dependability [A1.4]

Ability to perform as and when required.

Dependability is used generally in a *qualitative* sense to describe the ability to perform the required function under stated conditions at a given instant or for a given time interval, including thus its influencing factors like reliability, maintainability, and logistic support.

Derating

Designed reduction of stress from the rated value to enhance reliability.

The *stress factor S* expresses the ratio of actual to rated stress under standard operating conditions (generally at 40°C ambient temperature, see p. 33). *Designed* is used as a synonym for *deliberated*.

Design Review

Independent, documented, comprehensive examination of the design to evaluate the capability of the design to meet all requirements, to identify deviations or problems, and to propose solutions.

Design reviews are an important tool for *quality assurance* and *TQM* during the design and development of hardware and software (Tables A3.3, 5.3, 5.5, 2.8, 4.3, Appendix A4). An important objective of design reviews is also to *decide about continuation or stopping the project*, on the basis of objective considerations (*feasibility check* in Tables A3.3 & 5.3, and Fig. 1.6).

Environmental Stress Screening (ESS)

Test or set of tests intended to remove defective items, or those likely to exhibit early failures.

ESS is a screening procedure often performed at assembly (PCB) or equipment level on a 100% basis to find *defects* and *systematic failures* during the pilot production (**Reliability Growth**), or to provoke *early failures* in a series production. For electronic items, it consists generally of temperature cycles

and/or random vibrations. Stresses are in general *higher* than in field operation, but not so high as to stimulate *new failure mechanisms*. Experience shows that to be cost effective, ESS has to be *tailored* to the item and production processes. At component level, the term *screening* is often used.

Failure [A1.4]

Loss of ability to perform as required.

Perform as required means *perform the required function under stated conditions*. Failure is an *event leading to an inoperative state*. It should be considered (classified) with respect to the *mode, cause, effect, and mechanism*. The *cause* of a failure can be *intrinsic* (early failures, failures with constant failure rate, wear-out failures) or *extrinsic* (systematic failures, i. e., failures resulting from errors or mistakes in design, production, or operation which are *deterministic* and have to be considered as *defects*). The *effect* (consequence) of a failure can be different if considered on the directly affected item or on a higher level. A failure is an *event* appearing in time (randomly distributed), in contrast to a **Defect** which is present at $t=0$ (even if hidden).

Failure Intensity ($z(t)$) [A1.4]

Limit, if it exists, of the expected (mean) number of failures of a repairable item within time interval $(t, t+\delta t]$, to δt when $\delta t \rightarrow 0$.

At system level, $z_S(t)$ is used (*system* refers in this book, and often in practical applications, to the highest integration level of the item considered). Failure intensity applies for repairable items, in particular when repair times are neglected. It must be clearly distinguished from **Failure Rate**, and is investigated in Appendix A7 for Poisson processes (homogeneous ($z(t)=\lambda$) & nonhomogeneous ($z(t)=m(t)$)) and renewal processes ($z(t)=h(t)$). For practical applications and $\delta t \rightarrow 0$ it holds that $z(t)\delta t = \Pr\{v(t+\delta t) - v(t) = 1\}$, $v(t)$ = number of failures in $(0, t]$.

Failure Modes and Effects Analysis (FMEA)

Qualitative method of analysis that involves the study of possible failure modes in subitems, and their effects on the item.

See FMECA for comments.

Failure Modes, Effects, and Criticality Analysis (FMECA) [A1.4]

Quantitative or qualitative method of analysis that involves *failure modes and effects analysis* together with a consideration of the probability of the failure mode occurrence and the severity of the effects.

Goal of an FMEA or FMECA is to identify all *potential hazards* and to analyze the possibilities of reducing (mitigating) their effect and / or occurrence probability. All possible failure modes with corresponding causes have to be considered *bottom-up* from lowest to highest integration level of the item considered. Often one distinguishes between design and process (production) FMEA or FMECA. *Fault modes* is to use if *failures and defects* have to be considered, allowing errors as possible causes as well.

Failure Rate ($\lambda(t)$)

Limit, if it exists, of the conditional probability that the failure occurs within time interval $(t, t+\delta t]$, to δt when $\delta t \rightarrow 0$, given that the item was new at $t=0$ and did not fail in the interval $(0, t]$ (Eq. (A1.1)).

At system level, $\lambda_S(t)$ is used (*system* refers in this book, and often in practical applications, to the highest integration level of the item considered). The failure rate applies in particular for *nonrepairable* items. In this case, if $\tau > 0$ is the item *failure-free time*, with distribution $F(t)=\Pr\{\tau \leq t\}$, ($F(0)=0$) and density $f(t)$, the failure rate $\lambda(t)$ follows as (Eq. (A6.25), $R(t)=1-F(t)$)

$$\lambda(t) = \lim_{\delta t \downarrow 0} \frac{1}{\delta t} \Pr\{t < \tau \leq t + \delta t \mid \tau > t\} = \frac{f(t)}{1-F(t)} = -\frac{dR(t)/dt}{R(t)}, \quad t > 0, F(0)=0. \quad (A1.1)$$

Considering $R(0)=1-F(0)=1$, Eq. (A1.1) yields $R(t) = e^{-\int_0^t \lambda(x) dx}$ and thus, $R(t) = e^{-\lambda t}$ for $\lambda(t) = \lambda$. This important result characterizes the *memoryless property* of the exponential distribution $F(t) = 1 - e^{-\lambda t}$, expressed by Eq. (A1.1) for $\lambda(t) = \lambda$. Only for $\lambda(t) = \lambda$ one can estimate the failure rate λ by $\hat{\lambda} = k/T$, where T is the given (fixed) cumulative operating time and $k > 0$ the total number of failures during T (Eq. (7.28)). Figure 1.2 shows a typical shape of $\lambda(t)$ for a large population of statistically identical and independent items. However, considering Eq. (A1.1),

the concept of failure rate also applies to repairable items which are as-good-as-new after repair (as a whole or with respect to the state considered), taking instead of t the variable x starting by 0 after each repair, as for interarrival times.

This extension is necessary when investigating repairable systems (Chapter 6). If a repairable system cannot be restored to be as-good-as-new after repair (as a whole or with respect to the state considered), i.e. if at least one element with *time dependent* failure rate has not been renewed at each repair, **Failure Intensity** $z(t)$ has to be used. The distinction between *failure rate* $\lambda(t)$ and *failure intensity* $z(t)$ or *intensity* $h(t)$ or $m(t)$ (for a renewal or Poisson process) is important. $z(t)$, $h(t)$, $m(t)$ are *unconditional intensities* (Eqs. (A7.229), (A7.24), (A7.194)) and differ basically from $\lambda(t)$, even for a *homogeneous Poisson process*, for which $z(t) = h(t) = m(t) = \lambda$ holds (Eq. (A7.42), see also pp. 7, 466, 516, 524). For $\lambda(t)$, *force of mortality* [6.1, A7.30] and *hazard rate* have been suggested; both terms should be avoided, and *conditional failure rate* (Eq. (6.28)) could be a good choice for *failure rate*. Also important is to note that $\lambda(t)$ is not a (probability) density (p. 426).

Fault [A1.4]

State of inability to perform as required, for internal reason.

Perform as required means *perform the required function under stated conditions*. A fault is a *state* resulting from a *defect* or a *failure*, having as possible cause an *error* or *flaw* for defects & systematic failures, a *failure mechanism* for failures. Not considered as fault are down states caused by external actions or events (preventive maintenance, loss of resources). For software, *faults* result from *defects*.

Fault Tree Analysis (FTA)

Analysis using logic diagrams, showing the faults of subitems, external events, or combination thereof, which cause a predefined, undesired event at item level.

FTA is a *top-down* approach, which allows inclusion of external causes more easily than for an FMEA/FMECA. However, it does not necessarily go through all possible *fault modes*. Combination

of FMEA / FMECA with FTA leads to *causes-to-effects chart*, showing the logical relationship between identified causes and their single or *multiple consequences* (see Sections 2.6, 6.9.2-6.9.3).

Item [A1.4]

Subject being considered.

An item is a functional or structural *unit*, generally considered as an *entity* for investigations. It can consist of hardware and/ or software and include human resources. For hardware it can be, for instance, a part, component, device, assembly, equipment, subsystem or system.

Life Cycle Cost (LCC)

Sum of the cost for acquisition, operation, maintenance, and disposal or recycling of the item.

Life-cycle cost have to consider also the effects to the environment of the production, use & disposal or recycling of the item considered (sustainable development). Their optimization uses *cost effectiveness* or *systems engineering* tools and can be positively influenced by *concurrent engineering*.

Lifetime

Time span between initial operation and failure of a nonrepairable item.

Logistic Support

All actions undertaken to provide effective and economical use of the item during its operating phase.

An emerging aspect related to logistic support is that of *obsolescence management*, i. e., for instance, how to assure operation over 20 years when components need for maintenance are no longer manufactured (see e. g. [A2.6 (IEC 62402)]).

Maintainability

Probability that a given maintenance action, performed under stated conditions and using stated procedures and resources, can be completed within a given time interval.

Maintainability is a *characteristic* of the item and refers to preventive and corrective maintenance. A qualitative definition, focused on *ability*, is also possible. In specifying or evaluating maintainability, it is important to consider the available *logistic support* (procedures, personnel, spare parts, etc.).

Mission Profile

Specific tasks which must be fulfilled by the item, under stated conditions, during a given time interval.

The mission profile defines the *required function* and the *environmental conditions* as a function of time. A system with a variable required function is termed a *phased-mission system* (Section 6.8.6.2).

MTBF**Mean operating time between failures**

At system level, $MTBF_S$ is used (*system* refers in this book, and often in practical applications, to the highest integration level of the item considered). *MTBF applies for repairable items (systems)*. However,

it is important to recognize that operating times between successive system failures will have the same mean (expected value) only if they are independent and have the same distribution function, i. e. if the system is as-good-as-new after each repair; if only the failed element is restored to as-good-as-new after repair and at least one non-restored element has a time dependent failure rate, successive operating times between system failures are neither independent nor have a common distribution (see also pp. 6 & 316).

In the case of a series-system with constant failure rates $\lambda_1, \dots, \lambda_n$ for elements E_1, \dots, E_n , the flow of failures at system level is given by a homogeneous Poisson process, for which successive *interarrival times* (operating times between failures) are independent and distributed according to $F(x) = 1 - e^{-x(\lambda_1 + \dots + \lambda_n)} = 1 - e^{-x\lambda_S}$, with mean $MTBF_S = 1/\lambda_S$ (repaired elements are assumed to be as-good-as-new, yielding system as-good-as-new because of constant failure rates $\lambda_1, \dots, \lambda_n$, and x is used instead of t by considering interarrival times). The homogeneous Poisson process often holds, approximately, also for redundant structures (Eq. (6.94)), as well as for very large systems (Section 7.6.1 and Appendix A7.8.3). For all these reasons, and also because of the estimate $MTBF = T/k$, often used in practical applications (although valid only for $\lambda(t) = \lambda$, Eq. (7.28)), *MTBF* should be confined to *repairable systems with constant failure rates for all elements* (shortcomings are known, see e.g. [6.1, 7.11, A7.30]). In this book, *MTBF* is reserved for

$$MTBF = 1/\lambda \quad (\text{and } MTBF_S = 1/\lambda_S), \quad (\text{A1.2})$$

as generally occurs in practical applications (often tacitly and without distinction between repairable and nonrepairable items). *MTBF* is thus considered in this book as a particular case of the *MTTF*. However, at components level, $MTBF = 1/\lambda$ should be avoided ($MTBF = 10^8\text{h}$ for $\lambda = 10^{-8}\text{h}^{-1}$ has no practical significance). The use of *MOTBF* instead of *MTBF* can cause troubles. Further considerations at system level are in the comments on *MTTF*.

MTTF**Mean time to failure.**

At system level, $MTTF_S$ is used (*system* refers in this book, and often in practical applications, to the highest integration level of the item considered). *MTTF* is the mean (expected value) of the item *failure-free time* $\tau > 0$. It can be computed from the reliability function $R(t)$ as $MTTF = \int_0^\infty R(t) dt$, with T_L as upper limit of the integral if the useful life is limited to T_L ($R(t) = 0$ for $t > T_L$).

*MTTF applies for both nonrepairable and repairable items, if one assumes that after repair the item is as-good-as-new and the variable x starting by $x=0$ after each repair is used instead of t , as for interarrival times (see remarks on **Failure Rate** and on p. 41 & 316)*

As for *MTBF*, the condition to have the *system as-good-as-new after each repair* (as a whole or with respect to the state considered), necessary to give a sense to an *MTTF*, *applies only if the repaired element is as-good-as-new and all nonrepaired elements have constant (time independent) failure rates*. This holds, in particular, for systems described by Markov processes, for which all elements have constant failure and repair rates. For such systems, MUT_S (system mean up time in steady-state or for $t \rightarrow \infty$) is used at system level instead of $MTTF_S$ (Eq.(A7.142) or (6.293), as well as

Eq. (A7.179) for semi-Markov processes). For practical applications, $MUT_S \approx MTTF_{S0}$ can often be used, where S stands for system and 0 for the state entered at $t=0$ (system new, p. 279). An unbiased, empirical estimate for $MTTF$ is $\hat{MTTF} = (t_1 + \dots + t_n) / n$, where t_1, \dots, t_n are observed failure-free times of n statistically identical and independent items. The use of mean operating time to failure for $MTTF$ can cause troubles, as $MTTF$ refers to failure-free times.

MTTPM

Mean time to preventive maintenance

Time to *preventive maintenance* means time to *perform a preventive maintenance*.

MTBUR

Mean time between unscheduled removals.

MTTR

Mean time to repair / Mean time to restoration.

Mean time to restoration is to use, if administrative, logistic, and technical delays must be considered. Except for Example 6.7 & Fig. A7.12, in this book all delays are neglected, and *repair* is used as a synonym for *restoration* (it can be noted that mean time to restore is used for high redundant systems, as mean time to switch to a redundant backup unit [4.21]). $MTTR$ is the mean (expected value) of the item repair time, and can be computed from the distribution function $G(t)$ of the repair time as $MTTR = \int_0^{\infty} (1 - G(t)) dt$. $MTTR$ implies that the repaired item is *as-good-as-new after each repair*. At system level, same considerations hold as for $MTTF$. For system described by Markov or semi-Markov processes, $MDT_S = MUT_S (1 - PA_S) / PA_S$ is used (Eq. (A7.146) or (6.295) & (A7.179)) with $MDT_S =$ *system mean down time* (often further simplified as in Tables 6.9 and 6.10 with $MDT_S \approx MTR_S \approx 1 / \mu_S$). In specifying or evaluating $MTTR$, it is necessary to consider the logistic support available for repair (procedures, personnel, spare parts, test facilities, etc.). Repair time is often *lognormally distributed*. However, for reliability or availability calculation of repairable systems, a *constant repair rate* $\mu = 1 / MTTR$) can often be used to get valid approximate results, as long as $MTTR_i \ll MTTF_i$ holds for each element in the reliability block diagram (Examples 6.8- 10). An unbiased, empirical estimate of $MTTR$ is $\hat{MTTR} = (t_1 + \dots + t_n) / n$, where t_1, \dots, t_n are observed repair times of n statistically identical and independent items.

Nonconformity [A1.4]

Non-fulfillment of a requirement.

From a technical point of view, *nonconformity* is close to *defect*, however not necessarily from a legal point of view. In relation to product liability, nonconformity should be preferred.

Preventive Maintenance [A1.4]

Maintenance carried out to mitigate degradation and reduce the probability of failure.

The aim of preventive maintenance must also be to remove *hidden failures* (*faults* for failure and

defects), e.g. undetected failures in redundant elements. To simplify computations, it is generally assumed that the element in the reliability block diagram for which a preventive maintenance has been performed is *as-good-as-new* after preventive maintenance. This assumption applies to the *whole item (system) only if all components of the item* (which have not been renewed) *have constant failure rates*. Preventive maintenance is generally performed at scheduled time intervals.

Product Assurance

All planned and systematic activities necessary to provide adequate confidence that the item will meet all specified quality and reliability (RAMS) requirements.

The concept of product assurance is used in particular in aerospace programs. It includes quality assurance as well as reliability, maintainability, availability, safety, and logistic support engineering.

Product Liability

Generic term used to describe the onus on a producer or others to make restitution for loss related to personal injury, property damage, or other harm caused by the product.

The manufacturer (producer) *has to specify* a safe operational mode for the product (item). If *strict liability* applies, the manufacturer has to demonstrate (at a claim) that the product was conforming to all applicable specifications (i.e. free from defects and intrinsic systematic failures) when it left the production plant. This holds in the USA and partially also in Europe [1.10]. However, in Europe the causality between damage and nonconformity has still to be demonstrated by the user and the limitation period is short (often 3 years after the identification of the damage, defect, and manufacturer, or 10 years after the appearance of the product on the market). A return to *tort liability* (the user has to demonstrate the nonconformity of the product (item)) is not desirable. Moreover, it is hoped that liability will be extended to better cover software aspects.

Quality

Degree to which a set of inherent characteristics fulfills requirements.

This definition, given also in the ISO 9000 family [A1.6, A2.9], follows closely the traditional definition of quality as *fitness for use*, and refers to products and services as well.

Quality Assurance

All planned and systematic activities necessary to provide adequate confidence that quality requirements will be fulfilled.

Quality assurance is a part of *quality management*, as per ISO 9000 [A2.9]. It refers to *hardware and software* as well, and includes *configuration management, quality tests, quality control during production, quality data reporting systems, and software quality* (Fig. 1.3). For complex equipment and

systems, quality assurance activities are coordinated by a *quality and reliability (RAMS) assurance program* (Appendix A3). An important target for quality assurance is to achieve the quality requirements with a *minimum of cost and time*. Concurrent engineering also strive to short the time to develop & market the product.

Quality Control During Production

Control of the production processes and procedures to reach a stated quality of manufacturing.

Quality Data Reporting System

System to collect, analyze, and correct all defects and failures occurring during production and test of the item, as well as to evaluate and feedback the corresponding quality and reliability (RAMS) data.

A quality data reporting system is generally computer aided. Its basic concept is illustrated in Fig. 1.8. Analysis of defects and failures must be *traced to the cause* in order to determine the best *corrective action* necessary to avoid repetition of the same problem. For complex systems, the quality data reporting system should remain active during the *operating phase* (at least during warranty).

Quality Management

Coordinated activities to direct and control an organization with regard to quality.

Organization is defined as group of people and facilities (e.g. a company) with an arrangement of responsibilities, authorities, and relationships [A2.9].

Quality Test

Test to verify whether the item conforms to specified requirements.

Quality tests include incoming inspections, qualification tests, production & acceptance tests, and cover performance, reliability, maintainability, safety, and software aspects. To optimize cost and time schedule, tests should be integrated in a *test (and screening) strategy* at system level. The terms *inspection* should be avoided.

Redundancy

Provision of more than one means for performing the required function.

For hardware, distinction is made between *active* (hot, parallel), *warm* (lightly loaded), and *standby* (cold) redundancy. Redundancy does not necessarily imply a *duplication* of hardware; it can, for instance, be implemented at the software level or as a *time redundancy*. To avoid *common cause failures*, redundant elements should be realized *independently* from each other. Should the redundant elements fulfill only a part of the required function, a *pseudo redundancy* is present.

Reliability (R , $R(t)$)

Probability that the item is able to perform as required for a given time interval.

Perform as required means *perform the required function under stated conditions*. According to the above definition, reliability is a *characteristic* of the item, generally designated by R for the case of a fixed mission and $R(t)$ for a mission with t as a parameter. At system level $R_{S_i}(t)$ is used, where S stands for system and i for the state entered at $t=0$, Table 6.2 (*system* refers in this book, and often in practical applications, to the highest integration level of the item considered). A qualitative definition, focused on *ability*, is also possible. $R(T)$ gives the probability that no *operational interruption* at item (system) level will occur during a stated mission of duration T . This does not mean that redundant parts may not fail, such parts can fail and be repaired. Thus,

the concept of reliability applies for nonrepairable as well as for repairable items.

Should T be considered as a variable t , the *reliability function* is given by $R(t)$. If τ is the failure-free time, with $F(t) = \Pr\{\tau \leq t\}$ & $F(0) = 0$, then $R(t) = \Pr\{\tau > t\} = 1 - F(t)$ & $R(0) = 1$. The concept of reliability can also be used for processes or services, although modeling human aspects can lead to some difficulties (pp. 10, 294-8). To avoid misinterpretations, $R(t_1, t_2)$ should be reserved for the *interval reliability* $IR(t_1, t_2)$ as per Eq. (6.25), see the remarks on pp. 40, 179, 426.

Reliability Block Diagram

Logical block diagram showing how failures of subitems, represented by the blocks, can result in a failure of the item.

The reliability block diagram (RBD) is an *event diagram*. It answers the question: *Which elements of the item are necessary to fulfill the required function and which ones can fail without affecting it?* The elements (blocks in the RBD) which must operate are connected *in series* (the ordering of these elements is not relevant for reliability computation) and the elements which can fail (redundant elements) are connected *in parallel*. Elements which are not relevant (used) for the required function are removed from the RBD and put into a reference list, after having verified (FMEA) that their failure does not affect elements involved in the required function. In a reliability block diagram, *redundant elements still appear in parallel*, irrespective of the failure mode. However, only *one failure mode* (e. g. short, open) and *two states* (good, failed) can be considered for each element.

Reliability Growth [A1.4]

Iterative process for reliability improvement by addressing design and manufacturing weaknesses.

Faults detected during a reliability growth program are often *deterministic* (defects or systematic failures present in every item of a given lot), and less frequently caused by early failures or failures with constant failure rate. Reliability growth is thus performed during the *pilot production*, seldom for series-produced items. Investigation of the cause of each fault is important to select the most appropriate corrective action. As for environmental stress screening (*ESS*), stresses during reliability growth often *exceed* those expected in field operation, but are not so high as to stimulate new failure mechanisms (see also **Burn-in**). Models for reliability growth can also be used to investigate the occurrence of *defects in software*. Although software defects often appear in time (dynamic defects), *software quality* should be preferred to *software reliability*.

Required Function [A1.4]

Function considered necessary to fulfill a given requirement.

The definition of the required function is the starting point for every reliability analysis, as it defines *failures*. However, difficulties can appear with complex items (systems). For practical purposes, parameters should be specified with tolerances.

Run-in (see **Burn-in**)**Safety**

Ability of the item to cause neither injury to persons, nor significant material damage or other unacceptable consequences.

Safety expresses freedom from unacceptable risk of harm. In practical applications, it is useful to subdivide safety into *accident prevention* (the item is safe working while it is operating correctly) and *technical safety* (the item has to remain safe even if a *failure* occurs). *Technical safety* can be defined as the *probability that the item will not cause injury to persons, significant material damage or other unacceptable consequences above a stated (fixed) level for a given time interval, when operating under stated conditions*. Methods and procedures used to investigate technical safety are similar to those used for reliability analyses, however with emphasis on fault/ failure *effects* (consequences). In particular, *safety analysis* includes *identification of potential hazards, identification of their causes, determination of their effect, classification of their effect & probability of occurrence, and investigation of possibilities to avoid hazards or at least to mitigate their effects*.

System [A1.4]

Set of interrelated elements that collectively fulfill a requirement.

A system generally includes hardware, software, services, and personnel (for operation and support) to the degree that it can be considered self-sufficient in its intended operational environment. For computations, ideal conditions for *human factors* and *logistic support* are often assumed, leading to a *technical system*. For simplicity, *system* is used in this book as a synonym for *technical system*. Elements of a system are e.g. components, assemblies, equipment, and subsystems, for hardware. For maintenance purposes, systems are partitioned into independent *line replaceable units* (LRUs), i.e. spare parts at equipment and systems level. *System* refers in this book, and often in practical applications, to the highest integration level of the item considered.

Systematic Failure [A1.4]

Failure that consistently occurs under particular conditions of handling, storage or use.

Systematic failures are also known as *dynamic defects*, for instance in software quality, and have a deterministic character. However, they must not be present at $t=0$ (e.g. cooling problems) and, because of the item's complexity, can appear as if they were randomly distributed in time.

Systems Engineering

Application of the mathematical and physical sciences to develop systems that utilize resources economically for the benefit of society.

TQM and concurrent engineering can help to optimize systems engineering.

Total Quality Management (TQM)

Management approach of an organization centered on quality, based on the participation of all its members, and aiming at long-term success through customer satisfaction and benefits to all members of the organization and to society.

Within TQM, everyone involved in the product (directly during development, production, installation, and servicing, or indirectly with management or staff activities) is jointly responsible for the quality of that product.

Useful Life [A1.4]

Time interval, from first use until user requirements are no longer met, due to economics of operation and maintenance, or obsolescence.

Useful life refers to repairable equipment and systems (see **Lifetime** for nonrepairable items). Economic aspects can be related to an unacceptable failure intensity or other. Typical values for useful life are 3 to 6 years for commercial applications, 5 to 15 years for military installations, and 10 to 30 years for distribution or power systems.

Value Analysis (VA)

Optimization of the item's configuration, as well as of the production processes and procedures, to provide the required item characteristics at the lowest possible cost without loss of capability, reliability, maintainability, and safety.

Value Engineering (VE)

Application of value analysis methods during the design phase to optimize the life-cycle cost of the item.

A2 Quality and Reliability (RAMS) Standards

Complex equipment & systems must be *safe* and, when repairable, *reliability* implies also *maintainability* and *availability*. RAMS is used here, as well as in Chapter 1 and Appendix A3, to point out this fact. To assure RAMS figures, besides *quantitative requirements* ($MTBF=1/\lambda$, *MTTR*, *availability*) customers require a *quality assurance / management system* and often also the realization of an *assurance program*. Such general requirements are covered by national and international *standards*, the most important of which are briefly discussed in this appendix. The term *management* is used explicitly where the organization (company) is involved, as per *ISO 9000: 2000 family* and *TQM (total quality management)*. A basic procedure for setting up and realizing quality and reliability (RAMS) requirements for complex equipment and systems, with the corresponding *quality and reliability (RAMS) assurance program*, is discussed in Appendix A3.

A2.1 Introduction

Customer requirements for quality and reliability (RAMS) can be quantitative or qualitative. As with performance parameters, *quantitative requirements* are given in *system specifications* and contracts. They fix, in particular, targets for reliability, maintainability, availability, and safety, as necessary, along with associated specifications for required function, operating conditions, logistic support, and criteria for acceptance tests. *Qualitative requirements* are in national and international *standards*, and generally deal with a *quality assurance / management system*. Depending upon the field of application (aerospace, nuclear, defense, or industrial), these requirements can be more or less stringent. Objectives of such *standards* are in particular:

1. Harmonization of quality assurance/ management systems, as well as of terms and definitions.
2. Enhancement of customer satisfaction.
- 3 Standardization of configuration, operating conditions, logistic support, and test procedures, as well as of selection/ qualification criteria for components, materials, and production processes.

Important *standards* for quality and reliability (RAMS) assurance/ management are given in Table A2.1, see [A2.0 - A2.13] for a comprehensive list. Some of the *standards* in Table A2.1 are briefly discussed in the following sections.

A2.2 General Requirements in the Industrial Field

In the industrial field, the *ISO 9000: 2000 family of standards* [A2.9] supersedes the *ISO 9000: 1994 family* and open a new era in quality management requirements. Many definitions of the *ISO 8402 (1994)* have been revised and integrated in the *ISO 9000 (2005)* [A1.6, A2.9]. Structure & content of the *ISO 9000: 2000 family* are new, and adhere better to industrial needs and to the concept depicted in Fig. 1.3. Eight basic quality management principles have been identified and considered: Customer Focus, Leadership, Involvement of People, Process Approach, System Approach to Management, Continuous Improvement, Factual Approach to Decision Making, and Mutually Beneficial Supplier Relationships.

ISO 9000 (2005) describes *fundamentals of quality management systems* and specify the *terminology* involved.

ISO 9001 (2008) specifies that *for a company or organization it is necessary to have a quality management system that demonstrate its ability to provide products that satisfy customer needs and applicable regulatory requirements*. It focus on four main chapters: Management Responsibility, Resource Management, Product and/or Service Realization, and Measurement. A quality management system must ensure that everyone involved with a product (in its development, production, installation, or servicing, as well as in a management or staff function) shares responsibility for the quality of that product, in accordance to *TQM* (total quality management). At the same time, the system must be cost effective and contribute to a reduction of *time to market*. Thus, *bureaucracy* must be avoided and such a system must cover all aspects related to quality, reliability, maintainability, availability, and safety, including management, organization, planning, and engineering activities. Customer expects today that only items with agreed requirements will be delivered.

ISO 9004 (2009) provides guidelines that consider *efficiency & effectiveness* of the quality management system (see e.g. *ISO/IEC 15288 (2008)* for *life cycle processes*).

The *ISO 9000: 2000 family* deals with a broad class of products and services (technical and non-technical), its content is thus lacking in details, compared with application specific *standards* used e. g. in aerospace, railway, defense, and nuclear industries (Appendix A2.3). It has been accepted as national *standards* in many countries, and international recognition of certification has been greatly achieved.

Dependability aspects, focusing on reliability, maintainability, and logistic support of systems are considered in *IEC* standards, in particular *IEC 60300* for global requirements and *IEC 60605, 60706, 60812, 61014, 61025, 61078, 61124, 61163, 61165, 61508, 61709, and 62380* for specific aspects, see [A2.6] for a comprehensive list. *IEC 60300* deals with *dependability programs* (management, task descriptions, and application guides). Reliability tests for *constant failure rate* λ (or of *MTBF* for the case $MTBF = 1/\lambda$) are considered in *IEC 61124*. *Maintainability* aspects are in *IEC 60706* and *safety* aspects in *IEC 61508*.

Table A2.1 Main Stds for quality and reliability (RAMS) assurance of equipment & systems [A2.0-13]

Industrial			
1987-	Int.	ISO 9000: 2005	Quality Management Systems – Fundamentals and Vocabulary
1987-	Int.	ISO 9001: 2008	Quality Management Systems – Requirements (Cor. 1: 2009)
1987-	Int.	ISO 9004: 2009	Quality Management Systems – Managing the Sustained Success
2002-	Int.	ISO/IEC 15288	Systems&Software Eng. – System Life cycle Processes (2008)
2009-	Int.	IEC 31010	Risk Manag. - Risk Assessment Techniques (2009)
1984-	Int.	IEC 60300	Dependability Management -1 (2003): Systems, -2 (2004): Guidelines , -3 (2001-2011): Application Guides
1978-	Int.	IEC 60605	Equip. Rel. Testing. -2 (1994): Test Cycles, -4 (2001): λ Estim., -6 (2007): Goodness-of-fit for λ ; see also IEC 61124
1982-	Int.	IEC 60706	Guide on Maintainability of Equip., -2 (2006): Requirements, -3 (2006): Data Evaluation, -5 (2007): Testability
2005-	Int.	IEC 61508-SER	Functional Safety of el./el. progr. Safety-Related Systems (-0 to-7)
1997-	Int.	IEC 61124	Rel. testing - Compliance tests for λ (2012, supers. IEC 60605-7)
1969-	Int.	IEC (other as above)	60068, -319, -410, -447, -721, -749, -812, 61000, -014,-025,-070, -078, -123, -160, -163, -164, -165, -649, -650, -703, -709, -710, -882, -907, 62010, -198, -278, -308, -380, -396, -402, -429, -502, -506 (draft), -508, -550 (draft), -551, 628
1998-	Int.	IEEE Std 1332	IEEE Standard Reliability Program for the Development and Production of El. Systems & Equipment (see also 1413, 1624, 1633)
1999-	EU	EN 50126	Railway: RAMS Spec. & Dem. (1999), see also IEC 62278
1985	EU	85/374	Product Liability
Software Quality			
1987-	Int.	IEEE	Software and Systems Eng. Stds, in particular 730, 828, 829, 830, 982, 1012, 1016, 1028, 1044, 1045, 1062, 1061, 1063, 1074, 1175, 12207, 1228, 1420, 1465, 1517, 1633, 1636, 1734, 14102, 14471, 14764, 15026, 15939, 16326, 26513, 27748, 9003
2012-	Int.	IEC 62628	Guidance on Software Aspects of Dependability (2012)
1998-	Int.	ISO/IEC	12207, 14764, 15026, 15288, 15289, 15940, 16085. 16326. 18018. 24766. 26511, 26512, 26514, 26702, 29148, 29119
Defense			
1959-	USA	MIL-Q-9858	Quality Program Requirements, replaced by ISO 9000:2005
1965-	USA	MIL-STD-785	Rel. Prog. for Syst. & Eq. Dev. & Prod., repl. by GEIA-STD-0009
1987-	USA	MIL-HDBK-781	Rel. Test Met., Plans, Env. for Eng. Dev, Qual., Prod (Ed.A,1996)
1966-	USA	MIL-HDBK-470	Designing & Dev. Maintainable Systems (Ed. A, Not. 2, 2012)
1966-	USA	MIL-STD-882	System Safety (Ed. E 2012)
2008-	USA	GEIA-STD-0009	Rel. Progr. Std. for Systems Design, Dev. & Manuf. (ANSI-GEIA)
2008-	NATO	ARMP-1	NATO Requirements for Reliability & Maintainability (2008)
2011-	EU	Expert Group 17	Europ. HDBK for Defense Procurement: Dependability & Safety
Aerospace			
1998	USA	STD-8729.1	Planning, Developing & Managing an Effective R&M Program
2004-	(NASA)	STD-8739.8	Software assurance Standard
1996-	EU	ECSS-E	Engineering (-00, -10)
	(ESA)	ECSS-M	Project Management (-00, -10, -20, -30, -40, -50, -60,-70)
		ECSS-Q	Product Assurance (-00, -20, -30, -40, -60, -70, -80)
2003-	EU	EN 9100-2009	Quality Management System: Req. for Avionics, Space&Defense

For electronic equipment & systems, *IEEE Std 1332-1998* [A2.7] has been issued as a baseline for a reliability program for the development and production phases. This document, reinforced with *IEEE Std 1413-2010*, *1413.1-2002*, *1624-2008* & *1633-2008*, gives in short form the basic requirements, putting an accent on an *active cooperation* between supplier (manufacturer) and customer, and focusing three main aspects: Determination of the Customer's Requirements, Determination of a Process that satisfy the Customer's Requirements, and Assurance that Customer's Requirements are met. Examples of comprehensive requirements for industry application are e. g. in [A2.2, A2.3]. Software aspects are considered in IEEE Stds [A2.8], ISO/IEC Stds [A2.9 (12207 & following)], and in IEC 62628 (2012) [A2.6]. Requirements for *product liability* are in national and international directives, see for instance [1.10].

A2.3 Requirements in the Aerospace, Railway, Defense, and Nuclear Fields

Requirements in *space and railway fields* generally combine the aspects of quality, reliability, maintainability, safety, and software quality in well conceived *Product Assurance* or *RAMS* documents [A2.3, A2.4, A2.12]. Similar is in the *avionics field*, issued by reinforcing the *ISO 9000: 2000* family [A2.3(2003), A2.5, A2.6(IEC 62396)]. One can expect that space and avionics will unify *standards* in an *Aerospace Series*.

MIL-Standards have played an important role in the last 40 years, in particular *MIL-Q-9858*, *MIL-STD-470,-471,-781,-785,-882*, and corresponding *MIL-HDBK* [A2.10]. *MIL-Q-9858* (firstEd. 1959), now replaced by *ISO 9000: 2000 family*, was the basis for many quality assurance standards. However, as it does not cover specific aspects of reliability, maintainability & safety, *MIL-STD-785*, *-470* & *-882* were issued. *MIL-STD-785* (first Ed. 1965), now *ANSI-GEIA-STD-0009* [A2.0], was the basis for most *reliability programs*. *MTBF=1/λ acceptance tests* in *MIL-STD-781* (first Ed. 1965) are now in *MIL-HDBK-781*. *MIL-STD-470* (first Ed. 1966), now *MIL-HDBK-470*, requires the realization of a *maintainability program*, with emphasis on design rules, design reviews & FMEA/FMECA. *Maintainability demonstration* is also covered by *MIL HDBK-470*. *MIL-STD-882* requires a *safety program*, in particular *analysis of potential hazards*. For *NATO* countries, *AQAP Requirements*, now *ARMP-1*, were issued starting 1968. *MIL-STDs/HDBKs* have dropped their importance (since 1998). However, they can still be useful in developing procedures for industrial applications. *ANSI-GEIA-STD-0009* (2008) [A2.0], focusing on four main objectives (Understand the User's Requirements and Constraints, Design & Redesign for Reliability, Produce Reliable Systems, Monitor User Reliability), opens probably a new era for MIL-Documents, insisting more on "what to do" rather than on "how do".

The *nuclear field* has its own specific, well established *standards* with emphasis on safety aspects, design reviews, configuration accounting, *traceability*, qualification of components/materials/production processes, and quality tests.

A3 Definition and Realization of Quality and Reliability (RAMS) Requirements

For complex equipment & systems, *reliability* implies also *maintainability*, *availability* and *safety*. RAMS is used here, in Appendix A2, and in Chapter 1 to point out this fact. In defining *quality and reliability (RAMS) requirements*, it is important that market needs, life-cycle cost aspects, time to market as well as development and production risks (for instance when using new technologies) are considered with care. For *complex equipment and systems with high quality and reliability (RAMS) requirements*, the realization of such requirements is best achieved with

a quality and reliability (RAMS) assurance program, integrated in the project activities and performed without bureaucracy.

Such a program (*plan* with a time schedule) defines the *project specific* activities for quality and reliability (RAMS) assurance and assigns responsibilities for their realization in agreement to *TQM*. This appendix discusses important aspects in defining quality & reliability (RAMS) requirements and the content of a quality & reliability (RAMS) assurance program for complex equipment and systems with high quality and reliability requirements *for the case in which tailoring is not mandatory*. It has been added to support managers in answering the question of

how to specify and achieve high reliability (RAMS) targets for complex equipment and systems.

For less stringent requirements, *tailoring is necessary* to meet real needs and to be cost and time effective. Software specific quality assurance aspects are considered in Section 5.3. Examples for check lists for design reviews are in Table 2.8, Table 4.3, and Appendix A4; requirements for a quality data system are in Appendix A5.

A3.1 Definition of Quality and Reliability (RAMS) Requirements

In defining *quantitative*, project specific, *quality and reliability (RAMS) requirements*, attention has to be paid to the actual possibility to realize them (development and production), as well as to demonstrate them at a final or acceptance test. These requirements are derived from *customer or market needs*, taking care of limitations given by technical, cost, and ecological aspects. This section deals with some important considerations by setting *MTBF*, *MTR*, and steady-state availability ($PA=AA$) requirements. *MTBF* is used for $MTBF=1/\lambda$, where λ is the constant (time independent) failure rate of the item (system) considered.

Tentative targets for *MTBF*, *MTTR*, and *PA* are set by considering

- operational requirements relating to reliability, maintainability, and availability
- required function, expected environmental conditions, allowed logistic support
- experience with similar equipment or systems
- possibility for redundancy at higher integration level
- requirements for life-cycle cost, dimensions, weight, power consumption, etc.
- ecological consequences (sustainability, sustainable development).

Typical figures for failure rates λ of electronic assemblies (PCBs) are between 100 and $1,000 \cdot 10^{-9} \text{h}^{-1}$ at ambient temperature θ_A of 40°C and with a duty cycle d of 0.3, see Table A3.1 for some examples. The duty cycle ($0 < d \leq 1$) gives the mean of the ratio between operational time and calendar time. Assuming a constant failure rate λ and no reliability degradation caused by power on/off, an equivalent failure rate

$$\lambda_d = d \cdot \lambda \quad (\text{A3.1})$$

can be used for practical purposes. Often it can be useful to operate with the mean expected number of failures per year and 100 items

$$m_{\% / y} = \lambda_d \cdot 8,600 \text{ h} \cdot 100\% \approx \lambda_d \cdot 10^6 \text{ h}. \quad (\text{A3.2})$$

$m_{\% / y} < 1$ is a good target for equipment and can influence acquisition cost.

Tentative targets are refined successively by performing rough analysis and comparative studies (allocation down to assemblies is often necessary (Eqs. (2.71), (2.72)).

For acceptance testing (demonstration) of an *MTBF* for the case $MTBF = 1/\lambda$, the following data are important (Sections 7.2.3.2 and 7.2.3.3):

1. $MTBF_0$ = specified *MTBF* and/or $MTBF_1$ = minimum acceptable *MTBF*.
2. Required function (mission profile).

Table A3.1 Indicative values of failure rates λ and mean expected number $m_{\% / y}$ of failures per year and 100 items for a duty cycle $d = 30\%$ and $d = 100\%$ ($\theta_A = 40^\circ\text{C}$)

	$d = 30\%$		$d = 100\%$	
	$\lambda_d [10^{-9} \text{ h}^{-1}]$	$m_{\% / y}$	$\lambda [10^{-9} \text{ h}^{-1}]$	$m_{\% / y}$
Telephone exchanger	2,000	2	6,000	6
Telephone receiver (multifunction)	200	0.2	600	0.6
Photocopier incl. mechanical parts	30,000	30	100,000	100
Personal computer	3,000	3	9,000	9
Radar equipment (ground mobile)	300,000	300	900,000	900
Control card for automatic process control	300	0.3	900	0.9
Mainframe computer system	—	—	20,000	20

3. Environmental conditions (thermal, mechanical, climatic).
4. Allowed producer's and/or consumer's risks (α and/or β).
5. Cumulative operating time T and number c of allowed failures during T .
6. Number of systems under test ($T / MTBF_0$ as a rule of thumb).
7. Parameters which should be tested and frequency of measurement.
8. Failures which should be ignored for the $MTBF$ acceptance test.
9. Maintenance and screening before the acceptance test.
10. Maintenance procedures during the acceptance test.
11. Form and content of test protocols and reports.
12. Actions in the case of a negative test result.

For acceptance testing (demonstration) of an $MTTR$, the following data are important (Section 7.3.2):

1. Quantitative requirements ($MTTR$, variance, quantile).
2. Test conditions (environment, personnel, tools, external support, spare parts).
3. Acceptance conditions (number of repairs and observed empirical $MTTR$).
4. Extent of repairs to be undertaken for the case of simulated/introduced failures.
5. Allocation of the repair time (detection, localization, correction, checkout).
6. Form and content of test protocols and reports.
7. Actions in the case of a negative test result.

Availability usually follows from the relationship $PA = MTBF / (MTBF + MTTR)$. However, specific test procedures for $PA = AA$ are given in Section 7.2.2).

A3.2 Realization of Quality & Reliability (RAMS) Requirements for Complex Equipment & Systems

For complex items, in particular at equipment & systems level, quality and reliability targets are best achieved with a *quality and reliability (RAMS) assurance program*, integrated in the project activities and performed without bureaucracy. In such a program, *project specific* tasks and activities are clearly described and assigned. Table A3.2 can be used as a *checklist* by defining the content of a quality and reliability (RAMS) assurance program for *complex equipment and systems with high quality and reliability requirements, when tailoring is not mandatory* (see also Section 5.3 & [A2.8 (730-2002)] for software specific quality assurance aspects). Tab. A3.2 is a refinement of Tab. 1.2 and shows a possible *task assignment* in a company as per Fig. 1.7. Depending on the item technology & complexity, or because of tailoring, Tab. A3.2 is to be shortened or extended. The given responsibilities (R, C, I) can be modified to reflect the company's personnel situation. For a description of reliability assurance tasks see e. g. [A2.0, A2.2, A2.6 (60300), A3.1].

Table A3.2 Basic tasks and possible tasks assignment for quality and reliability (RAMS) assurance of complex equipment and systems with high quality and reliability requirements, when tailoring is not mandatory (software quality appears in tasks 4, 8-11, 14-16, see also the remark on p. 159)

<p>Basic tasks and possible tasks assignment for <i>quality and reliability (RAMS) assurance</i>, in agreement to Fig. 1.7 and <i>TQM</i> (checklist for the preparation of a quality and reliability assurance program; R stands for responsibility, C for cooperation (must cooperate), I for information (can cooperate); <i>software quality appears in tasks 4, 8 - 11, 14 - 16, see also the remark on p. 159</i>)</p>	Marketing (M)	Development (R&D)	Production (P)	Q&R Assurance (Q&R)
<p>1 Customer and market requirements</p>				
<p>1 Evaluation of delivered equipment and systems</p>	R	I	I	C
<p>2 Determination of market and customer demands and real needs</p>	R	I	I	C
<p>3 Customer support</p>	R			C
<p>2 Preliminary analyses</p>				
<p>1 Definition of tentative quantitative targets for reliability, maintainability, availability, safety, and quality level</p>	C	C	C	R
<p>2 Rough analyses and identification of potential problems</p>	I	C		R
<p>3 Comparative investigations</p>	I	C		R
<p>3 Quality and reliability (RAMS) aspects in specifications, quotations, contracts, etc.</p>				
<p>1 Definition of the required function</p>	I	R		C
<p>2 Determination of (external) environmental conditions</p>	C	R		C
<p>3 Definition of realistic quantitative targets for reliability, maintainability, availability, safety, and quality level</p>	C	C	C	R
<p>4 Specification of test and acceptance criteria</p>	C	C	C	R
<p>5 Identification of the possibility to obtain field data</p>	R			C
<p>6 Cost estimate for quality & rel. (RAMS) assurance activities</p>	C	C	C	R
<p>4 Quality and reliability (RAMS) assurance program</p>				
<p>1 Preparation</p>	C	C	C	R
<p>2 Realization</p>	I	R	I	C
<p>– design and evaluation</p>	I	I	R	C
<p>– production</p>				
<p>5 Reliability and maintainability analyses</p>				
<p>1 Specification of the required function for each element</p>		R		C
<p>2 Determination of environmental, functional, and time-dependent stresses (detailed operating conditions)</p>		R		C
<p>3 Assessment of derating factors</p>		C		R
<p>4 Reliability and maintainability allocation</p>		C		R
<p>5 Preparation of reliability block diagrams</p>				
<p>– assembly level</p>		R		C
<p>– system level</p>		C		R
<p>6 Identification and analysis of reliability weaknesses (FMEA/FMECA, FTA, worst-case, drift, stress-strength-analyses, etc.)</p>				
<p>– assembly level</p>		R		C
<p>– system level</p>		C		R

Table A3.2 (cont.)

	M	R&D	P	Q&R
7 Carrying out comparative studies				
– assembly level		R		C
– system level		C		R
8 Reliability improvement through redundancy				
– assembly level		R		C
– system level		C		R
9 Identification of components with limited lifetime	I	R		C
10 Elaboration of the maintenance concept	I	R	I	C
11 Elaboration of a test and screening strategy	C	C	C	R
12 Analysis of maintainability		R		C
13 Elaboration of mathematical models		C		R
14 Calculation of the predicted reliability and maintainability				
– assembly level	I	R		C
– system level	I	C		R
15 Reliability and availability calculation at system level	I	I		R
<i>6. Safety and human factor analyses</i>				
1 Analysis of safety (avoidance of liability problems)				
– accident prevention	C	R	C	C
– technical safety				
• identification and analysis of critical failures and of risk situations (FMEA/FMECA, FTA, etc.)				
– assembly level		R		C
– system level	I	C		R
• theoretical investigations		C		R
2 Analysis of human and ergonomic factors	C	R	C	C
<i>7. Selection and qualification of components and materials</i>				
1 Updating of the list of preferred components and materials	I	C	I	R
2 Selection of non-preferred components and materials		R	C	C
3 Qualification of non-preferred components and materials				
– planning		C	I	R
– realization			C	R
– analysis of test results		I	I	R
4 Screening of components and materials		I	C	R
<i>8. Supplier selection and qualification</i>				
1 Supplier selection				
– purchased components and materials		R	C	C
– external production		C	R	C
2 Supplier qualification (quality and reliability (RAMS))				
– purchased components and materials		I	I	R
– external production		I	I	R
3 Incoming inspections				
– planning		C	C	R
– realization			R	C
– analysis of test results			C	R
– decision on corrective actions				
• purchased components and materials		C	C	R
• external production		R	C	C

Table A3.2 (cont.)

	M	R&D	P	Q&R
<i>9. Project-dependent procedures and work instructions</i>				
1 Reliability guidelines	I	C	I	R
2 Maintainability, safety, and human factors guidelines	C	C	I	R
3 Software quality guidelines	I	R	I	C
4 Other procedures, rules, and work instructions				
• for development		R	I	C
• for production		I	R	C
5 Compliance monitoring	C	C	C	R
<i>10. Configuration management</i>				
1 Planning and monitoring	C	C	C	R
2 Realization				
– configuration identification				
• during design		R		C
• during production		I	R	C
• during use (warranty period)	R	I	I	C
– configuration auditing (design reviews, Tables A3.3, 5.3, 5.5)	C	R	C	C
– configuration control (evaluation, coordination, and release or rejection of changes and modifications)				
• during design	C	R	C	C
• during production	C	C	R	C
• during use (warranty period)	R	C	C	C
– configuration accounting		R	C	C
<i>11. Prototype qualification tests</i>				
1 Planning	I	R	I	C
2 Realization	C	R	C	C
3 Analysis of test results	I	R	I	C
4 Special tests for reliability, maintainability, and safety	I	C	C	R
<i>12. Quality control during production</i>				
1 Selection and qualification of processes and procedures		R	C	C
2 Production planning		C	R	C
3 Monitoring of production processes		I	R	C
<i>13. In-process tests</i>				
1 Planning		C	R	C
2 Realization		I	R	I
<i>14. Final and acceptance tests</i>				
1 Environmental tests and/or screening of series-produced items				
– planning	I	C	C	R
– realization	I	I	C	R
– analysis of test results	I	C	C	R
2 Final and acceptance tests				
– planning	C	C	C	R
– realization	I	I	C	R
– analysis of test results	C	C	C	R
3 Procurement, maintenance, and calibration of test equipment	I	C	C	R

Table A3.2 (cont.)

	M	R&D	P	Q&R
<i>15. Quality data reporting system (see e. g. Fig 1.8)</i>				
1 Data collection	C	C	C	R
2 Decision on corrective actions				
– during prototype qualification		R	I	C
– during in-process tests		C	R	C
– during final and acceptance tests	C	C	C	R
– during use (warranty period)	R	C	C	C
3 Realization of corrective actions on hardware or software (repair, rework, waiver, scrap, etc.)	I	C	C	R
4 Implementation of the changes in the documentation (technical, production, customer)	C	C	C	R
5 Data compression, processing, storage, and feedback	I	I	I	R
6 Monitoring of the quality data reporting system	I	I	I	R
<i>16. Logistic support</i>				
1 Supply of special tools and test equipment for maintenance	C	R	I	C
2 Preparation of customer/user documentation	R	C	I	I
3 Training of operating and maintenance personnel	R	I	I	I
4 Determination of the required number of spare parts, maintenance personnel, etc.	R	C	C	C
5 After-sales (after market) support	R	I	I	C
<i>17. Coordination and monitoring (quality and reliability (RAMS))</i>				
1 Project-specific	C	C	C	R
2 Project-independent	I	I	I	R
3 Planning and realization of quality audits				
– project-specific	C	C	C	R
– project-independent	I	I	I	R
4 Information feedback	I	I	I	R
<i>18. Quality cost</i>				
1 Collection of quality cost	C	C	C	R
2 Cost analysis and initiation of appropriate actions	C	C	C	R
3 Preparation of periodic and special reports	C	C	C	R
4 Evaluation of efficiency of quality & rel. (RAMS) assurance	I	I	I	R
<i>19. Concepts, methods, and general procedures (quality and reliability (RAMS))</i>				
1 Development of concepts	C	C	C	R
2 Investigation of methods	I	I	I	R
3 Preparation and updating of the quality handbook	C	C	C	R
4 Development of software packages	I	I	I	R
5 Collection, evaluation, and distribution of data, experience and know-how	I	I	I	R
<i>20. Motivation and training (quality and reliability (RAMS), Fig 1.9)</i>				
1 Planning	C	C	C	R
2 Preparation of courses and documentation	C	C	C	R
3 Realization of the motivation and training program	C	C	C	R

A3.3 Elements of a Quality and Reliability (RAMS) Assurance Program

The basic elements of a quality and reliability (RAMS) assurance program, as defined in Appendix A.3.2, can be summarized as follows:

1. Project organization, planning, and scheduling
2. Quality and reliability (RAMS) requirements
3. Reliability, maintainability, and safety analysis
4. Selection and qualification of components, materials, and processes
5. Software quality assurance
6. Configuration management
7. Quality tests
8. Quality data reporting system

These elements are discussed in this section for the case of *complex equipment and systems with high quality & reliability requirements (RAMS), when tailoring is not mandatory*. In addition, Appendix A4 gives a catalog of questions useful to generate *checklists for design reviews* and Appendix A5 specifies the requirements for a *quality data reporting system*. As suggested in task 4 of Table A3.2, the *realization* of a quality and reliability (RAMS) assurance program should be the responsibility of the *project manager*. It is appropriate to separate the quality and reliability (RAMS) assurance program for the development phase and for the production phase.

A3.3.1 Project Organization, Planning, and Scheduling

A clearly defined project organization and planning is necessary for the realization of a quality and reliability (RAMS) assurance program. Organization and planning must also satisfy present needs for *cost management* and *concurrent engineering*.

The *system specification* is the basic document for all considerations at project level. The following is a typical outline for system specifications:

1. State of the art, need for a new product
2. Target to be achieved
3. Cost, time schedule
4. Market potential (turnover, price, competition)
5. Technical performance
6. Environmental conditions
7. Operational capabilities (reliability, maintainability, availability, logistic support)
8. Quality and reliability (RAMS) assurance, inclusive software quality assurance
9. Special aspects (new technologies, patents, value engineering, etc.)
10. Appendices

The organization of a project begins with the definition of the main task groups. The following groups are usual for a complex system: Project Management, Systems Engineering, Life-Cycle Cost, Quality and Reliability (RAMS) Assurance (incl. software quality assurance), Software Development and Validation, Assembly Design, Prototype Qualification Tests, Production, Integration and Final Testing. Project organization, task lists, task assignment, and milestones can be derived from the task groups, allowing the quantification of the personnel, material, and financial resources needed for the project. The quality and reliability (RAMS) assurance program must assess that the project is clearly and suitably organized and planned.

A3.3.2 Quality and Reliability (RAMS) Requirements

Important steps in defining quality and reliability (RAMS) targets for complex equipment and systems have been discussed in Appendix A.3.1.

A3.3.3 Reliability, Maintainability, and Safety Analysis

Reliability and safety analyses include, in particular, *failure rate* analysis, *failure modes* analysis (FMEA/FMECA, FTA), *sneak circuit analysis* (to identify latent paths which can cause unwanted functions or inhibit desired functions, while all components are functioning properly), evaluation of *concrete* possibilities to improve reliability and safety (derating, screening, redundancy), as well as *comparative studies*; see Chapters 2 - 6 for methods and tools.

The quality and reliability (RAMS) assurance program must consider tasks 5, 6, 9 of Table A3.2 and show what is *actually being done* for the project considered. In particular, it should be able to supply answers to the following questions:

1. Which derating rules are considered?
2. How are the actual component-level operating conditions determined?
3. Which failure rate data are used? Which are the associated factors (π_E & π_Q)?
4. Which tool is used for failure modes analysis? To which items does it apply?
5. Which kind of comparative studies will be performed?
6. Which design guidelines for reliability, maintainability (incl. human, ergonomic, & safety aspects), and software quality are used? How will their adherence be verified?

Additionally, interfaces to the selection and qualification of components and materials, design reviews, test and screening strategies, reliability tests, quality data reporting system, and subcontractor activities must be shown. The data used for components failure rates calculation should be critically evaluated (source, present relevance, assumed environmental and quality factors π_E & π_Q).

A3.3.4 Selection and Qualification of Components, Materials, and Manufacturing Processes

Components, materials, and production processes have a great impact on product quality and reliability. They must be carefully selected and qualified. Examples for qualification tests on electronic components and assemblies are given in Chapter 3. For production processes one may refer e. g. to [8.1 - 8.14, 3.70 - 3.93].

The quality and reliability (RAMS) assurance program should give how components, materials, and processes are (or have already previously been) selected and qualified. In particular, the following questions should be answered:

1. Does a *list of preferred components and materials* exist? Will critical components be available on the market-place at least for the required production and warranty time?
2. How will obsolescence problems be solved?
3. Under what conditions can a designer use nonqualified components / materials?
4. How are new components selected? What is the qualification procedure?
5. How have the standard manufacturing processes been qualified?
6. How are special manufacturing processes qualified?

Special manufacturing processes are those which quality can't be tested directly on the product, have high requirements with respect to reproducibility, or can have an important negative effect on the product quality or reliability.

A3.3.5 Software Quality Assurance

For complex equipment and systems, software quality assurance can take a great portion of the effort devoted to the quality and reliability (RAMS) assurance program. Considering that software faults are caused by *defects*, even if they appears *randomly* in time (dynamic defects), software problems are basically *quality problems* which have to be solved with *quality assurance tools* (defect prevention, configuration management, testing, and quality data reporting system), as described in Sections 5.3.1 - 5.3.3 and Appendices A3.3.6 - A3.3.8. Defects modeling can be useful in the context of software quality growth (Section 5.3.4).

The quality and reliability (RAMS) assurance program should, in particular, answer the following questions (see e. g. also Section 5.3, Appendix A4.2 (Point 1), and [A2.8, A2.9 (29119)] for further specific questions):

1. What is the priority list of quality attributes (Table 5.4)? How will the customer (user) be involved in this list? How it is assured that this list will be consequently followed by all engineers involved in the project?
2. Which project specific written procedures (in particular design guidelines) will be worked out? From who? How it is assured that these procedures will be followed by all engineers in the project?

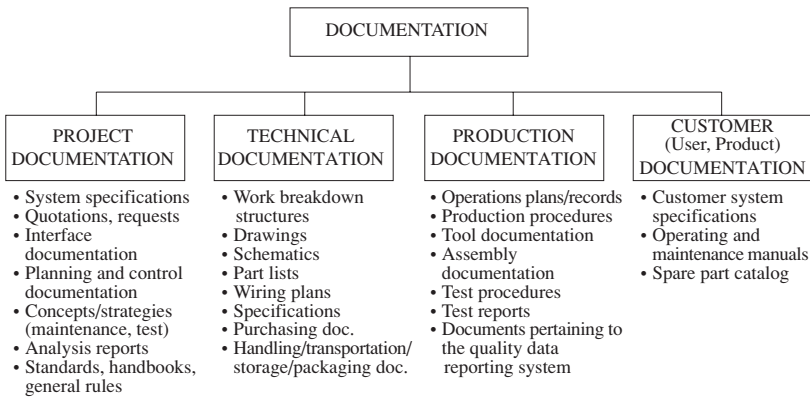


Fig. A3.1 Possible documentation outline for *complex equipment and systems*

3. How is the software life-cycle partitioned (Table 5.3)? Is each of these phases closed with a comprehensive design review (Tables 5.5)?
4. Is the software configuration management at the same level as that for hardware?
5. How is the software test strategy? Who is involved in its definition / approval?
6. How it is assured that the software will be conceived and developed to be defect tolerant?

A3.3.6 Configuration Management

Configuration management is an important tool for quality assurance, in particular during design and development. Within a project, it is often subdivided into configuration identification, auditing, control, and accounting.

The *identification* of an item is recorded in its documentation. A possible documentation outline for *complex equipment and systems* is given in Fig. A3.1.

Configuration auditing is done via *design reviews* (often also termed *gate review*), the aim of which is to assure/verify that the item (system) will meet all requirements. In a design review, all aspects of design and development (selection and use of components and materials, dimensioning, interfaces (hardware and / or software), software aspects, etc.), production (manufacturability, testability, reproducibility), reliability, maintainability, safety, patent regulations, value engineering, and value analysis are critically examined with the help of *checklists*. The most important design reviews are described in Table A3.3 on p. 403, see also Table 5.5 on p. 165 for software aspects. For complex systems a preproduction design review or a review of the first production unit is often required. A further important objective of design reviews is to *decide about continuation or stopping* the project considered, on the basis of objective considerations (*feasibility check* in Tables A3.3

and 5.3, Fig. 1.6). About a week before the design review, participants should present project specific checklists, see Appendix A4 and Tables 2.8 and 4.3 for some suggestions. Design reviews are chaired by the *project manager* and should be cochaired by the project quality and reliability (RAMS) assurance manager. For complex equipment and systems, the review team may vary according to the following list:

- project manager,
- project quality and reliability (RAMS) assurance manager,
- designer(s),
- independent design engineer or external expert,
- representatives from production, marketing, customer (as necessary/appropriate).

Configuration control includes evaluation, coordination, and release or rejection of all proposed changes and modifications. *Changes* occur as a result of mistakes, defects, or failures; *modifications* are triggered by a revision of system specifications.

Configuration accounting ensures that all approved changes and modifications have been implemented and recorded. This calls for a defined procedure, as changes/modifications must be realized in hardware, software, and documentation.

A *faultless correspondence* between hardware or software and documentation is important during all life-cycle phases of a product. Complete records over all life-cycle phases become necessary if *traceability* is *explicitly* required, as e. g. in the aerospace or nuclear field. Partial traceability can also be required for products which are critical with respect to *safety*, or because of *product liability*.

Referring to configuration management, the quality and reliability (RAMS) assurance program should, in particular, answer the following questions:

1. Which documents will be produced by whom, when, and with what content?
2. Does document contents agree with quality and reliability (RAMS) requirements?
3. Is the release procedure for technical and production documentation compatible with quality requirements?
4. Are the procedures for changes/modifications clearly defined?
5. How is compatibility (upward and/or downward) assured?
6. How is configuration accounting assured during production?
7. Which items are subject to traceability requirements?

A3.3.7 Quality Tests

Quality tests are necessary to verify whether an item conforms to specified requirements. Such tests include incoming inspections, qualification tests, production & acceptance tests, and cover performance, reliability, maintainability, safety, and software aspects. To optimize cost and time schedule, tests should be integrated in a *test* (and screening) *strategy* at system level.

Table A3.3 Design reviews during definition, design&development of *complex equipment & systems*

	System Design Review (SDR)	Preliminary Design Reviews (PDR)	Critical Design Review (CDR)
To be performed	At the end of the definition phase	During the design phase, each time an assembly has been developed	At the end of prototype qualification tests
Goal	<ul style="list-style-type: none"> • Critical review of the system specifications on the basis of results from market research, rough analysis, comparative studies, patent situation, etc. • Feasibility check 	<ul style="list-style-type: none"> • Critical review of all documents belonging to the assembly under consideration (calculations, schematics, parts lists, test specifications, etc.) • Comparison of the target achieved with the system specifications requirements • Checking interfaces to other assemblies • Feasibility check 	<ul style="list-style-type: none"> • Critical comparison of prototype qualification test results with system requirements • Formal review of the correspondence between technical documentation and prototype • Verification of manufacturability, testability, and reproducibility • Feasibility check
Input	<ul style="list-style-type: none"> • Item list • System specifications (draft) • Documentation (analyses, reports, etc.) • Checklists (one for each participant)* 	<ul style="list-style-type: none"> • Item list • Documentation (analyses, schematics, drawings, parts lists, test specifications, work breakdown structure, interface specifications, etc.) • Reports of relevant earlier design reviews • Checklists (one for each participant)* 	<ul style="list-style-type: none"> • Item list • Technical documentation • Testing plan and procedures for prototype qualification tests • Results of prototype qualification tests • List of deviations from the system requirements • Maintenance concept • Checklists (one for each participant)*
Output	<ul style="list-style-type: none"> • System specifications • Proposal for the design phase • Interface definitions • Rough maintenance and logistic support concept • Report 	<ul style="list-style-type: none"> • Reference configuration (baseline) of the assembly considered • List of deviations from the system specifications • Report 	<ul style="list-style-type: none"> • List of the final deviations from the system specs. • Qualified and released prototypes • Frozen technical documentation • Revised maintain. concept • Production proposal • Report

* see Appendix A4 for a catalog of questions to generate project specific checklists, and Tab. 5.5 for software specific aspects; *gate review* is often used, in software projects, instead of *design review*

For hardware, methods for statistical quality control, reliability and maintainability tests (incl. accelerated tests), as well as qualification tests and screening procedures are carefully discussed in Chapter 7 and Sections 3.2-3.4 & 8.2-8.3, respectively. Test and screening strategies with *cost optimization* are developed in Section 8.4. Reliability growth is investigated in Section 7.7.

For software, basic considerations on testing are given in Section 5.3.3, see e.g. [A2.8, A2.9 (29119)] for greater details. Models for software quality growth are discussed in Section 5.3.4.

The quality and reliability (RAMS) assurance program should, in particular, answer the following questions:

1. What are the test and screening strategies at system level?
2. How are subcontractors/suppliers selected, qualified and monitored?
3. What is specified in the procurement documentation?
4. How is the incoming inspection performed?
5. Which components and materials are 100% tested? Which are 100% screened? What are the procedures for screening?
6. How are prototypes qualified? Who decides on test results?
7. How are production tests performed? Who decides on test results?
8. Which procedures are applied to defective or failed items?
9. What are the instructions for handling, transportation, storage, and shipping?
10. How is the software test strategy? Who is involved in its definition / approval?

A3.3.8 Quality Data Reporting System

Starting at the prototype qualification tests, all defects and failures should be systematically collected, analyzed and corrected. Analysis should go back to the *cause of the fault*, in order to find those actions most appropriate for avoiding *repetition of the same problem*. The concept of a *quality data reporting system* is illustrated in Fig. 1.8 and applies basically to hardware and software; detailed requirements are given in Appendix A5.

The quality and reliability (RAMS) assurance program should, in particular, answer the following questions:

1. How is the collection of defect and failure data carried out? At which project phase is started with?
2. How are defects and failures analyzed?
3. Who carries out corrective actions? Who monitors their realization? Who checks the final configuration?
4. How is evaluation and feedback of quality and reliability data organized?
5. Who is responsible for the quality data reporting system? Does production have their own locally limited version of such a system? How does this systems interface with the company's quality data reporting system?

A4 Checklists for Design Reviews

In a design review, all aspects of design and development (selection and use of components and materials, dimensioning, interfaces (hardware and/or software), software aspects, etc.), production (manufacturability, testability, reproducibility), reliability, maintainability, safety, patent regulations, value engineering, and value analysis are critically examined with the help of *checklists*. The most important design reviews are described in Table A3.3 on p. 403, see also Table 5.5 on p. 165 for software aspects. A further objective of design reviews is to *decide about continuation or stopping* the project on the basis of objective considerations (*feasibility check* in Tables A3.3 & 5.3 and in Fig. 1.6). This appendix gives a catalog of questions which can be used to generate *project specific checklists for design reviews for complex equipment and systems with high quality & reliability (RAMS) requirements*.

A4.1 System Design Review (Table A3.3)

1. What experience exists with similar equipment or systems?
2. What are the goals for performance (capability), reliability, maintainability, availability, and safety? How have they been defined? Which mission profile (required function and environmental conditions) is applicable?
3. Are the requirements realistic? Do they correspond to a market need?
4. What tentative allocation of reliability and maintainability down to assembly /unit level was undertaken?
5. What are the critical items? Are potential problems to be expected (new technologies, components or materials interfaces hardware and/or software)?
6. Have comparative studies been done? What are the results?
7. Are EMC interference problems (external/internal) to be expected?
8. Are interface problems (hard/hard, hard/soft, soft/soft) to be expected?
9. Are there potential safety/liability problems?
10. Is there a maintenance concept? Do special ergonomic requirements exist?
11. Are there special software requirements?
12. Has the patent situation been verified? Are licenses necessary?
13. Are there estimates of life-cycle cost? Have these been optimized with respect to reliability and maintainability requirements?

14. Is there a feasibility study? Where does the competition stand?
Has development risk been assessed?
15. Is the project time schedule realistic? Can the system be marketed at the right time?
16. Can supply problems be expected during production ramp-up?

A4.2 Preliminary Design Reviews (Table A3.3)

a) General

1. Is the assembly/unit under consideration a new development or only a change/modification? Can existing items (e.g. sub assemblies) be used?
2. Is there experience with similar assembly/unit? What were the problems?
3. Is there redundancy hardware and/ or software? Have common cause failures (faults) been avoided?
4. Have customer and market demands changed since the beginning of development? Can individual requirements be reduced?
5. Can the chosen solution be further simplified?
6. Are there patent problems? Do licenses have to be purchased?
7. Have expected cost and deadlines been met? Were value engineering used?

b) Environmental Conditions

1. Have environmental conditions been defined? As a function of time? Were these consequently used to determine component operating conditions?
2. How were EMC interference been determined? Has his influence been taken into account in worst case calculation/simulation?

c) Performance Parameters

1. How have been defined the main performance parameters of the assembly/unit under consideration? How was their fulfillment verified (calculations, simulation, tests)?
2. Have worst case situations been considered in calculations/simulations?
3. Have interference problems EMC (external/internal) or between hardware and software been solved? How?
4. Have applicable standards been observed during design and development?
5. Have interface problems (hardware/hardware, hardware/software, software/software) been solved? How?
6. Have prototypes been adequately tested in laboratory? How?

d) Components and Materials

1. Which components and materials do not appear in the preferred lists? For which reasons? How were these components and materials qualified?
2. Are incoming inspections necessary? For which components and materials? How and where will they be performed?
3. Which components and materials were screened? How and where will screening be performed?
4. Are suppliers guaranteed for series production? Is there at least one second source for each component and material? Have requirements for quality, reliability, and safety been met?
5. Are obsolescence problems to be expected? How will they be solved?

e) Reliability

See Table 2.8 (p. 79).

f) Maintainability

See Table 4.3 (p. 120).

g) Safety, Sustainability (sustainable development)

1. Have applicable standards concerning accident prevention and sustainable development been observed?
2. Has safety been considered with regard to external causes (natural catastrophe, sabotage, etc.)? How?
3. Has an FMEA/FMECA or similar causes-to-effects analysis been performed? Are there failure modes with critical or even catastrophic consequence? Can these be avoided? Have all single-point failures been identified? Can these be avoided?
4. Has a fail-safe analysis been performed? What were the results?
5. What safety tests are planned? Are they sufficient?
6. Have safety aspects been dealt with adequately in the documentation?

h) Human and Ergonomic Aspects (see also Section 5.2.5, pp. 158-159)

1. Have operating and maintenance procedures been defined with regard to the training level of operators and maintainers?
2. Have ergonomic factors been taken into account by defining operating conditions and operating sequences?
3. Has the man-machine interface been sufficiently considered?

i) Standardization

1. Have standard components and materials been used wherever possible?
2. Has items exchangeability been considered during design and construction?

j) Configuration

1. Is the technical documentation (schematics, drawings, etc.) complete, free of errors, and does it reflect the current state of the assembly / unit considered and of the project?
2. Have all interface problems (hardware / hardware, hardware/ software, software/software) been solved? How?
3. Can the technical documentation be frozen and considered as reference documentation (baseline)?
4. How is compatibility (upward and/or downward) assured?

k) Production and Testing

1. Which qualification tests are foreseen for prototypes? Have reliability, maintainability, and safety aspects been sufficiently considered in these tests?
2. Have all questions been answered regarding manufacturability, testability, and reproducibility?
3. Are special production processes necessary? How were the qualification results?
4. Are special transport, packaging, or storage problems to be expected?

l) Software quality (see e.g. Section 5.3 & [A2.8, A2.9 (29119)] for further specific questions)

1. Which priority list of quality attributes (Table 5.4) has been defined? How were the user involved in this list? How it has been assured that this list was consequently followed by all engineers involved in the project?
2. Which project specific written procedures for software quality have been worked out? By whom? How it has been assured that these procedures were consequently followed by all engineers involved in the project?
3. How has been the software life-cycle partitioned? Was each phase (Table 5.3) closed with a comprehensive design review (Tables 5.5)?
4. Were the interface specifications between software modules as well as between software and hardware clear, complete, and precise?
5. Is the software defect tolerant?
6. Has a fail-safe strategy been realized? Considering also hardware faults?
7. Has the software configuration management been consequently realized?
8. Has been the test strategy carefully defined and consequently realized?
9. Is an appropriate software quality growth program been realized? Are all information (Appendix A5) carefully recorded? What are the results?

A4.3 Critical Design Review (System Level, Table A3.3)

a) Technical Aspects

1. Does the documentation allow an exhaustive and correct interpretation of test procedures and results? Has the technical documentation been frozen? Has conformance with present hardware and software been checked?
2. Has a representative mission profile, with the corresponding required function and environmental conditions, been clearly defined for reliability tests?
3. Have fault criteria been defined for critical parameters? Is an indirect measurement planned for those parameters which cannot be measured accurately enough during tests?
4. Have EMC aspects been tested? How? What were the results?
5. Have human and ergonomic aspects (pp. 158-159) been checked? How?
6. How have test specifications and procedures for functional, environmental, and reliability tests been defined?
7. How have test criteria for maintainability been defined? Which failures were simulated/ introduced? How have personnel and material conditions been fixed?
8. How has availability been tested? In accordance with Section 7.2.2?
9. How have test criteria for safety been defined (accident prevention and technical safety)?
10. Have defects and failures been systematically analyzed (mode, cause, effect)?
11. Has the usefulness of corrective actions been verified? How? Also with respect to cost?
12. Have all deviations been recorded? Can they be accepted?
13. Does the system still satisfy customer/market needs?
14. Are manufacturability and reproducibility guaranteed within the framework of a production environment?
15. Can packaging, transport and storage cause problems?

b) Formal Aspects

1. Is the technical documentation complete?
2. Has the technical documentation been checked for correctness? For coherence?
3. Is uniqueness in numbering guaranteed? Even in the case of changes?
4. Is hardware labeling appropriate? Does it satisfy production and maintenance requirements?
5. Has conformance between prototype and documentation been checked?
6. Is the maintenance concept fully realized? Inclusive logistic support? Are spare parts having a different change status fully interchangeable?
7. Are production tests sufficient from today's point of view?

A5 Requirements for Quality Data Reporting Systems

A *quality data reporting system* (known also as failure reporting and corrective action system, FRACAS) is a system to collect, analyze, and correct all *defects* and *failures* occurring during production and testing of an item, as well as to evaluate and feedback the corresponding quality and reliability (RAMS) data (Fig. 1.8, p. 22). The system is generally computer-aided. Analysis of failures and defects must go back to the *root cause* in order to determine the *most appropriate (corrective) action necessary to avoid repetition of the same problem*. The quality data reporting system applies to hardware and software. It should remain active during the *operating phase*, at least for the warranty time, to collect also *field data*. This appendix summarizes the requirements for a computer-aided quality data reporting system for *complex equipment and systems* (see e. g. [A5.1–A5.6] for applications).

a) General Requirements

1. Updating, completeness, and utility of the delivered information must be the primary concern (best compromise).
2. A high level of *usability & integrity*, and minimal manual intervention should be a goal.
3. Procedures and responsibilities should be clearly defined (several levels depending upon the consequence of defects or failures).
4. The system should be flexible and easily adaptable to new needs.

b) Requirements for Data Collection

1. All data concerning *defects* and *failures* (relevant to quality, reliability, maintainability, and safety) have to be collected, from the begin of prototype qualification tests to (at least) the end of the warranty time.
2. Data collection forms should
 - be preferably 8" × 11" or A4 format
 - be project-independent and easy to fill in

- ensure that only the relevant information is entered and answers the questions: what, where, when, why, and how?
 - have a separate field (20-30%) for free-format comments (requests for analysis, logistic information, etc.), these comments do not need to be processed and should be easily separable from the fixed portion of the form.
3. Description of the *symptom* (mode), *analysis* (cause, effect), and *corrective action* undertaken should be recorded in clear text and coded at data entry by trained personnel.
 4. Data collection can be carried out in different ways
 - at a single reporting location (adequate for simple problems which can be solved directly at the reporting location)
 - from different reporting locations which *report the fault (defect or failure), analysis result, and corrective action separately*.
 Operating, reliability, maintainability, or logistic data can also be reported.
 5. Data collection forms should be entered into the computer *daily* (on line if possible), so that corrective actions can be quickly initiated (for field data, a weekly or monthly entry can be sufficient for many purposes).

c) Requirements for Analysis

1. The *cause* should be found for each defect or failure
 - at the reporting location, in the case of simple problems
 - by a fault review board, in critical cases.
2. Failures (and defects) should be classified according to
 - mode
 - sudden failure (short, open, fracture, etc.)
 - gradual failure (drift, wear-out, etc.)
 - intermittent failures, others if needed
 - cause
 - intrinsic (inherent weaknesses, wear-out, or any other intrinsic cause)
 - extrinsic (systematic failure; i.e., misuse, mishandling, design, or manufacturing error/mistake)
 - secondary failure
 - effect
 - irrelevant
 - partial failure
 - complete failure
 - critical failure (safety problem).
3. Consequence of the analysis (*repair, rework, change, scraping*) must be reported.

d) Requirements for Corrective Actions

1. Every record is considered *pending* until the necessary corrective action has been successfully completed and certified.
2. The quality data reporting system must monitor *all* corrective actions.
3. Procedures and responsibilities pertaining to *corrective action* have to be defined (simple cases usually solved by the reporting location).
4. The reporting location must be informed about a *completed* corrective action.

e) Requirements Related to Data Processing, Feedback, and Storage

1. Adequate coding must allow *data compression* and simplify data processing.
2. Up-to-date information should be available *on-line*.
3. Problem-dependent and periodic *data evaluation* must be possible.
4. At the end of a project, relevant information should be stored for comparative investigations.

f) Requirements Related to Compatibility with other Software Packages

1. Compatibility with company's configuration management and data banks should be assured.
2. Data transfer with the following external software packages should be assured (as far as possible/necessary)
 - important reliability data banks
 - quality data reporting systems of subsidiary companies
 - quality data reporting systems of large contractors.

The effort required for implementing a quality data reporting system as described above can take 3 - 6 man-years for a medium-sized company. Competence for operation and maintenance of the quality data reporting system should be with the company's quality and reliability (RAMS) assurance department (Fig. 1.7, Table A3.2). The priority for the realization of *corrective actions* is project specific and should be fixed by the *project manager*. Major problems (defects and failures) should be discussed periodically by a *fault review board* chaired by the company's quality and reliability (RAMS) assurance manager, which should have, in critical cases defined in the company's quality assurance handbook, the competence to take go/ no-go decisions.

A6 Basic Probability Theory

In many practical situations, experiments have a *random outcome*; i. e., results cannot be predicted exactly, although the *same experiment* is repeated under *identical conditions*. Examples in reliability engineering are failure-free time of a given system, repair time of an equipment, inspection of a given item during production, etc. Experience shows that as the number of repetitions of the same experiment increases, certain *regularities* appear regarding the occurrence of the event considered. *Probability theory* is a mathematical discipline which investigates laws describing such regularities. The assumption of *unlimited repeatability* of the same experiment is basic to probability theory. This assumption permits the introduction of the concept of *probability* for an event starting from the properties of the *relative frequency* of its occurrence in a long series of trials. The *axiomatic theory of probability*, introduced by A.N. Kolmogorov [A6.10], brought probability theory to a *mathematical discipline*. In *reliability analysis*, probability theory allows the investigation of the probability that a given item will operate failure-free for a stated period of time under given conditions, i. e., the calculation of the item's *reliability* on the basis of a *mathematical model*. The corresponding rules are presented in Sections A6.1–A6.4. The following sections are devoted to the concept of *random variables*, necessary to investigate reliability as a function of time and as a basis for *stochastic processes* (Appendix A7) and *mathematical statistics* (Appendix A8). This appendix is a compendium of probability theory, consistent from a mathematical point of view but still with reliability engineering applications in mind (demonstration of established theorems is referred, and for all other propositions or equations, sufficient details for complete demonstration are given). To simplify the notation, *mean* is used for *expected value*, and *independent* for *totally* (mutually, statistically, stochastically) *independent* (p. 419). Selected examples illustrate the practical aspects.

A6.1 Field of Events

As introduced 1933 by A.N. Kolmogorov [A6.10], the mathematical model of an experiment with random outcome is a triplet $[\Omega, \mathcal{F}, \text{Pr}]$, also called *probability space*. Ω is the *sample space*, \mathcal{F} the *event field*, and Pr the *probability* of each element of \mathcal{F} . Ω is a set containing as elements all possible outcomes of the experiment considered. Hence $\Omega = \{1, 2, 3, 4, 5, 6\}$ if the experiment consists of a single throw of a die, and $\Omega = (0, \infty)$ in the case of failure-free times of an item. The elements of Ω are called *elementary events* and are represented by ω . If the logical

statement “the outcome of the experiment is a subset A of Ω ” is identified with the subset A itself, combinations of statements become equivalent to operations with subsets of Ω . If the sample space Ω is finite or countable, a probability can be assigned to every subset of Ω . In this case, the event field \mathcal{F} contains *all* subsets of Ω and all combinations of them. If Ω is continuous, restrictions are necessary. The *event field* \mathcal{F} is thus a system of subsets of Ω to each of which a probability has been assigned according to the situation considered. Such a field is called a σ -field (σ -algebra) and has the following properties:

1. Ω is an element of \mathcal{F} .
2. If A is an element of \mathcal{F} , its complement \bar{A} is also an element of \mathcal{F} .
3. If A_1, A_2, \dots are elements of \mathcal{F} , the countable union $A_1 \cup A_2 \cup \dots$ is also an element of \mathcal{F} .

From the first two properties it follows that the *empty set* \emptyset belongs to \mathcal{F} . From the last two properties and *De Morgan's law* one recognizes that the countable intersection $A_1 \cap A_2 \cap \dots$ also belongs to \mathcal{F} . In probability theory, the elements of \mathcal{F} are called (random) *events*. The most important *operations on events* are the union, the intersection, and the complement:

1. The *union* of a finite or countable sequence A_1, A_2, \dots of events is an event which occurs if *at least one* of the events A_1, A_2, \dots occurs; it will be denoted by $A_1 \cup A_2 \cup \dots$ or by $\bigcup_i A_i$.
2. The *intersection* of a finite or countable sequence A_1, A_2, \dots of events is an event which occurs if *each one* of the events A_1, A_2, \dots occurs; it will be denoted by $A_1 \cap A_2 \cap \dots$ or by $\bigcap_i A_i$.
3. The *complement* of an event A is an event which occurs if and only if A does not occur; it is denoted by \bar{A} , $\bar{A} = \{\omega: \omega \notin A\} = \Omega \setminus A$, $A \cup \bar{A} = \Omega$, $A \cap \bar{A} = \emptyset$.

Important properties of *set operations* are:

- Commutative law : $A \cup B = B \cup A$; $A \cap B = B \cap A$
- Associative law : $A \cup (B \cap C) = (A \cup B) \cap C$; $A \cap (B \cup C) = (A \cap B) \cup C$
- Distributive law : $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$; $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- Complement law : $A \cap \bar{A} = \emptyset$; $A \cup \bar{A} = \Omega$
- Idempotent law : $A \cup A = A$; $A \cap A = A$
- De Morgan's law : $\overline{A \cup B} = \bar{A} \cap \bar{B}$; $\overline{A \cap B} = \bar{A} \cup \bar{B}$
- Identity law : $\bar{\bar{A}} = A$; $A \cup (A \cap B) = A \cup B$.

The sample space Ω is also called the *sure event* and \emptyset is the *impossible event*. The events A_1, A_2, \dots are *mutually exclusive* if $A_i \cap A_j = \emptyset$ holds for any $i \neq j$. The events A and B are *equivalent* if either they occur together or neither of them occur, equivalent events have the same probability. In the following, events will be mainly enclosed in braces $\{ \}$.

A6.2 Concept of Probability

Let us assume that 10 *samples* (random samples) of size $n = 100$ were taken from a large and homogeneous lot of populated printed circuit boards (PCBs), for incoming inspection. Examination yielded the following results:

Sample number:	1	2	3	4	5	6	7	8	9	10
No. of defective PCBs:	6	5	1	3	4	0	3	4	5	7

For 1000 repetitions of the “testing a PCB” experiment, the *relative frequency* of the occurrence of event {PCB defective} is

$$\frac{6+5+1+3+4+0+3+4+5+7}{1000} = \frac{38}{1000} = 3.8\%.$$

It is *intuitively appealing* to consider 0.038 as the *probability* of the event {PCB defective}. As shown below, 0.038 is a *reasonable estimation* of this probability (on the basis of the experimental observations made).

Relative frequencies of the occurrence of events have the property that if n is the number of trial repetitions and $n(A)$ the number of those trial repetitions in which the event A occurred, then

$$\hat{p}_n(A) = \frac{n(A)}{n} \tag{A6.1}$$

is the *relative frequency* of the occurrence of A , and the following rules apply:

1. R1: $\hat{p}_n(A) \geq 0$.
2. R2: $\hat{p}_n(\Omega) = 1$.
3. R3: if the events A_1, \dots, A_m are *mutually exclusive*, then $n(A_1 \cup \dots \cup A_m) = n(A_1) + \dots + n(A_m)$ and $\hat{p}_n(A_1 \cup \dots \cup A_m) = \hat{p}_n(A_1) + \dots + \hat{p}_n(A_m)$.

Experience shows that for a second group of n trials, the relative frequency $\hat{p}_n(A)$ can be different from that of the first group. $\hat{p}_n(A)$ also depends on the number of trials n . On the other hand, experiments have confirmed that with increasing n , the value $\hat{p}_n(A)$ converges toward a fixed value $p(A)$, see Fig. A6.1 for an example. It therefore seems reasonable to designate the limiting value $p(A)$ as the *probability* $\Pr\{A\}$ of the event A , with $\hat{p}_n(A)$ as an *estimate* of $\Pr\{A\}$. Although intuitive, such a definition of probability would lead to problems in the case of continuous (non-denumerable) sample spaces.

Since Kolmogorov's work [A6.10], the probability $\Pr\{A\}$ has been defined as a function on the event field \mathcal{F} of subsets of Ω . The following axioms hold for this function:

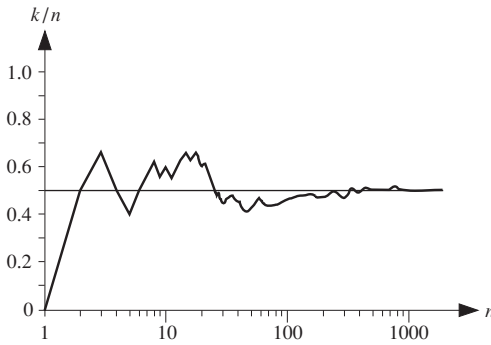


Figure A6.1 Example of relative frequency k/n of “heads” when tossing a symmetric coin n times

1. Axiom 1: For each $A \in \mathcal{F}$ is $\Pr\{A\} \geq 0$.
2. Axiom 2: $\Pr\{\Omega\} = 1$.
3. Axiom 3: If events A_1, A_2, \dots are mutually exclusive, then

$$\Pr\left\{\bigcup_{i=1}^{\infty} A_i\right\} = \sum_{i=1}^{\infty} \Pr\{A_i\}.$$

Axiom 3 is equivalent to the following statements taken together:

4. Axiom 3': For any *finite* collection of mutually exclusive events,

$$\Pr\{A_1 \cup \dots \cup A_n\} = \Pr\{A_1\} + \dots + \Pr\{A_n\}.$$
5. Axiom 3'': If events A_1, A_2, \dots are increasing, i.e. $A_n \subseteq A_{n+1}$, $n = 1, 2, \dots$,

$$\text{then } \lim_{n \rightarrow \infty} \Pr\{A_n\} = \Pr\left\{\bigcup_{i=1}^{\infty} A_i\right\}.$$

The relationships between Axiom 1 and R1, and between Axiom 2 and R2 are obvious. Axiom 3 postulates the *total additivity* of the set function $\Pr\{A\}$. Axiom 3' corresponds to R3. Axiom 3'' implies a *continuity property* of the set function $\Pr\{A\}$ which cannot be derived from the properties of $\hat{p}_n(A)$, but which is of great importance in probability theory. It should be noted that the interpretation of the probability of an event as the *limit of the relative frequency* of occurrence of this event in a long series of trial repetitions, appears as a theorem within the probability theory (laws of large numbers, Eqs. (A6.144) and (A6.146)).

From axioms 1 to 3 it follows that:

$$\Pr\{\emptyset\} = 0,$$

$$\Pr\{A\} \leq \Pr\{B\} \text{ if } A \subseteq B,$$

$$\Pr\{\bar{A}\} = 1 - \Pr\{A\},$$

$$0 \leq \Pr\{A\} \leq 1.$$

When modeling an experiment with random outcome by means of the probability space $[\Omega, \mathcal{F}, \Pr]$, the difficulty is often in the determination of the probabilities $\Pr\{A\}$ for every $A \in \mathcal{F}$. The structure of the experiment can help here. Beside the *statistical probability*, defined as the limit for $n \rightarrow \infty$ of the relative frequency k/n , the following rules can be used if one assumes that all elementary events ω have the *same chance of occurrence*:

1. *Classical probability* (discrete uniform distribution): If Ω is a finite set and A a subset of Ω , then

$$\Pr\{A\} = \frac{\text{number of elements in } A}{\text{number of elements in } \Omega}$$

or

$$\Pr\{A\} = \frac{\text{number of favorable outcomes}}{\text{number of possible outcomes}}. \tag{A6.2}$$

2. *Geometric probability* (spatial uniform distribution): If Ω is a set in the plane \mathcal{R}^2 of area Ω and A a subset of Ω , then

$$\Pr\{A\} = \frac{\text{area of } A}{\text{area of } \Omega}. \tag{A6.3}$$

It should be noted that the geometric probability can also be defined if Ω is a part of the Euclidean space having a finite area. Examples A6.1 and A6.2 illustrate the use of Eqs. (A6.2) and (A6.3).

Example A6.1

From a shipment containing 97 good and 3 defective ICs, one IC is randomly selected. What is the probability that it is defective?

Solution

From Eq. (A6.2),

$$\Pr\{\text{IC defective}\} = \frac{3}{100}.$$

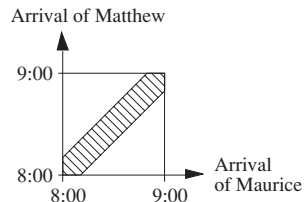
Example A6.2

Maurice and Matthew wish to meet between 8:00 and 9:00 a.m. according to the following rules: 1) They come independently of each other and each will wait 12 minutes. 2) The time of arrival is equally distributed between 8:00 and 9:00 a.m. What is the probability that they will meet?

Solution

Equation (A6.3) can be applied and leads to, see graph,

$$\Pr\{\text{Matthew meets Maurice}\} = \frac{1 - 2 \cdot \frac{0.8 \cdot 0.8}{2}}{1} = 0.36.$$



Another way to determine probabilities is to calculate them from other probabilities which are known. This involves paying attention to the structure of the experiment and application of the rules of probability theory (Appendix A6.4). For example, the predicted reliability of a system can be calculated from the reliability of its elements and the system's structure. However, there is often no alternative to determining probabilities as the limits of relative frequencies, with the aid of statistical methods (Appendices A6.11 and A8).

A6.3 Conditional Probability, Independence

The concept of conditional probability is of great importance in practical applications. It is not difficult to accept that the information "event A has occurred in an experiment" can modify the probabilities of other events. These new probabilities are defined as *conditional probabilities* and denoted by $\Pr\{B \mid A\}$. If for example $A \subseteq B$, then $\Pr\{B \mid A\} = 1$, which is in general different from the original unconditional probability $\Pr\{B\}$. The concept of conditional probability $\Pr\{B \mid A\}$ of the event B under the condition "event A has occurred", is introduced here using the properties of relative frequency. Let n be the total number of trial repetitions and let $n(A)$, $n(B)$, and $n(A \cap B)$ be the number of occurrences of A , B and $A \cap B$, respectively, with $n(A) > 0$ assumed. When considering only the $n(A)$ trials (trials in which A occurs), then B occurs in these $n(A)$ trials exactly when it occurred together with A in the original trial series, i. e. $n(A \cap B)$ times. The relative frequency of B in the trials with the information "A has occurred" is therefore

$$\frac{n(A \cap B)}{n(A)} = \frac{\frac{n(A \cap B)}{n}}{\frac{n(A)}{n}} = \frac{\hat{p}_n(A \cap B)}{\hat{p}_n(A)}. \quad (\text{A6.4})$$

Equation (A6.4) leads to the following *definition* of the *conditional probability* $\Pr\{B \mid A\}$ of an event B under the condition A (i.e., assuming that A has occurred)

$$\Pr\{B \mid A\} = \frac{\Pr\{A \cap B\}}{\Pr\{A\}}, \quad \Pr\{A\} > 0. \quad (\text{A6.5})$$

From Eq. (A6.5) it follows that

$$\Pr\{A \cap B\} = \Pr\{A\} \Pr\{B \mid A\} = \Pr\{B\} \Pr\{A \mid B\}. \quad (\text{A6.6})$$

Using Eq. (A6.5), probabilities $\Pr\{B \mid A\}$ will be defined for all $B \in \mathcal{F}$. $\Pr\{B \mid A\}$

is a function of B which satisfies Axioms 1 to 3 of Appendix A6.2, obviously with $\Pr\{A | A\} = 1$. The information “event A has occurred” thus leads to a new probability space $[A, \mathcal{F}_A, \Pr_A]$, where \mathcal{F}_A consists of events of the form $A \cap B$, with $B \in \mathcal{F}$ and $\Pr_A\{B\} = \Pr\{B | A\}$, see Example A6.5. However, when considering Eq. (A6.6), another definition, with symmetry in A and B is obtained, where $\Pr\{A\} > 0$ is not required.

It is reasonable to define the events A and B as *independent* if the information “event A has occurred” does not influence the *probability* of the occurrence of event B , i. e., if

$$\Pr\{B | A\} = \Pr\{B\}. \quad (\text{A6.7})$$

From the above considerations, two events A & B are *independent* if and only if

$$\Pr\{A \cap B\} = \Pr\{A\} \Pr\{B\}. \quad (\text{A6.8})$$

For $n > 2$, the events A_1, \dots, A_n are *totally* (mutually, statistically, stochastically) *independent* if and only if for each $1 < k \leq n$ and arbitrary $1 \leq i_1 < \dots < i_k \leq n$

$$\Pr\{A_{i_1} \cap \dots \cap A_{i_k}\} = \Pr\{A_{i_1}\} \dots \Pr\{A_{i_k}\} \quad (\text{A6.9})$$

holds. Note that for *totally* (mutually, statistically, stochastically) *independence*, *pairwise independence* is a necessary but not sufficient condition for $n > 2$ (see e. g. [A6.6 (Vol 1), A6.7] for some examples). However, for reliability applications, pairwise independence assures in general totally independence;

for this reason, independent will be used in this book for totally (mutually, statistically, stochastically) independent.

A6.4 Fundamental Rules of Probability Theory

The probability calculation of event combinations is based on the fundamental rules of probability theory introduced in this section.

A6.4.1 Addition Theorem for Mutually Exclusive Events

The events A and B are *mutually exclusive* if the *occurrence* of one event *excludes* the occurrence of the other, formally $A \cap B = \emptyset$. Considering a component which can fail due to a short or an open circuit, the events

{ failure occurs due to a short circuit }

and

{ failure occurs due to an open circuit }

are mutually exclusive. Application of Axiom 3 (Appendix A6.2) leads to

$$\Pr\{A \cup B\} = \Pr\{A\} + \Pr\{B\}. \quad (\text{A6.10})$$

Equation (A6.10) is considered a theorem by tradition only; indeed, it is a particular case of Axiom A3 in Appendix A6.2.

Example A6.3

A shipment of 100 diodes contains 3 diodes with shorts and 2 diodes with opens. If one diode is randomly selected from the shipment, what is the probability that it is defective?

Solution

From Eqs. (A6.10) and (A6.2),

$$\Pr\{\text{diode defective}\} = \frac{3}{100} + \frac{2}{100} = \frac{5}{100}.$$

If the events A_1, A_2, \dots are mutually exclusive ($A_i \cap A_j = \emptyset$ for all $i \neq j$), they are also *totally exclusive*. According to Axiom 3 it follows that

$$\Pr\{A_1 \cup A_2 \cup \dots\} = \sum_i \Pr\{A_i\}. \quad (\text{A6.11})$$

A6.4.2 Multiplication Theorem for Two Independent Events

The events A and B are *independent* if the information about occurrence (or nonoccurrence) of one event has no influence on the *probability* of occurrence of the other event ($\Pr\{B | A\} = \Pr\{B\}$, $\Pr\{A | B\} = \Pr\{A\}$). In this case Eq. (A6.8) applies

$$\Pr\{A \cap B\} = \Pr\{A\} \Pr\{B\}.$$

Example A6.4

A system consists of two elements E_1 and E_2 necessary to fulfill the required function. The failure of one element has *no influence* on the other. $R_1 = 0.8$ is the reliability of E_1 and $R_2 = 0.9$ is that of E_2 . What is the reliability R_S of the system?

Solution

Considering the assumed independence between the elements E_1 and E_2 and the definition of R_1 , R_2 , and R_S as $R_1 = \Pr\{E_1 \text{ fulfills the required function}\}$, $R_2 = \Pr\{E_2 \text{ fulfills the required function}\}$, and $R_S = \Pr\{E_1 \text{ fulfills the required function} \cap E_2 \text{ fulfills the required function}\}$, one obtains from Eq. (A6.8)

$$R_S = R_1 R_2 = 0.72.$$

A6.4.3 Multiplication Theorem for Arbitrary Events

For *arbitrary events* A and B , with $\Pr\{A\} > 0$ and $\Pr\{B\} > 0$, Eq. (A6.6) applies

$$\Pr\{A \cap B\} = \Pr\{A\} \Pr\{B \mid A\} = \Pr\{B\} \Pr\{A \mid B\}.$$

Example A6.5

2 ICs are randomly selected from a shipment of 95 good and 5 defective ICs. What is the probability of having (i) no defective ICs, and (ii) exactly one defective IC?

Solution

(i) From Eqs. (A6.6) and (A6.2),

$$\Pr\{\text{first IC good} \cap \text{second IC good}\} = \frac{95}{100} \cdot \frac{94}{99} = 0.902.$$

(ii) $\Pr\{\text{exactly one defective IC}\} = \Pr\{(\text{first IC good} \cap \text{second IC defective}) \cup (\text{first IC defective} \cap \text{second IC good})\}$; from Eqs. (A6.6) and (A6.2),

$$\Pr\{\text{one IC defective}\} = \frac{95}{100} \cdot \frac{5}{99} + \frac{5}{100} \cdot \frac{95}{99} = 0.096.$$

Generalization of Eq. (A6.6) leads to the *multiplication theorem*

$$\begin{aligned} \Pr\{A_1 \cap \dots \cap A_n\} &= \Pr\{A_1\} \Pr\{A_2 \mid A_1\} \Pr\{A_3 \mid (A_1 \cap A_2)\} \\ &\quad \dots \Pr\{A_n \mid (A_1 \cap \dots \cap A_{n-1})\}. \end{aligned} \quad (\text{A6.12})$$

Here, $\Pr\{A_1 \cap \dots \cap A_{n-1}\} > 0$ is assumed. An important special case arises when the events A_1, \dots, A_n are *independent*, in this case Eq. (A6.9) yields

$$\Pr\{A_1 \cap \dots \cap A_n\} = \Pr\{A_1\} \dots \Pr\{A_n\} = \prod_{i=1}^n \Pr\{A_i\}.$$

This last equation implies that A_1, \dots, A_n are *totally* (mutually, statistically, stochastically) *independent* (*independent* in this book, as pointed out with Eq. (A6.9)).

A6.4.4 Addition Theorem for Arbitrary Events

The probability of *occurrence of at least one* of the arbitrary events A and B (not necessarily mutually exclusive, nor independent) is given by

$$\Pr\{A \cup B\} = \Pr\{A\} + \Pr\{B\} - \Pr\{A \cap B\}. \quad (\text{A6.13})$$

To prove this, consider Axiom 3 and the partitioning of the events $A \cup B$ and B into mutually exclusive events ($A \cup B = A \cup (\bar{A} \cap B)$ and $B = (A \cap B) \cup (\bar{A} \cap B)$).

Example A6.6

To increase the reliability of a system, 2 machines are used in active (parallel) redundancy. The reliability of each machine is 0.9 and each machine operates and fails *independently* of the other. What is the system's reliability?

Solution

From Eqs. (A6.13) and (A6.8), $\Pr\{\text{the first machine fulfills the required function} \cup \text{the second machine fulfills the required function}\} = 0.9 + 0.9 - 0.9 \cdot 0.9 = 0.99$.

The *addition theorem* can be generalized to n arbitrary events. For $n = 3$ one obtains

$$\begin{aligned} \Pr\{A \cup B \cup C\} &= \Pr\{A \cup (B \cup C)\} = \Pr\{A\} + \Pr\{B \cup C\} - \Pr\{A \cap (B \cup C)\} \\ &= \Pr\{A\} + \Pr\{B\} + \Pr\{C\} - \Pr\{B \cap C\} - \Pr\{A \cap B\} \\ &\quad - \Pr\{A \cap C\} + \Pr\{A \cap B \cap C\}. \end{aligned} \quad (\text{A6.14})$$

In general, $\Pr\{A_1 \cup \dots \cup A_n\}$ follows from the so-called *inclusion/exclusion* method

$$\Pr\{A_1 \cup \dots \cup A_n\} = \sum_{k=1}^n (-1)^{k+1} S_k \quad (\text{A6.15})$$

with

$$S_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} \Pr\{A_{i_1} \cap \dots \cap A_{i_k}\} . \quad (\text{A6.16})$$

It can be shown that $S = \Pr\{A_1 \cup \dots \cup A_n\} \leq S_1$, $S \geq S_1 - S_2$, $S \leq S_1 - S_2 + S_3$, etc. Although the upper bounds do not necessarily decrease and the lower bounds do not necessarily increase, a good approximation for S often results from only a few S_i (considering e.g. the *Fréchet theorem* $S_{k+1} \leq S_k (n-k)/(k+1)$).

A6.4.5 Theorem of Total Probability

Let A_1, A_2, \dots be *mutually exclusive* events ($A_i \cap A_j = \emptyset$, $i \neq j$), $\Omega = A_1 \cup A_2 \cup \dots$, and $\Pr\{A_i\} > 0$, $i = 1, 2, \dots$. For an arbitrary event B one has $B = B \cap \Omega = B \cap (A_1 \cup A_2 \cup \dots) = (B \cap A_1) \cup (B \cap A_2) \cup \dots$, where the events $B \cap A_1, B \cap A_2, \dots$ are mutually exclusive. Use of Axiom 3 (Appendix A6.2) and Eq. (A6.6) yields

$$\Pr\{B\} = \sum_i \Pr\{B \cap A_i\} = \sum_i \Pr\{A_i\} \Pr\{B \mid A_i\}. \quad (\text{A6.17})$$

Equation (A6.17) expresses the *theorem of total probability*. Equations (A6.17) and (A6.6) lead to the *Bayes theorem*, which allows calculation of the *a posteriori probability* $\Pr\{A_k \mid B\}$, $k = 1, 2, \dots$ as a function of *a priori probabilities* $\Pr\{A_i\}$,

$$\Pr\{A_k \mid B\} = \frac{\Pr\{A_k \cap B\}}{\Pr\{B\}} = \frac{\Pr\{A_k\} \Pr\{B \mid A_k\}}{\sum_i \Pr\{A_i\} \Pr\{B \mid A_i\}}. \quad (\text{A6.18})$$

Example A6.7

ICs are purchased from 3 suppliers (A_1, A_2, A_3) in quantities of 1000, 600, and 400 pieces, respectively. The probabilities for an IC to be defective are 0.006 for A_1 , 0.02 for A_2 , and 0.03 for A_3 . The ICs are stored in a common container disregarding their source. What is the probability that one IC randomly selected from the stock is defective?

Solution

From Eqs. (A6.17) and (A6.2),

$$\Pr\{\text{the selected IC is defective}\} = \frac{1000}{2000} \cdot 0.006 + \frac{600}{2000} \cdot 0.02 + \frac{400}{2000} \cdot 0.03 = 0.015.$$

Example A6.8

Let the IC as selected in Example A6.7 be defective. What is the probability that it is from supplier A_1 ?

Solution

$$\text{From Eq. (A6.18), } \Pr\{\text{IC from } A_1 \mid \text{IC defective}\} = \frac{(1000 / 2000) \cdot 0.006}{0.015} = 0.2.$$

A6.5 Random Variables, Distribution Functions

If the result of an experiment with a random outcome is a (real) number, then the underlying quantity is a (real) *random variable*. For example, the number appearing when throwing a die is a random variable taking on values in $\{1, \dots, 6\}$. Random variables are designated hereafter with Greek letters τ, ξ, ζ , etc. The triplet $[\Omega, \mathcal{F}, \Pr]$ introduced in Appendix A6.2 becomes $[\mathcal{R}, \mathcal{B}, \Pr]$, where $\mathcal{R} = (-\infty, \infty)$ and \mathcal{B} is the smallest event field containing all (semi) intervals $(a, b]$ with $a < b$. The probabilities $\Pr\{A\} = \Pr\{\tau \in A\}$, $A \in \mathcal{B}$, define the distribution law of the random variable τ . Among the many possibilities to characterize this *distribution law*, the most frequently used is to define

$$F(t) = \Pr\{\tau \leq t\}. \quad (\text{A6.19})$$

$F(t)$ is called the (cumulative) *distribution function* of the *random variable* τ ⁺⁾ . For each t , $F(t)$ gives the *probability* that the random variable will assume a value smaller than or equal to t . Since $s > t$ implies $\{\tau \leq t\} \subseteq \{\tau \leq s\}$, $F(t)$ is a *non-decreasing function*. Moreover, $F(-\infty) = 0$ and $F(\infty) = 1$. If $\Pr\{\tau = t_0\} > 0$ holds, then $F(t)$ has a jump of height $\Pr\{\tau = t_0\} = F(t_0) - F(t_0 - 0)$ at t_0 . As stated also with Eq. (A6.19), $F(t)$ is *continuous from the right* (Fig. A8.1); however, $F(t)$ can have at most a countable number of jumps (see e.g. [A6.7]). The probability that the

⁺⁾ From a mathematical point of view, the random variable τ is defined as a *measurable mapping* of Ω onto the axis of real numbers $\mathcal{R} = (-\infty, \infty)$, i.e. a mapping such that for each real value x the set of ω for which $\{\tau = \tau(\omega) \leq x\}$ belongs to \mathcal{F} ; the distribution function of τ is then obtained by setting $F(t) = \Pr\{\tau \leq t\} = \Pr\{\omega: \tau(\omega) \leq t\}$.

random variable τ takes on a value within the interval $(a, b]$ is

$$\Pr\{a < \tau \leq b\} = F(b) - F(a).$$

The following two kinds of random variables are of particular importance:

1. *Discrete random variables:* A random variable τ is discrete if it can only assume a finite or countable number of values, i. e., if there is a sequence t_1, t_2, \dots such that

$$p_k = \Pr\{\tau = t_k\}, \quad \text{with} \quad \sum_k p_k = 1. \tag{A6.20}$$

A discrete random variable is best described by a table

Values of τ	t_1	t_2	\dots
Probabilities	p_1	p_2	\dots

The distribution function $F(t)$ of a discrete random variable τ is a *step function*

$$F(t) = \sum_{k: t_k \leq t} p_k .$$

Assuming the sequence t_1, t_2, \dots ordered ($t_k < t_{k+1}$), then

$$F(t) = \sum_{j \leq k} p_j, \quad \text{for} \quad t_k \leq t < t_{k+1} \quad (k = 0, 1, 2, \dots, t_0 < t_1, p_0 = 0) . \tag{A6.21}$$

If only the value $k = 1$ occurs in Eqs. (A6.21), τ is a *constant* ($\tau = t_1 = C$). A constant C can thus be regarded as a random variable with distribution function

$$F(t) = \begin{cases} 0 & \text{for } t < C \\ 1 & \text{for } t \geq C . \end{cases}$$

An important special case is that of *arithmetic random variables*. τ is arithmetic if it can take the values $\dots, -\Delta t, 0, \Delta t, \dots$, with probabilities

$$p_k = \Pr\{\tau = k \Delta t\}, \quad k = \dots, -1, 0, 1, \dots .$$

2. *Continuous random variables:* The random variable τ is *absolutely continuous* if a function $f(x) \geq 0$ exists such that

$$F(t) = \Pr\{\tau \leq t\} = \int_{-\infty}^t f(x) dx . \tag{A6.22}$$

$f(t)$ is called (probability) *density* of the random variable τ and satisfies

$$f(t) \geq 0 \quad \text{and} \quad \int_{-\infty}^{\infty} f(t) dt = 1 .$$

$F(t)$ and $f(t)$ are related (almost everywhere) by (Fig. A6.2)

$$f(t) = dF(t) / dt . \tag{A6.23}$$

Mixed distribution functions, exhibiting jumps and continuous growth, can occur in some applications, requiring a piecewise definition of the distribution function.

In reliability theory, $\tau > 0$ generally denotes (as in this book) the *failure-free time* (failure-free operating time) of an item, distributed according to $F(t)=\Pr\{\tau \leq t\}$ with $F(0)=0$. The *reliability function* $R(t)$ (also known as *survival function*) gives the probability that the item new at $t=0$ will operate failure-free in $(0, t]$; thus,

$$F(t)=\Pr\{\tau \leq t\} \text{ and } R(t)=\Pr\{\tau > t\}=1-F(t), \quad t > 0, F(0)=0, R(0)=1. \quad (\text{A6.24})$$

The *failure rate* $\lambda(t)$ (instantaneous failure rate in some standards) of an item new at $t=0$ and exhibiting a continuous failure-free time $\tau > 0$ is defined as

$$\lambda(t)=\lim_{\delta t \downarrow 0} \frac{1}{\delta t} \cdot \Pr\{t < \tau \leq t+\delta t \mid \tau > t\}.$$

Calculation leads to (Eq. (A6.5) and Fig. A6.3a)

$$\lambda(t)=\lim_{\delta t \downarrow 0} \frac{1}{\delta t} \cdot \frac{\Pr\{t < \tau \leq t+\delta t \cap \tau > t\}}{\Pr\{\tau > t\}} = \lim_{\delta t \downarrow 0} \frac{1}{\delta t} \cdot \frac{\Pr\{t < \tau \leq t+\delta t\}}{\Pr\{\tau > t\}},$$

and thus, assuming the existence of $f(t)=dF(t)/dt$,

$$\lambda(t)=\frac{f(t)}{1-F(t)} = -\frac{dR(t)/dt}{R(t)}, \quad t > 0, (\lambda(t)=F(t)=f(t)=0 \text{ for } t \leq 0). \quad (\text{A6.25})$$

It is important to distinguish between *density* $f(t)$ and *failure rate* $\lambda(t)$. For an item new at $t=0$ & $\delta t \rightarrow 0$, $f(t)\delta t$ is the *unconditional* probability for failure in $(t, t+\delta t]$, whereas $\lambda(t)\delta t$ is the *conditional* probability for failure in $(t, t+\delta t]$ given that the

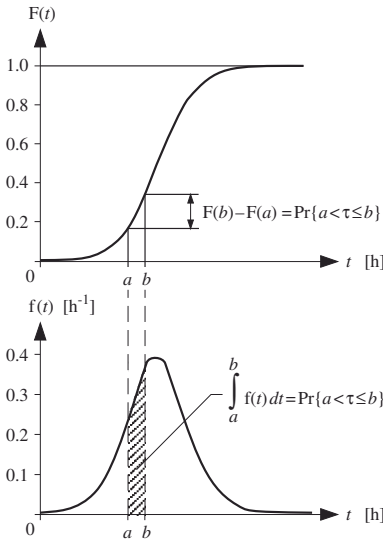


Figure A6.2 Relationship between the distribution function $F(t)$ and the density $f(t)$

item has not failed in $(0, t]$. Moreover, $\int_0^\infty f(t)dt=1$ and $\int_0^\infty \lambda(t)dt = \ln R(0) - \ln R(\infty) = \infty$, showing that $\lambda(t)$ is not a density (as defined by Eqs. (A6.22)-(A6.23)).⁺⁾

The failure rate $\lambda(t)$ applies to *nonrepairable* items. However,

considering Eq. (A6.25) it can also be defined for repairable items which are as-good-as-new after repair (renewal), taking instead of t the variable x starting by $x=0$ at each repair (as for interarrival times); this is necessary when investigating repairable items (systems).

If a repairable item can not be restored to as-good-as-new after repair, *failure intensity* $z(t)$ (Eq. (A7.228)) has to be used (see pp. 377 & 524).

$\lambda(t)$ completely define $R(t)$. In fact, considering $R(0) = 1$, Eq. (A6.25) yields

$$\Pr\{\tau > t\} = 1 - F(t) = R(t) = e^{-\int_0^t \lambda(x)dx}, \quad t > 0, R(0) = 1. \quad (A6.26)$$

from which $R(t) = e^{-\lambda t}$ for $\lambda(x) = \lambda$.

The probability for failure-free operation in $(0, t]$ given that at $t=0$ the item has already operated a failure-free time $x_0 > 0$ is often asked; Eqs. (A6.5) & (A6.26) yield

$$\Pr\{\tau > t+x_0 \mid \tau > x_0\} = R(t \mid x_0) = R(t+x_0) / R(x_0) = e^{-\int_{x_0}^{t+x_0} \lambda(x)dx}. \quad (A6.27)$$

$R(t \mid x_0)$ is the *conditional reliability function*. Equations (A6.25) & (A6.27) lead to

$$-\frac{dR(t \mid x_0)/dt}{R(t \mid x_0)} = \lambda(t \mid x_0) = \lambda(t+x_0) \quad \& \quad E[\tau-x_0 \mid \tau > x_0] = \int_0^\infty R(t \mid x_0)dt = \int_{x_0}^\infty \frac{R(x)}{R(x_0)} dx. \quad (A6.28)$$

The 2nd part of Eq. (A6.28) gives the *mean of the survival failure-free time at age x_0* (conditional mean). From Eqs. (A6.26)-(A6.28) following conclusions can be drawn:

1. The *conditional failure rate* $\lambda(t \mid x_0)$ at time t given that the item has operated failure-free a time x_0 before $t=0$ is the *failure rate at time $t+x_0$* .
2. For *strictly increasing failure rate* $\lambda(t)$ it holds that $R(t+x_0) < R(t) \cdot R(x_0)$ and $E[\tau-x_0 \mid \tau > x_0] < E[\tau]$; the contrary for strictly decreasing failure rate.
3. In point 2, = *instead of $<$ holds if and only if $\lambda(t) = \lambda$* , i.e., if the failure-free time is exponentially distributed.

To point 2, note that for $\lambda(t)$ strictly increasing $R(t \mid x_0) = e^{-\int_{x_0}^{t+x_0} \lambda(x)dx} < e^{-\int_0^t \lambda(x)dx} = R(t)$, yielding $R(t+x_0) < R(t) \cdot R(x_0)$ & $E[\tau-x_0 \mid \tau > x_0] < E[\tau]$. In addition to Eq. (A6.27),

$$\Pr\{\tau > t+u \mid \tau > u\} > \Pr\{\tau > t+s \mid \tau > s\}, \quad \text{for } s > u > 0 \text{ and } t > 0,$$

holds for $\lambda(t)$ strictly increasing, reinforcing that the probability of surviving a

⁺⁾ The quantity $\lambda(t)$, termed *failure rate* in this book and in most standards (Eq. (A6.25)), is known also as *hazard rate, force of mortality, density rate*. To avoid ambiguities, *conditional failure rate* could be a good choice for *failure rate*.

further period t decreases with the achieved age (contrary for decreasing failure rate). No aging exists in the case of a *constant failure rate*, i.e. for $R(t) = e^{-\lambda t}$, yielding

$$\Pr\{\tau > t + x_0 \mid \tau > x_0\} = R(t \mid x_0) = R(t) = \Pr\{\tau > t\} = e^{-\lambda t}, \quad \lambda(t) = \lambda. \quad (\text{A6.29})$$

Equation (A6.29) expresses best the *memoryless property of the exponential distribution* (Eq.(A6.81)), for which, and only for which, it holds that $\lambda(t) = \lambda$.

For a time dependent failure rate $\lambda(t)$, above considerations lead to concepts like

- (i) *bad-as-old* or *minimal repair* ($\lambda(t)$ after repair $\approx \lambda(t)$ just before failure; idealized model, if the repaired part has *time dependent failure rate* (pp.138 & 519)),
- (ii) *new-better-than-used* ($R(t + x_0) < R(t)R(x_0)$, follows for $\lambda(t)$ strictly increasing),
- (iii) *new-worse-than-used* ($R(t + x_0) > R(t)R(x_0)$, follows for $\lambda(t)$ strictly decreasing),
- (iv) *new-better-than-used in expectation* ($E[\tau - x_0 \mid \tau > x_0] < E[\tau]$, follows from ii),
- (v) *new-worse-than-used in expectation* ($E[\tau - x_0 \mid \tau > x_0] > E[\tau]$, follows from iii),

on which, *maintenance strategies* can be based (see e.g. [2.34, 4.14, 4.18, 6.3, A7.4(62)] and remarks on pp.134 and 519). Maintenance strategies are considered in Sections 4.6 & 6.8.2. Equality holds in (i)-(v) *if and only if* $\lambda(t) = \lambda$ (Eq. (A6.29)); case which should be clearly distinguished from both increasing or decreasing $\lambda(t)$, also because of the memoryless property which characterizes $\lambda(t) = \lambda$.

In applications dealing with preventive maintenance (Section 6.8.2), distribution and mean of the *undetected (latent) fault time* τ_{UFT} are often of interest. Considering a repairable *one-item structure* with failure-free time $\tau > 0$ distributed according to $F(x) = \Pr\{\tau \leq x\}$, on which preventive maintenance (PM) is performed at 0, T_{PM} , $2T_{PM}$, ... and at each PM the item is *as-good-as-new*, distribution and mean of τ_{UFT} , taking at each PM $\tau_{UFT} = 0$ for $\tau > T_{PM}$, follows as (Fig. A6.3b)

$$F_{UFT}(x) = \Pr\{\tau_{UFT} \leq x\} = 1 - F(T_{PM} - x), \quad 0 < x \leq T_{PM}, \quad F(0) = 0, \quad F_{UFT}(0) = 1 - F(T_{PM}),$$

$$E[\tau_{UFT}] = \int_0^{T_{PM}} (1 - F_{UFT}(x)) dx = \int_0^{T_{PM}} F(T_{PM} - x) dx = \int_0^{T_{PM}} F(x) dx, \quad (\text{A6.30})$$

yielding $F_{UFT}(x) = e^{-\lambda(T_{PM} - x)}$ and $E[\tau_{UFT}] = T_{PM} - (1 - e^{-\lambda T_{PM}}) / \lambda \approx \lambda T_{PM} \cdot T_{PM} / 2$ for $F(x) = 1 - e^{-\lambda x}$ & $\lambda T_{PM} \ll 1$. Less realistic seems to consider for τ_{UFT} only the cases with $\tau < T_{PM}$, yielding $F_{UFT}(x) = 1 - F(T_{PM} - x) / F(T_{PM})$, and $E[\tau_{UFT}] \approx T_{PM} / 2$ for $F(x) = 1 - e^{-\lambda x}$ & $\lambda T_{PM} \ll 1$. Further aspects related to undetected fault times are discussed with Eq. (6.223), dealing with incomplete coverage in redundant structures.

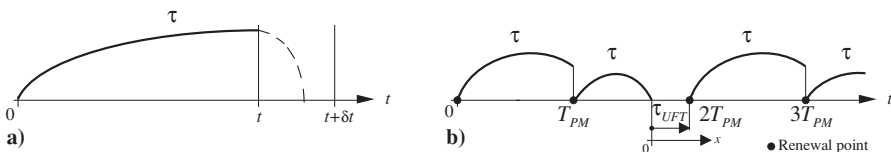


Figure A6.3 Visual aids to investigate: **a)** The failure rate $\lambda(t)$; **b)** The undetected fault time τ_{UFT}

For an arithmetic random variable, the failure rate is defined as

$$\lambda(k) = \Pr\{\tau = k \Delta t \mid \tau > (k-1)\Delta t\} = p_k / \sum_{i \geq k} p_i, \quad k = 1, 2, \dots$$

Following concepts are important to reliability theory (see also Eqs. (A6.78), (A6.79) for *minimum* (τ_{\min}) and *maximum* (τ_{\max}) of a set of random variables τ_1, \dots, τ_n):

1. *Function of a random variable*: If $u(x)$ is a *strictly increasing*, continuous function and τ a continuous random variable with distribution function $F_\tau(t)$, then $\Pr\{\tau \leq t\} = \Pr\{\eta = u(\tau) \leq u(t)\}$, and $\eta = u(\tau)$ has distribution function

$$F_\eta(t) = \Pr\{\eta \leq t\} = \Pr\{\tau \leq u^{-1}(t)\} = F_\tau(u^{-1}(t)), \quad (\text{A6.31})$$

with $u^{-1}(x)$ as *inverse function* of $u(x)$; see Example A6.18 on p. 448 (for *strictly decreasing* $u(x)$, $f_\eta(t) = f_\tau(u^{-1}(t)) \mid du^{-1}(t)/dt \mid$).

2. *Distributions with random parameter*: If the distribution function $F(t, \delta)$ of τ depends on a parameter δ with density $f_\delta(x)$, then for τ it holds that

$$F(t) = \Pr\{\tau \leq t\} = \int_0^\infty F(t, \delta) f_\delta(x) dx, \quad t, \delta \geq 0. \quad (\text{A6.32})$$

3. *Truncated distribution*: In some practical applications it can be assumed that realizations $\leq a$ or $> b$ of a random variable ξ with distribution function $F(t)$ are discarded (e. g. lifetimes ≤ 0). For a truncated random variable it holds that

$$F(t \mid a < \xi \leq b) = \begin{cases} 0 & \text{for } t \leq a \\ (F(t) - F(a)) / (F(b) - F(a)) & \text{for } a < t \leq b \\ 1 & \text{for } t > b. \end{cases} \quad (\text{A6.33})$$

4. *Mixture of distributions*: Some possibilities of how early failures and wear-out, with distribution function $F_1(t)$ and $F_2(t)$, can be considered are, for instance,

- for any of the items considered, only early failures (with probability p) or wear-out (with probability $1 - p$) can appear,
- both failure mechanisms can appear in any item,
- a percentage p of the items will show both failure mechanisms and $1 - p$ only one failure mechanism, e. g. wear-out governed by $F_2(t)$.

The distribution functions $F(t)$ of the failure-free time are in these three cases:

$$\begin{aligned} F(t) &= pF_1(t) + (1 - p)F_2(t), \\ F(t) &= 1 - (1 - F_1(t))(1 - F_2(t)) = F_1(t) + F_2(t) - F_1(t)F_2(t), \\ F(t) &= p[F_1(t) + F_2(t) - F_1(t)F_2(t)] + (1 - p)F_2(t) = pF_1(t) + F_2(t) - pF_1(t)F_2(t). \end{aligned} \quad (\text{A6.34})$$

The first case gives a *mixture* with weights p and $1 - p$ (Example 7.16). The second case corresponds to a *series model* with two independent elements, (Eq. (2.17)). The 3th case is a combination of both previous cases. The mixture can be extended to n components, yielding $F(t) = \sum_n p_k F_k(t)$ with $\sum_n p_k = 1$.

The main properties of the distribution functions frequently used in reliability theory are summarized in Table A6.1 and discussed in Appendix A6.10.

A6.6 Numerical Parameters of Random Variables

For a rough characterization of a random variable τ , some typical values such as the expected value (mean), variance, and median can be used.

A6.6.1 Expected Value (Mean)

For a discrete random variable τ taking values t_1, t_2, \dots , with probabilities p_1, p_2, \dots , the *expected value* or *mean* $E[\tau]$ is given by

$$E[\tau] = \sum_k t_k p_k, \quad (\text{A6.35})$$

provided the series converges absolutely. If τ only takes the values t_1, \dots, t_m , Eq. (A6.35) can be heuristically explained as follows. Consider n repetitions of a trial whose outcome is τ and assume that k_1 times the value t_1, \dots, k_m times the value t_m has been observed ($n = k_1 + \dots + k_m$), the arithmetic mean of the observed values is

$$(t_1 k_1 + \dots + t_m k_m) / n = t_1 k_1 / n + \dots + t_m k_m / n.$$

As $n \rightarrow \infty$, k_i/n converges to p_i (Eq. (A6.146)), and the above mean tends towards the *expected value* $E[\tau]$ given by Eq. (A6.35). For this reason, *expected value* and *mean* are often used for the same quantity $E[\tau]$; this will often occur in this book. From Eq. (A6.35), the *mean of a constant* C is the constant itself

$$E[C] = C.$$

For a random variable taking values 0 & 1 with probabilities p_0 & $p_1 = 1 - p_0$ one has

$$E[\tau] = 0 \cdot p_0 + 1 \cdot p_1 = p_1. \quad (\text{A6.36})$$

The mean of a continuous random variable τ with density $f(t)$ is given by

$$E[\tau] = \int_{-\infty}^{\infty} t f(t) dt, \quad (\text{A6.37})$$

provided the integral converges absolutely. For positive continuous random variables, Eq. (A6.37) yields (Example A6.9)

$$E[\tau] = \int_0^{\infty} t f(t) dt = \int_0^{\infty} (1 - F(t)) dt = \int_0^{\infty} R(t) dt, \quad \tau > 0. \quad (\text{A6.38})$$

For the expected value of the random variable $\eta = u(\tau)$

$$E[\eta] = \sum_k u(t_k) p_k \quad \text{or} \quad E[\eta] = \int_{-\infty}^{\infty} u(t) f(t) dt \quad (\text{A6.39})$$

holds, provided that $u(x)$ is continuous and series & integral converge absolutely.

Table A6.1 Distribution functions used in reliability analysis (with x instead of t for interarrival times)

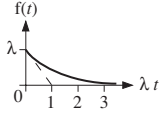
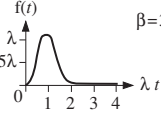
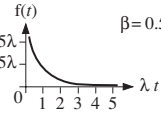
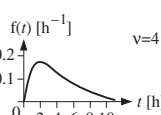
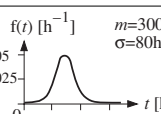
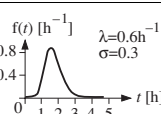
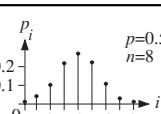
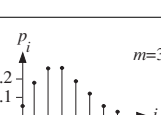
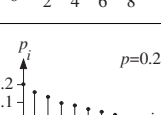
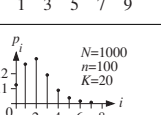
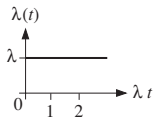
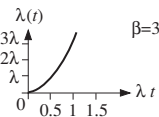
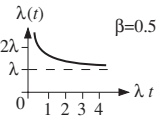
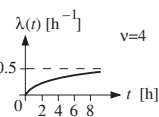
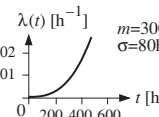
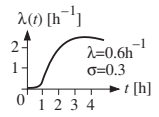
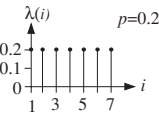
Name	Distribution Function $F(t) = \text{Pr}\{\tau \leq t\}$	Density $f(t) = dF(t)/dt$	Parameter Range
Exponential	$1 - e^{-\lambda t}$		$t > 0$ ($F(t)=0, t \leq 0$) $\lambda > 0$
Weibull	$1 - e^{-(\lambda t)^\beta}$		$t > 0$ ($F(t)=0, t \leq 0$) $\lambda, \beta > 0$
Gamma	$\frac{1}{\Gamma(\beta)} \int_0^{\lambda t} x^{\beta-1} e^{-x} dx$		$t > 0$ ($F(t)=0, t \leq 0$) $\lambda, \beta > 0$
Chi-square (χ^2)	$\frac{\int_0^t x^{v/2-1} e^{-x/2} dx}{2^{v/2} \Gamma(v/2)}$		$t > 0$ ($F(t)=0, t \leq 0$) $v = 1, 2, \dots$ (degrees of freedom)
Normal	$\frac{1}{\sigma \sqrt{2\pi}} \int_{-\infty}^t e^{-(x-m)^2/2\sigma^2} dx$		$-\infty < t, m < \infty$ $\sigma > 0$
Lognormal	$\frac{1}{\sqrt{2\pi}} \frac{\ln(\lambda t)}{\sigma} \int_{-\infty}^t e^{-x^2/2} dx$		$t > 0$ ($F(t)=0, t \leq 0$) $\lambda, \sigma > 0$
Binomial	$\text{Pr}\{\zeta \leq k\} = \sum_{i=0}^k p_i$ $p_i = \binom{n}{i} p^i (1-p)^{n-i}$		$k = 0, \dots, n$ $0 < p < 1$
Poisson	$\text{Pr}\{\zeta \leq k\} = \sum_{i=0}^k p_i$ $p_i = \frac{m^i}{i!} e^{-m}$		$k = 0, 1, \dots$ $m > 0$
Geometric	$\text{Pr}\{\zeta \leq k\} = \sum_{i=1}^k p_i = 1 - (1-p)^k$ $p_i = p(1-p)^{i-1}$		$k = 1, 2, \dots$ $0 < p < 1$
Hyper-geometric	$\text{Pr}\{\zeta \leq k\} = \sum_{i=0}^k \frac{\binom{K}{i} \binom{N-K}{n-i}}{\binom{N}{n}}$		$k = 0, 1, \dots$ $\dots, \min(K, n)$

Table A6.1 (cont.)

Failure Rate $\lambda(t) = f(t) / (1 - F(t))$	Mean $E[\tau]$	Variance $Var[\tau]$	Properties
	$\frac{1}{\lambda}$	$\frac{1}{\lambda^2}$	Memoryless: $Pr\{\tau > t + x_0 \mid \tau > x_0\} = Pr\{\tau > t\} = e^{-\lambda t}$
	$\frac{\Gamma(1 + \frac{1}{\beta})}{\lambda}$	$\frac{\Gamma(1 + \frac{2}{\beta}) - \Gamma^2(1 + \frac{1}{\beta})}{\lambda^2}$	Monotonic failure rate, strictly increasing for $\beta > 1$ ($\lambda(+0) = 0, \lambda(\infty) = \infty$), decreasing for $\beta < 1$ ($\lambda(+0) = \infty, \lambda(\infty) = 0$)
	$\frac{\beta}{\lambda}$	$\frac{\beta}{\lambda^2}$	Laplace transf. exists: $\tilde{f}(s) = \lambda\beta / (s + \lambda)^\beta$; Monotonic failure rate with $\lambda(\infty) = \lambda$; Exp. for $\beta = 1$, Erlangian for $\beta = n = 2, 3, \dots$ (sum of n exp. distrib. random variables $\mid \lambda$)
	v	$2v$	Gamma with $\beta = v/2, v = 1, 2, \dots$ and $\lambda = 1/2$; for $v = 2, 4, \dots \Rightarrow F(t) = 1 - \sum_{i=0}^{v/2-1} \frac{(t/2)^i}{i!} e^{-t/2}$ (sum of $v/2$ exp. distrib. random var. $\mid \lambda = 1/2$)
	m	σ^2	$F(t) = \Phi((t - m) / \sigma)$ $\Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^t e^{-x^2/2} dx$
	$\frac{e \sigma^2 / 2}{\lambda}$	$\frac{e^2 \sigma^2 - e \sigma^2}{\lambda^2}$	$F(t) = \Phi(\ln(\lambda t) / \sigma)$; In τ has a normal distribution with $m = \ln(1/\lambda) = E[\ln \tau]$ and $\sigma^2 = Var[\ln \tau]$
not relevant	np	$np(1-p)$	$p_i = Pr\{i \text{ successes in } n \text{ Bernoulli trials}\}$ (n independent trials with $Pr\{A\} = p$); Random sample with replacement
not relevant	m	m	$m = \lambda t \Rightarrow (\lambda t)^i e^{-\lambda t} / i! = Pr\{i \text{ failures in } (0, t] \mid \lambda\}$; $\binom{n}{i} p^i (1-p)^{n-i} \approx \frac{(np)^i}{i!} e^{-np}$
	$\frac{1}{p}$	$\frac{1-p}{p^2}$	Memoryless: $Pr\{\zeta > i + j \mid \zeta > i\} = (1-p)^j$; $P_i = Pr\{\text{first success in a sequence of Bernoulli trials occurs at the } i \text{ th trial}\}$
not relevant	$n \frac{K}{N}$	$\frac{K n (N - K) (N - n)}{N^2 (N - 1)}$	Random sample without replacement

Example A6.9

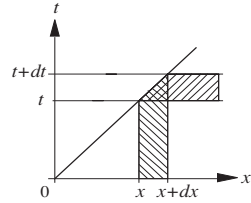
Prove Eq. (A6.38).

Solution

$$R(t) = 1 - F(t) = \int_t^\infty f(x) dx \text{ yields } \int_0^\infty R(t) dt = \int_0^\infty \left(\int_t^\infty f(x) dx \right) dt$$

Changing the order of integration it follows that (see graph)

$$\int_0^\infty R(t) dt = \int_0^\infty \left(\int_0^x dt \right) f(x) dx = \int_0^\infty x f(x) dx = E[\tau].$$



Supplementary results: Integrating by parts Eq. (A6.37) yields Eq. (A6.38) if $\lim_{x \rightarrow \infty} (x(1 - F(x))) = 0$. This holds for $E[\tau] < \infty$. To see this, consider $\int_c^d x f(x) dx \geq c \int_c^d f(x) dx = c(F(d) - F(c))$. Thus, $\lim_{d \rightarrow \infty} \int_c^d x f(x) dx \geq c(1 - F(c))$. Given $E[\tau] < \infty$, one can find for an arbitrarily small $\epsilon > 0$ a c such that $\int_c^\infty x f(x) dx < \epsilon$. From this, $c(1 - F(c)) < \epsilon$ and thus $\lim_{c \rightarrow \infty} (c(1 - F(c))) = 0$.

Two particular cases of Eq. (A6.39) are:

- 1. $u(x) = Cx$,

$$E[C\tau] = \int_{-\infty}^\infty C t f(t) dt = C E[\tau], \quad -\infty < C < \infty. \tag{A6.40}$$

- 2. $u(x) = x^k$, which leads to the k th moment of τ ,

$$E[\tau^k] = \int_{-\infty}^\infty t^k f(t) dt, \quad k > 1. \tag{A6.41}$$

Further important properties of the mean are given by Eqs. (A6.68) and (A6.69).

A6.6.2 Variance

The *variance* of a random variable τ is a measure of the spread (or dispersion) of the random variable around its mean $E[\tau]$. Variance is defined as

$$\text{Var}[\tau] = E[(\tau - E[\tau])^2], \tag{A6.42}$$

and can be calculated as

$$\text{Var}[\tau] = \sum_k (t_k - E[\tau])^2 p_k \tag{A6.43}$$

for a discrete random variable, and as

$$\text{Var}[\tau] = \int_{-\infty}^\infty (t - E[\tau])^2 f(t) dt \tag{A6.44}$$

for a continuous random variable. In both cases,

$$\text{Var}[\tau] = E[\tau^2] - (E[\tau])^2. \tag{A6.45}$$

If $E[\tau]$ or $\text{Var}[\tau]$ is infinite, τ is said to have an infinite variance. For arbitrary constants C and A , Eqs. (A6.45) and (A6.40) yield

$$\begin{aligned} \text{Var}[C\tau - A] &= C^2 \text{Var}[\tau], & -\infty < C < \infty, \\ \text{and} \\ \text{Var}[C] &= 0. \end{aligned} \tag{A6.46}$$

The quantity

$$\sigma = \sqrt{\text{Var}[\tau]} \tag{A6.47}$$

is the *standard deviation* of τ and, for $\tau \geq 0$,

$$\kappa = \sigma / E[\tau] \tag{A6.48}$$

is the *coefficient of variation* of τ . The random variable

$$(\tau - E[\tau]) / \sigma$$

has mean 0 (Eqs. (A6.40) & (A6.68)) and variance 1 (Eq. (A6.46)), and is a *standardized random variable*.

A good understanding of the variance as a measure of dispersion is given by the *Chebyshev's inequality*, which states (Example A6.10) that for every $\epsilon > 0$

$$\text{Pr}\{|\tau - E[\tau]| > \epsilon\} \leq \text{Var}[\tau] / \epsilon^2. \tag{A6.49}$$

The Chebyshev inequality (known also as Bienaymé-Chebyshev inequality) is more useful in proving convergence than as an approximation. Further important properties of the variance are given by Eqs. (A6.70) and (A6.71).

Generalization of the exponent in Eqs. (A6.43) and (A6.44) leads to the *k*th *central moment* of τ

$$E[(\tau - E[\tau])^k] = \int_{-\infty}^{\infty} (t - E[\tau])^k f(t) dt, \quad k > 1. \tag{A6.50}$$

Example A6.10

Prove the Chebyshev inequality for a continuous random variable (Eq. (A6.49)).

Solution

For a continuous random variable τ with density $f(t)$, the definition of the variance implies

$$\begin{aligned} \text{Pr}\{|\tau - E[\tau]| > \epsilon\} &= \int_{|t - E[\tau]| > \epsilon} f(t) dt \leq \int_{|t - E[\tau]| > \epsilon} \frac{(t - E[\tau])^2}{\epsilon^2} f(t) dt \\ &\leq \int_{-\infty}^{\infty} \frac{(t - E[\tau])^2}{\epsilon^2} f(t) dt = \frac{1}{\epsilon^2} \text{Var}[\tau]. \end{aligned}$$

A6.6.3 Modal Value, Quantile, Median

In addition to the moments discussed in Appendices A6.6.1 and A6.6.2, the modal value, quantile, and median are defined as follows:

1. For a continuous random variable τ , the *modal value* is the value of t for which $f(t)$ reaches its maximum; the distribution of τ is *multimodal* if $f(t)$ exhibits more than one maximum.
2. The q *quantile* is the value t_q for which $F(t)$ reaches the value q , $t_q = \inf\{t: F(t) \geq q\}$; in general, $F(t_q) = q$ for a continuous random variable (t_p , for which $1 - F(t_p) = Q(t_p) = p$, is termed *percentage point*).
3. The 0.5 quantile ($t_{0.5}$) is the *median*.

A6.7 Multidimensional Random Variables, Conditional Distributions

Multidimensional random variables (random vectors) are often required in reliability and availability investigations of repairable systems. For random vectors, the outcome of an experiment is a point in the n -dimensional space \mathcal{R}^n . The probability space $[\Omega, \mathcal{F}, \Pr]$ introduced in Appendix A6.1 becomes $[\mathcal{R}^n, \mathcal{B}^n, \Pr]$, where \mathcal{B}^n is the smallest event field which contains all "intervals" of the form $(a_1, b_1] \dots (a_n, b_n] = \{(t_1, \dots, t_n): t_i \in (a_i, b_i], i = 1, \dots, n\}$. *Random vectors* are designated by Greek letters with an arrow ($\vec{\tau} = (\tau_1, \dots, \tau_n)$, $\vec{\xi} = (\xi_1, \dots, \xi_n)$, etc.). The probabilities $\Pr\{A\} = \Pr\{\vec{\tau} \in A\}$, $A \in \mathcal{B}^n$ define the *distribution law* of $\vec{\tau}$ (n -dimensional distribution function). The function

$$F(t_1, \dots, t_n) = \Pr\{\tau_1 \leq t_1, \dots, \tau_n \leq t_n\}, \quad (\text{A6.51})$$

where

$$\{\tau_1 \leq t_1, \dots, \tau_n \leq t_n\} \equiv \{(\tau_1 \leq t_1) \cap \dots \cap (\tau_n \leq t_n)\},$$

is the distribution function of the *random vector* $\vec{\tau}$, known as *joint distribution function* of τ_1, \dots, τ_n . $F(t_1, \dots, t_n)$ is:

- monotonically nondecreasing in each variable,
- zero (in the limit) if at least one variable goes to $-\infty$,
- one (in the limit) if all variables go to ∞ ,
- continuous from the right in each variable,
- such that the probabilities $\Pr\{a_1 < \tau_1 \leq b_1, \dots, a_n < \tau_n \leq b_n\}$, calculated for arbitrary $a_1, \dots, a_n, b_1, \dots, b_n$ with $a_i < b_i$, are not negative (see e.g. [A6.7]).

It can be shown that every component τ_i of $\vec{\tau} = (\tau_1, \dots, \tau_n)$ is a random variable with distribution function, *marginal distribution function*,

$$F_i(t_i) = \Pr\{\tau_i \leq t_i\} = F(\infty, \dots, \infty, t_i, \infty, \dots, \infty), \quad F_i(-\infty) = 0, F_i(\infty) = 1. \quad (\text{A6.52})$$

Similarly as for events (Eq.(A6.9)), the random variables τ_1, \dots, τ_n of $\vec{\tau}$ are *totally* (mutually, statistically, stochastically) *independent* (*independent* in this book, p.419) if and only if, for any $1 < k \leq n$ and k -tuple $(t_1, \dots, t_k) \in \mathcal{R}^k$, $F(t_1, \dots, t_k) = \prod_{i=1}^k F_i(t_i)$ holds, see e.g. [A6.7]. In particular,

$$F(t_1, \dots, t_n) = \prod_{i=1}^n F_i(t_i) \quad (\text{A6.53})$$

must be satisfied for arbitrary t_1, \dots, t_n . Equation(A6.53) is equivalent to

$$\Pr\left\{\bigcap_{i=1}^n (\tau_i \in B_i)\right\} = \prod_{i=1}^n \Pr\{\tau_i \in B_i\}$$

for every $B_i \in \mathcal{B}^n$.

The random vector $\vec{\tau} = (\tau_1, \dots, \tau_n)$ is *absolutely continuous* if a function $f(x_1, \dots, x_n) \geq 0$ exists such that for any n and n -tuple t_1, \dots, t_n

$$F(t_1, \dots, t_n) = \int_{-\infty}^{t_1} \dots \int_{-\infty}^{t_n} f(x_1, \dots, x_n) dx_1 \dots dx_n. \quad (\text{A6.54})$$

$f(x_1, \dots, x_n)$ is the *density* of $\vec{\tau}$, known also as *joint density* of τ_1, \dots, τ_n , and satisfies the condition

$$\int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} f(x_1, \dots, x_n) dx_1 \dots dx_n = 1.$$

For any subset $A \in \mathcal{B}^n$, it follows that

$$\Pr\{(\tau_1, \dots, \tau_n) \in A\} = \int_A \dots \int f(t_1, \dots, t_n) dt_1 \dots dt_n. \quad (\text{A6.55})$$

The density of τ_i (*marginal density*) can be obtained from $f(t_1, \dots, t_n)$ as

$$f_i(t_i) = \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} f(t_1, \dots, t_n) dt_1 \dots dt_{i-1} dt_{i+1} \dots dt_n. \quad (\text{A6.56})$$

If the random variables τ_1, \dots, τ_n of $\vec{\tau}$ are *independent* (totally, mutually, statistically, stochastically independent) and have densities $f_1(x), \dots, f_n(x)$, the random vector $\vec{\tau}$ has *density*

$$f(t_1, \dots, t_n) = \prod_{i=1}^n f_i(t_i). \quad (\text{A6.57})$$

For a two dimensional continuous random vector $\vec{\tau} = (\tau_1, \tau_2)$, the function

$$f_2(t_2 | t_1) = \frac{f(t_1, t_2)}{f_1(t_1)} \tag{A6.58}$$

is the *conditional density* of τ_2 under the condition $\tau_1 = t_1$, with $f_1(t_1) > 0$. Similarly, $f_1(t_1 | t_2) = f(t_1, t_2) / f_2(t_2)$ is the conditional density for τ_1 given $\tau_2 = t_2$, with $f_2(t_2) > 0$. For the marginal density of τ_2 it follows that

$$f_2(t_2) = \int_{-\infty}^{\infty} f(t_1, t_2) dt_1 = \int_{-\infty}^{\infty} f_1(t_1) f_2(t_2 | t_1) dt_1. \tag{A6.59}$$

Therefore, for any $A \in \mathcal{B}^2$

$$\Pr\{\tau_2 \in A\} = \int_A f_2(t_2) dt_2 = \int_A \left(\int_{-\infty}^{\infty} f_1(t_1) f_2(t_2 | t_1) dt_1 \right) dt_2, \tag{A6.60}$$

and in particular

$$F_2(t) = \Pr\{\tau_2 \leq t\} = \int_{-\infty}^t f_2(t_2) dt_2 = \int_{-\infty}^t \left(\int_{-\infty}^{\infty} f_1(t_1) f_2(t_2 | t_1) dt_1 \right) dt_2. \tag{A6.61}$$

Equations (A6.58) & (A6.59) lead to the *Bayes theorem* for continuous random variables

$$f_2(t_2 | t_1) = (f_2(t_2) f_1(t_1 | t_2)) / \int_{-\infty}^{\infty} f_2(t_2) f_1(t_1 | t_2) dt_2,$$

used in Bayesian statistics.

Two dimensional distribution function, known as *bivariate distributions*, have been proposed for some reliability models, see e. g. [2.34 (1975)].

A6.8 Numerical Parameters of Random Vectors

Let $\vec{\tau} = (\tau_1, \dots, \tau_n)$ be a random vector, and u a continuous real-valued function in \mathcal{R}^n . The *expected value* or *mean* of the random variable $u(\vec{\tau})$ is

$$E[u(\vec{\tau})] = \sum_{i_1=1}^{k_1} \dots \sum_{i_n=1}^{k_n} u(t_{1,i_1}, \dots, t_{n,i_n}) p(i_1, \dots, i_n) \tag{A6.62}$$

for the discrete case and

$$E[u(\vec{\tau})] = \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} u(t_1, \dots, t_n) f(t_1, \dots, t_n) dt_1 \dots dt_n \tag{A6.63}$$

for the continuous case, assuming that series and integral converge absolutely.

As an example for $n=2$, the *conditional expected value* (mean) of τ_2 given $\tau_1 = t_1$ follows in the continuous case from Eqs. (A6.36) and (A6.58), as

$$E[\tau_2 | \tau_1 = t_1] = \int_{-\infty}^{\infty} t_2 f(t_2 | t_1) dt_2. \quad (\text{A6.64})$$

Thus the *unconditional expected value* (mean) of τ_2 can be obtained from

$$E[\tau_2] = \int_{-\infty}^{\infty} E[\tau_2 | \tau_1 = t_1] f_1(t_1) dt_1. \quad (\text{A6.65})$$

Equation (A6.65) is known as the formula of *total expectation* and is useful in practical applications.

A6.8.1 Covariance Matrix, Correlation Coefficient

Assuming for $\vec{\tau} = (\tau_1, \dots, \tau_n)$ that $\text{Var}[\tau_i] < \infty$, $i=1, \dots, n$, an important rough characterization of a random vector is the *covariance matrix* $|a_{ij}|$, where (Eq. (A6.68))

$$\begin{aligned} a_{ij} &= \text{Cov}[\tau_i, \tau_j] = E[(\tau_i - E[\tau_i])(\tau_j - E[\tau_j])] \\ &= E[\tau_i \tau_j] - E[\tau_i] E[\tau_j]. \end{aligned} \quad (\text{A6.66})$$

The diagonal elements of the covariance matrix are the *variances* of components τ_i , $i=1, \dots, n$. Elements outside the diagonal give a measure of the degree of dependency between components (obviously $a_{ij} = a_{ji}$). For τ_i *independent* of τ_j , $a_{ij} = a_{ji} = 0$ holds.

For a two dimensional random vector $\vec{\tau} = (\tau_1, \tau_2)$, the quantity

$$\rho(\tau_1, \tau_2) = \frac{\text{Cov}[\tau_1, \tau_2]}{\sigma_1 \cdot \sigma_2} \quad (\text{A6.67})$$

is the *correlation coefficient* of the random variables τ_1 and τ_2 , provided

$$\sigma_i = \sqrt{\text{Var}[\tau_i]} < \infty, \quad i=1, 2.$$

The main properties of the correlation coefficient are:

1. $|\rho| \leq 1$,
2. if τ_1 and τ_2 are *independent*, then $\rho = 0$,
3. $\rho = \pm 1$ if and only if τ_1 and τ_2 are linearly dependent.

The contrary in Point 2 is not necessarily true.

A6.8.2 Further Properties of Expected Value and Variance

Let τ_1, \dots, τ_n be *arbitrary* random variables (components of a random vector $\vec{\tau}$) and C_1, \dots, C_n constants. Using Eq. (A6.63) with $u(t_1, t_2) = t_1 + t_2$, Eq. (A6.56), and Eq. (A6.40) for $n=2$, and similarly as for Eq. (A6.14) for $n>2$, it follows that

$$E[C_1 \tau_1 + \dots + C_n \tau_n] = C_1 E[\tau_1] + \dots + C_n E[\tau_n], \quad -\infty < C_i < \infty. \quad (\text{A6.68})$$

If τ_1 and τ_2 are *independent*, Eqs. (A6.63) and (A6.57) & Eq. (A6.45) yield

$$E[\tau_1 \tau_2] = E[\tau_1] E[\tau_2] \quad \& \quad \text{Var}[\tau_1 \tau_2] = E[\tau_1^2] E[\tau_2^2] - E^2[\tau_1] E^2[\tau_2]. \quad (\text{A6.69})$$

For *independent* random variables τ_1, \dots, τ_n , using Eq. (A6.42) in the form $\text{Var}[\tau_1 + \dots + \tau_n] = E[(\tau_1 + \dots + \tau_n - E[\tau_1] - \dots - E[\tau_n])^2] = E[(\tau_1 - E[\tau_1] + \dots + \tau_n - E[\tau_n])^2]$ and Eqs. (A6.45), (A6.68) & (A6.69), it follows that

$$\text{Var}[\tau_1 + \dots + \tau_n] = \text{Var}[\tau_1] + \dots + \text{Var}[\tau_n]. \quad (\text{A6.70})$$

For *arbitrary* random variables τ_1, \dots, τ_n , Eq. (A6.66) and the same procedure used for Eq. (A6.70) yield

$$\text{Var}[\tau_1 + \dots + \tau_n] = \sum_{j=1}^n \text{Var}[\tau_j] + 2 \sum_{i < j} \text{Cov}[\tau_i, \tau_j], \quad (\text{A6.71})$$

$\text{Cov}[\tau_i, \tau_j]$ summing over $n(n-1)/2$ terms.

A6.9 Distribution of the Sum of Independent Positive Random Variables and of τ_{\min} , τ_{\max}

Let τ_1 and τ_2 be *independent* non-negative arithmetic random variables with $a_i = \Pr\{\tau_1 = i\}$, $b_i = \Pr\{\tau_2 = i\}$, $i = 0, 1, \dots$. Obviously, $\tau_1 + \tau_2$ is also arithmetic, and therefore (theorem of total probability (Eq. (A6.17)) and Eq. (A6.7))

$$\begin{aligned} c_k &= \Pr\{\tau_1 + \tau_2 = k\} = \Pr\left\{ \bigcup_{i=0}^k \{\tau_1 = i \cap \tau_2 = k - i\} \right\} \\ &= \sum_{i=0}^k \Pr\{\tau_1 = i\} \Pr\{\tau_2 = k - i\} = \sum_{i=0}^k a_i b_{k-i}. \end{aligned} \quad (\text{A6.72})$$

The sequence c_0, c_1, \dots is the *convolution* of the sequences a_0, a_1, \dots and b_0, b_1, \dots .

Now, let τ_1 and τ_2 be two *independent* positive continuous random variables with distribution functions $F_1(t)$, $F_2(t)$ and densities $f_1(t)$, $f_2(t)$, respectively ($F_1(0) = F_2(0) = 0$). Using Eq. (A6.55), it can be shown (Example A6.11 and Fig. A6.4) that for the distribution of $\eta = \tau_1 + \tau_2$

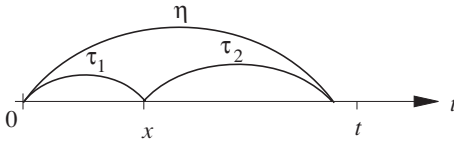


Figure A6.4 Visual aid to compute the distribution of $\eta = \tau_1 + \tau_2$ ($\tau_1, \tau_2 > 0$)

$$F_\eta(t) = \Pr\{\eta \leq t\} = \int_0^t f_1(x) F_2(t-x) dx, \quad t > 0, F_\eta(t) = 0 \text{ for } t \leq 0, \quad (\text{A6.73})$$

holds, and

$$f_\eta(t) = \int_0^t f_1(x) f_2(t-x) dx, \quad t > 0, f_\eta(t) = 0 \text{ for } t \leq 0. \quad (\text{A6.74})$$

The extension to two independent continuous random variables τ_1 and τ_2 defined over $(-\infty, \infty)$ leads to

$$F_\eta(t) = \int_{-\infty}^{\infty} f_1(x) F_2(t-x) dx \quad \text{and} \quad f_\eta(t) = \int_{-\infty}^{\infty} f_1(x) f_2(t-x) dx.$$

The right-hand side of Eq. (A6.74) represents the *convolution* of the densities $f_1(t)$ and $f_2(t)$, and will be denoted by

$$\int_0^t f_1(x) f_2(t-x) dx = f_1(t) * f_2(t). \quad (\text{A6.75})$$

The *Laplace transform* (Appendix A9.7) of $f_\eta(t)$ is thus the product of the Laplace transforms of $f_1(t)$ and $f_2(t)$

$$\tilde{f}_\eta(s) = \tilde{f}_1(s) \tilde{f}_2(s). \quad (\text{A6.76})$$

Example A6.11

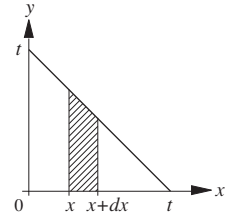
Prove Eq. (A6.74).

Solution

Let τ_1 and τ_2 be two independent positive and continuous random variables with distribution functions $F_1(t)$, $F_2(t)$ and densities $f_1(t)$, $f_2(t)$, respectively ($F_1(0) = F_2(0) = 0$). From Eq. (A6.55) with $f(x, y) = f_1(x) f_2(y)$ it follows that (see also the graph)

$$\begin{aligned}
 F_{\eta}(t) &= \Pr\{\eta = \tau_1 + \tau_2 \leq t\} = \iint_{x+y \leq t} f_1(x) f_2(y) dx dy \\
 &= \int_0^t \left(\int_0^{t-x} f_2(y) dy \right) f_1(x) dx = \int_0^t F_2(t-x) f_1(x) dx
 \end{aligned}$$

which proves Eq. (A6.73). Eq. (A6.74) follows with $F_2(0) = 0$.



Example A6.12

Two machines are used to increase the reliability of a system. The first is switched on at time $t = 0$, and the second at the time of failure of the first one, *standby redundancy*. The failure-free times of the machines, denoted by τ_1 and τ_2 are independent exponentially distributed with parameter λ (Eq. A6.81)). What is the reliability function of the system?

Solution

From $R_S(t) = \Pr\{\tau_1 + \tau_2 > t\} = 1 - \Pr\{\tau_1 + \tau_2 \leq t\}$ and Eq. (A6.73) it follows that

$$R_S(t) = 1 - \int_0^t \lambda e^{-\lambda x} (1 - e^{-\lambda(t-x)}) dx = e^{-\lambda t} + \lambda t e^{-\lambda t}.$$

$R_S(t)$ gives the probability for no failures ($e^{-\lambda t}$) or exactly one failure ($\lambda t e^{-\lambda t}$) in $(0, t]$.

Sums of positive random variables occur in reliability theory when investigating repairable systems (e.g. Example 6.12). For $n \geq 2$, the density $f_{\eta}(t)$ of $\eta = \tau_1 + \dots + \tau_n$ for *independent* positive continuous random variables τ_1, \dots, τ_n follows as

$$f_{\eta}(t) = f_1(t) * \dots * f_n(t). \tag{A6.77}$$

Other important distribution functions for reliability analyses are the *minimum* τ_{\min} and the *maximum* τ_{\max} of a finite set of positive, independent random variables τ_1, \dots, τ_n ; for instance, as failure-free time of a series or a 1-out-of- n parallel system, respectively. If τ_1, \dots, τ_n are *positive, independent* random variables with distribution functions $F_i(t) = \Pr\{\tau_i \leq t\}$, $F_i(0) = 0$, $i = 1, \dots, n$, then

$$\Pr\{\tau_{\min} > t\} = \Pr\{\tau_1 > t \cap \dots \cap \tau_n > t\} = \prod_{i=1}^n (1 - F_i(t)), \tag{A6.78}$$

and

$$\Pr\{\tau_{\max} \leq t\} = \Pr\{\tau_1 \leq t \cap \dots \cap \tau_n \leq t\} = \prod_{i=1}^n F_i(t). \tag{A6.79}$$

It can be noted that the failure rate related to τ_{\min} is given by (Eq. (A6.26))

$$\lambda_S(t) = \lambda_1(t) + \dots + \lambda_n(t), \tag{A6.80}$$

where $\lambda_i(t)$ is the failure rate related to $F_i(t)$. The distribution of τ_{\min} leads for $F_1(t) = \dots = F_n(t)$ and $n \rightarrow \infty$ to the *Weibull* distribution [A6.8]. For the mixture of distribution functions one refers to the considerations given by Eqs. (A6.34) & (2.15).

A6.10 Distribution Functions used in Reliability Analysis

This section introduces the most important distribution functions used in reliability analysis, see Table A6.1 for a summary. The variable t , used here for convenience, applies in particular to *nonrepairable* items (failure-free times $\tau > 0$). For *interarrival times* (e. g. when considering repairable systems), x has to be used instead of t .

A6.10.1 Exponential Distribution

A continuous positive random variable τ has an *exponential distribution* if

$$F(t) = 1 - e^{-\lambda t}, \quad t > 0; \lambda > 0 \quad (F(t) = 0 \text{ for } t \leq 0). \quad (\text{A6.81})$$

The *density* is given by

$$f(t) = \lambda e^{-\lambda t}, \quad t > 0; \lambda > 0 \quad (f(t) = 0 \text{ for } t \leq 0).^{+)} \quad (\text{A6.82})$$

and the *failure rate* (Eq. (A6.25)) by

$$\lambda(t) = \lambda, \quad t > 0 \quad (\lambda(t) = 0 \text{ for } t \leq 0).^{+)} \quad (\text{A6.83})$$

The *mean & variance* can be obtained from Eqs. (A6.37), (A6.82) & (A6.41), (A6.45), (A6.82) as

$$E[\tau] = 1/\lambda \quad (\text{A6.84})$$

and

$$\text{Var}[\tau] = 1/\lambda^2. \quad (\text{A6.85})$$

The *Laplace transform* of $f(t)$ is, according to Table A9.7,

$$\tilde{f}(s) = \frac{\lambda}{s + \lambda}. \quad (\text{A6.86})$$

Example A6.13

The failure-free time τ of an assembly is exponentially distributed with $\lambda = 10^{-5} \text{ h}^{-1}$. What is the probability of τ being (i) over 2,000 h, (ii) over 20,000 h, (iii) over 100,000 h, (iv) between 20,000 h and 100,000 h?

Solution

From Eqs. (A6.81), (A6.24) and (A6.19) one obtains

- (i) $\Pr\{\tau > 2,000 \text{ h}\} = e^{-0.02} \approx 0.98,$
- (ii) $\Pr\{\tau > 20,000 \text{ h}\} = e^{-0.2} \approx 0.819,$
- (iii) $\Pr\{\tau > 100,000 \text{ h}\} = \Pr\{\tau > 1/\lambda = E[\tau]\} = e^{-1} \approx 0.368,$
- (iv) $\Pr\{20,000 \text{ h} < \tau \leq 100,000 \text{ h}\} = e^{-0.2} - e^{-1} \approx 0.451.$

^{+) Note that only $F(t)$ has been defined right continuous (Eq. (A6.19)).}

For an exponential distribution, the failure rate is *constant* (time independent) and equal to λ . This important property is a *characteristic* of the exponential distribution and does not appear with any other continuous distribution. It greatly simplifies calculation because of the following properties:

1. *Memoryless property*: Assuming that the failure-free time is exponentially distributed and knowing that the item is functioning at the present time, its behavior in the future *will not depend on how long it has already been operating*. In particular, the probability that it will fail in the next time interval δt is *constant* and equal to $\lambda \delta t$. This is a consequence of Eq. (A6.29)

$$\Pr\{\tau > t + x_0 \mid \tau > x_0\} = e^{-\lambda t}. \quad (\text{A6.87})$$

2. *Constant failure rate at system level*: If a system *without redundancy* consists of elements E_1, \dots, E_n and the failure-free times τ_1, \dots, τ_n of these elements are *independent* and *exponentially distributed* with parameters $\lambda_1, \dots, \lambda_n$ then, according to Eqs. (A6.78) and (A6.25), the system failure rate is also *constant* (time independent) and equal to the sum of the failure rates of its elements

$$R_S(t) = e^{-\lambda_1 t} \dots e^{-\lambda_n t} = e^{-\lambda_S t}, \quad \text{with } \lambda_S = \lambda_1 + \dots + \lambda_n. \quad (\text{A6.88})$$

However, it must be noted that the expression $\lambda_S = \sum \lambda_i$ is a characteristic of the *series model* with independent elements, and also remains valid for the time dependent failure rates $\lambda_i = \lambda_i(t)$, see Eqs. (A6.80) and (2.18).

A6.10.2 Weibull Distribution

The *Weibull distribution* can be considered as a generalization of the exponential distribution. A continuous positive random variable τ has a Weibull distribution if

$$F(t) = 1 - e^{-(\lambda t)^\beta}, \quad t > 0; \lambda, \beta > 0 \quad (F(t) = 0 \text{ for } t \leq 0). \quad (\text{A6.89})$$

The *density* is given by

$$f(t) = \lambda \beta (\lambda t)^{\beta-1} e^{-(\lambda t)^\beta}, \quad t > 0; \lambda, \beta > 0 \quad (f(t) = 0 \text{ for } t \leq 0). \quad (\text{A6.90})$$

and the *failure rate* (Eq. (A6.25)) by

$$\lambda(t) = \beta \lambda (\lambda t)^{\beta-1}, \quad t > 0; \lambda, \beta > 0 \quad (\lambda(t) = 0 \text{ for } t \leq 0). \quad (\text{A6.91})$$

λ is the *scale parameter* ($F(t)$ depends on λt only) and β the *shape parameter*. $\beta = 1$ yields the exponential distribution. For $\beta > 1$, the failure rate $\lambda(t)$ is *strictly increasing*⁺, with $\lambda(+0) = 0$ & $\lambda(\infty) = \infty$. For $\beta < 1$, $\lambda(t)$ is *strictly decreasing*, with $\lambda(+0) = \infty$ and $\lambda(\infty) = 0$. The *mean* & *variance* are given by (Eqs. (A6.37), (A6.90), (A6.94) & (A6.45), (A6.41), (A6.90), (A6.94), and Appendix A9.6 for $\Gamma(z+1) = z\Gamma(z)$)

⁺ $\lambda(t)$ is increasing if $\lambda(t_2) \geq \lambda(t_1)$ for $t_2 > t_1$ and strictly increasing if $\lambda(t_2) > \lambda(t_1)$ for $t_2 > t_1$.

$$E[\tau] = \frac{\Gamma(1 + 1/\beta)}{\lambda} = \frac{\Gamma(1/\beta)}{\lambda\beta} \tag{A6.92}$$

and

$$\text{Var}[\tau] = \frac{\Gamma(1 + 2/\beta) - \Gamma^2(1 + 1/\beta)}{\lambda^2}, \tag{A6.93}$$

where

$$\Gamma(z) = \int_0^\infty x^{z-1} e^{-x} dx, \quad z > 0, \tag{A6.94}$$

is the *complete Gamma function* (Appendix A9.6). The coefficient of variation $\kappa = \sqrt{\text{Var}[\tau]} / E[\tau]$ is plotted in Fig. 4.5. For a given $E[\tau]$, the density of the Weibull distribution becomes peaked with increasing β . An analytical expression for the *Laplace transform* of the Weibull distribution function does not exist.

For a system without redundancy (*series model*) whose elements have independent failure-free times τ_1, \dots, τ_n distributed according to Eq. (A6.89), the reliability function is given by

$$R_S(t) = (e^{-(\lambda t)^\beta})^n = e^{-(\lambda' t)^\beta}, \quad t > 0, R_S(0) = 1, \tag{A6.95}$$

with $\lambda' = \lambda \sqrt[\beta]{n}$. Thus, the failure-free time of the system has a Weibull distribution with parameters λ' and β .

The Weibull distribution with $\beta > 1$ often occurs in practical applications as a distribution of the failure-free time of components which are subject to *wear-out* and / or *fatigue* (lamps, relays, mechanical components, etc.). It was introduced by W. Weibull in 1951, related to investigations on fatigue in metals [A6.20]. B.W. Gnedenko showed that a Weibull distribution occurs as one of the *extreme value distributions* for the smallest of $n \rightarrow \infty$ independent random variables with the same distribution function (Weibull-Gnedenko distribution [A6.7, A6.8]).

The Weibull distribution is often given with the parameter $\alpha = \lambda^\beta$ instead of λ or also with *three parameters* (see Example A6.14 and pp. 531-532 for a discussion)

$$F(t) = 1 - e^{-(\lambda(t-\psi))^\beta}, \quad t > \psi, \lambda, \beta > 0 \quad (F(t) = 0 \text{ for } t \leq \psi). \tag{A6.96}$$

Example A6.14

Shows that for a three parameter Weibull distribution, also the time scale parameter ψ can be determined (graphically) on a Weibull probability chart, e.g. for an *empirical evaluation of data*.

Solution

In the coordinates system $\log_{10}(t)$ and $\log_{10}\log_{10}(1/(1-F(t)))$ the 2 parameter Weibull distribution function (Eq. (A6.89)) appears as a straight line, allowing a graphical determination of λ, β (see Eq. (A8.16) & Fig. A8.2). The three parameter Weibull distribution (Eq. (A6.96)) leads to a concave curve. In this case, for two arbitrary points t_1 and $t_2 > t_1$ it holds, for the mean point on $\log_{10}\log_{10}(1/(1-F(t)))$, defining t_m , that $\log_{10}\log_{10}(1/(1-F(t_1))) + \log_{10}\log_{10}(1/(1-F(t_2))) = 2\log_{10}\log_{10}(1/(1-F(t_m)))$, considering Fig. A8.2 & $a+(b-a)/2 = (a+b)/2$. From this, Eq. (A8.16) with $F(t)$ per Eq. (A6.96) leads to $(t_2-\psi)(t_1-\psi) = (t_m-\psi)^2$ and $\psi = (t_1 t_2 - t_m^2) / (t_1 + t_2 - 2t_m)$.

A6.10.3 Gamma Distribution, Erlangian Distribution, and χ^2 -Distribution

A continuous positive random variable τ has a *Gamma distribution* if

$$F(t) = \Pr\{\tau \leq t\} = \frac{1}{\Gamma(\beta)} \int_0^{\lambda t} x^{\beta-1} e^{-x} dx = \frac{\gamma(\beta, \lambda t)}{\Gamma(\beta)}, \quad t > 0; \lambda, \beta > 0 \quad (F(t) = 0 \text{ for } t \leq 0). \tag{A6.97}$$

Γ is the *complete Gamma function* (Eq. (A6.94)). γ is the *incomplete Gamma function* (Appendix A9.6). The *density* of the Gamma distribution is given by

$$f(t) = \lambda \frac{(\lambda t)^{\beta-1}}{\Gamma(\beta)} e^{-\lambda t}, \quad t > 0; \lambda, \beta > 0 \quad (f(t) = 0 \text{ for } t \leq 0). \tag{A6.98}$$

and the *failure rate* is calculated from $\lambda(t) = f(t) / (1 - F(t))$. For $\beta = n = 1, 2, \dots$ (Eq. (6.102)) it holds that $\lambda(t) = \lambda^n t^{n-1} / [(n-1)! \sum_{i=0}^{n-1} (\lambda t)^i / i!]$. $\lambda(t)$ is constant (time independent) for $\beta = 1$, *strictly decreasing* for $\beta < 1$ and *strictly increasing* for $\beta > 1$. However, $\lambda(t)$ always converges to λ for $t \rightarrow \infty$, see Tab.A6.1. A Gamma distribution with $\beta < 1$ mixed with a three-parameter Weibull distribution (Eq. (A6.34, case 1)) can be used as an approximation to a distribution function yielding a *bathtub curve* (Fig. 1.2) as failure rate.

The *mean & variance* are given by (Eqs. (A6.37), (A6.98), (A6.94) & (A6.45), (A6.41), (A6.98), and Appendix A9.6 for $\Gamma(z+1) = z\Gamma(z)$)

$$E[\tau] = \beta / \lambda \tag{A6.99}$$

and

$$\text{Var}[\tau] = \beta / \lambda^2. \tag{A6.100}$$

The *Laplace transform* (Table A9.7) of the Gamma distribution density is

$$\tilde{f}(s) = \lambda^\beta / (s + \lambda)^\beta. \tag{A6.101}$$

From Eqs. (A6.101) and (A6.76), it follows that the sum of two *independent* Gamma-distributed random variables with parameters λ, β_1 and λ, β_2 has a Gamma distribution with parameters $\lambda, \beta_1 + \beta_2$ (Example A6.15).

Example A6.15

Let the random variables τ_1 and τ_2 be independent and distributed according to a Gamma distribution with the parameters λ and β . Determine the density of the sum $\eta = \tau_1 + \tau_2$.

Solution

According Eq. (A6.98), τ_1 and τ_2 have density $f(t) = \lambda (\lambda t)^{\beta-1} e^{-\lambda t} / \Gamma(\beta)$. The Laplace transform of $f(t)$ is $\tilde{f}(s) = \lambda^\beta / (s + \lambda)^\beta$ (Table A9.7). From Eq. (A6.76), the Laplace transform of the density of $\eta = \tau_1 + \tau_2$ follows as $\tilde{f}_\eta(s) = \lambda^{2\beta} / (s + \lambda)^{2\beta}$. The random variable $\eta = \tau_1 + \tau_2$ thus has a Gamma distribution with parameters λ and 2β (generalization to $n > 2$ is immediate).

Supplementary result: More generally, if τ_1 and τ_2 are Gamma distributed with parameters λ, β_1 and λ, β_2 , $\tau_1 + \tau_2$ is Gamma distributed with parameters $\lambda, \beta_1 + \beta_2$.

For $\beta = n = 2, 3, \dots$, the Gamma distribution given by Eq. (A6.97) leads to an *Erlangian distribution* with parameters λ and n (exponential distribution for $\beta = 1$). Considering Eqs. (A6.86), (A6.77) and (A6.101) with $\beta = n$, it follows that:

If τ is Erlang distributed with parameters λ and n , then τ can be considered as the sum of n independent, exponentially distributed random variables with parameter λ ($\tau = \tau_1 + \dots + \tau_n$ with $\Pr\{\tau_i \leq t\} = 1 - e^{-\lambda t}$, $i = 1, \dots, n$).

The *Erlangian distribution* can be obtained by partial integration of the right-hand side of Eq. (A6.97), with $\beta = n$, yielding (see also Eq. (A7.39))

$$F(t) = \Pr\{\tau_1 + \dots + \tau_n \leq t\} = \int_0^{\lambda t} \frac{x^{n-1}}{\Gamma(n)} e^{-x} dx = 1 - \sum_{i=0}^{n-1} \frac{(\lambda t)^i}{i!} e^{-\lambda t}, \quad t > 0 \quad (F(t) = 0 \text{ for } t \leq 0), n \geq 1. \tag{A6.102}$$

From Example A6.15, if failure-free times are Erlangian distributed with parameters (n, λ) , the sum of k failure-free times is Erlangian distributed with parameters (kn, λ) .

For $\lambda = 1/2$ and $\beta = \nu/2$, $\nu = 1, 2, \dots$, the Gamma distribution given by Eq. (A6.97) is a *chi-square distribution* (χ^2 -distribution) with ν degrees of freedom. The corresponding random variable is denoted χ^2_ν . The chi-square distribution with ν degrees of freedom is thus given by (see also Appendix A9.2)

$$F(t) = \Pr\{\chi^2_\nu \leq t\} = \frac{1}{\Gamma(\frac{\nu}{2})} \int_0^{t/2} x^{\frac{\nu}{2}-1} e^{-x} dx = \frac{1}{2^{\nu/2} \Gamma(\frac{\nu}{2})} \int_0^t y^{\frac{\nu}{2}-1} e^{-y/2} dy, \quad t > 0 \quad (F(t) = 0 \text{ for } t \leq 0), \nu = 1, 2, 3, \dots \tag{A6.103}$$

From Eqs. (A6.97), (A6.102), and (A6.103) it follows that

$$2\lambda(\tau_1 + \dots + \tau_n) \tag{A6.104}$$

has a χ^2 distribution with $\nu = 2n$ degrees of freedom. If ξ_1, \dots, ξ_n are *independent, normally distributed* random variables with mean m and variance σ^2 , then

$$\sum_{i=1}^n \left(\frac{\xi_i - m}{\sigma}\right)^2 = \frac{1}{\sigma^2} \sum_{i=1}^n (\xi_i - m)^2$$

is χ^2 distributed with n degrees of freedom (see Problem A6.7 in Appendix A11 for $n = 1$ and Example 6.15 for $n > 1$, as well as Appendix A9.4 for further relations). Above considerations show the importance of the χ^2 -distribution. The χ^2 -distribution is also used to compute the *Poisson distribution* (Eq. (A6.130), Eq. (A6.102) with $n = \nu/2$ & $\lambda = 1/2$, or Eq. (A6.126) with $k = \nu/2 - 1$ & $m = t/2$, $\nu = 2, 4, \dots$).

Example A6.16

Prove the affirmation to Eq. (A6.104).

Solution

From Eq. (A6.102) it follows that $\Pr\{\tau_1 + \tau_2 + \dots + \tau_n \leq t\} = \Pr\{2\lambda(\tau_1 + \tau_2 + \dots + \tau_n) \leq 2\lambda t\} = \int_0^{2\lambda t} x^{n-1} e^{-x} dx / \Gamma(n)$. $2\lambda t = y$ yields $\Pr\{2\lambda(\tau_1 + \tau_2 + \dots + \tau_n) \leq y\} = \int_0^{y/2} x^{n-1} e^{-x} dx / \Gamma(n)$. Finally, setting $x = z/2$ it follow that $\Pr\{2\lambda(\tau_1 + \tau_2 + \dots + \tau_n) \leq y\} = \int_0^y z^{n-1} e^{-z/2} dz / 2^n \Gamma(n)$.

A6.10.4 Normal Distribution

A widely used distribution function, in theory and practice, is the *normal distribution*, or Gaussian distribution. The random variable τ has a normal distribution if

$$F(t) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^t e^{-\frac{(y-m)^2}{2\sigma^2}} dy = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{t-m}{\sigma}} e^{-x^2/2} dx, \quad -\infty < t, m < \infty, \sigma > 0. \quad (\text{A6.105})$$

The *density* of the normal distribution is given by

$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(t-m)^2}{2\sigma^2}}, \quad -\infty < t, m < \infty, \sigma > 0. \quad (\text{A6.106})$$

The failure rate is calculated from $\lambda(t) = f(t)/(1 - F(t))$. The *mean* and *variance* are (Eqs. (A6.37), (A6.106) with $x = (t - m)/\sigma\sqrt{2}$, (A6.44), the Poisson integral (p.566), and $\int_{-\infty}^{\infty} xe^{-x^2} dx = 0$ & $\int_{-\infty}^{\infty} e^{-ax^2} dx = \sqrt{\pi/a} \Rightarrow d/da (-\int_{-\infty}^{\infty} e^{-ax^2} dx) = \int_{-\infty}^{\infty} x^2 e^{-ax^2} dx = \sqrt{\pi/a}/2a, a = 1$)

$$E[\tau] = m \quad (\text{A6.107})$$

and

$$\text{Var}[\tau] = \sigma^2, \quad (\text{A6.108})$$

The density of the normal distribution is *symmetric* with respect to the line $x = m$. Its width depends upon the variance. The area under the density curve is equal to (Table A9.1, [A9.1])

- 0.6827 for the interval $m \pm \sigma$,
- 0.95450 for the interval $m \pm 2\sigma$,
- 0.99730 for the interval $m \pm 3\sigma$,
- 0.9999367 for the interval $m \pm 4\sigma$,
- 0.9999932 for the interval $m \pm 4.5\sigma$,
- 0.99999943 for the interval $m \pm 5\sigma$.

A normal distributed random variable takes values in $(-\infty, +\infty)$. However, for $m > 3\sigma$ it is often possible to consider it as a positive random variable in practical applications. $m \pm 6\sigma$ is often used as a sharp limit for controlling the process quality (*6- σ approach*). By *accepting a shift of the mean of $\pm 1.5\sigma$ in the manufacturing process, the 6- σ approach yields* (for a normal distribution) *3.4 ppm right and 3.4 ppm left the sharp limit ($m \pm 4.5\sigma$).*

If τ has a normal distribution with parameters m and σ^2 , $(\tau - m)/\sigma$ is normally distributed with parameters 0 and 1, which is the *standard normal distribution* $\Phi(t)$

$$\Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^t e^{-x^2/2} dx. \quad (\text{A6.109})$$

If τ_1 and τ_2 are independent, normally distributed random variables with parameters m_1, σ_1^2 , and m_2, σ_2^2 , $\eta = \tau_1 + \tau_2$ is normally distributed with parameters $m_1 + m_2, \sigma_1^2 + \sigma_2^2$ (Example A6.17). This rule can be generalized to the sum of n independent normally distributed random variables, and extended to dependent normally distributed random variables (Example A6.17, supplementary results).

Example A6.17

Let the random variables τ_1 and τ_2 be independent and normally distributed with means m_1 and m_2 and variances σ_1^2 and σ_2^2 . Give the density of the sum $\eta = \tau_1 + \tau_2$.

Solution

According to Eq. (A6.106) and the results of Appendix A6.9, the density of $\eta = \tau_1 + \tau_2$ follows as

$$f_{\eta}(t) = \frac{1}{2\pi\sigma_1\sigma_2} \int_{-\infty}^{\infty} e^{-\left(\frac{(x-m_1)^2}{2\sigma_1^2} + \frac{(t-x-m_2)^2}{2\sigma_2^2}\right)} dx.$$

Setting $u = x - m_1$ & $v = t - m_1 - m_2$, considering

$$\frac{u^2}{\sigma_1^2} + \frac{(v-u)^2}{\sigma_2^2} = \left[\frac{u\sqrt{\sigma_1^2 + \sigma_2^2}}{\sigma_1\sigma_2} - \frac{v\sigma_1}{\sigma_2\sqrt{\sigma_1^2 + \sigma_2^2}} \right]^2 + \frac{v^2}{\sigma_1^2 + \sigma_2^2},$$

and setting finally $u\sqrt{\sigma_1^2 + \sigma_2^2} / \sigma_1\sigma_2 - v\sigma_1 / \sigma_2\sqrt{\sigma_1^2 + \sigma_2^2} = y$, the result

$$f_{\eta}(t) = \frac{1}{\sqrt{2\pi}\sqrt{\sigma_1^2 + \sigma_2^2}} e^{-\frac{(t-m_1-m_2)^2}{2(\sigma_1^2 + \sigma_2^2)}}$$

is obtained. Thus the sum of two independent normally distributed random variables is also normally distributed with mean $m_1 + m_2$ and variance $\sigma_1^2 + \sigma_2^2$.

Supplementary results: If τ_1 and τ_2 are not independent, the distribution function of $\tau_1 + \tau_2$ is still a normal distribution with $m = m_1 + m_2$, but with variance $\sigma^2 = \sigma_1^2 + \sigma_2^2 + 2\rho\sigma_1\sigma_2$ [A6.7] ($\rho =$ correlation coefficient, Eq. (A6.67)).

The normal distribution often occurs in practical applications, also because the distribution function of the sum of a large number of independent random variables converges under weak conditions to a normal distribution (central limit theorem, Eq. (A6.148)).

A6.10.5 Lognormal Distribution

A continuous positive random variable τ has a *lognormal distribution* if its logarithm is normally distributed (Example A6.18). For the lognormal distribution,

$$F(t) = \frac{1}{\sigma\sqrt{2\pi}} \int_0^t \frac{1}{y} e^{-\frac{(\ln(\lambda y))^2}{2\sigma^2}} dy = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{\ln(\lambda t)}{\sigma}} e^{-x^2/2} dx = \Phi(\ln(\lambda t / \sigma)),$$

$t > 0; \lambda, \sigma > 0$ ($F(0) = 0$ for $t \leq 0$). (A 6.110)

The *density* is given by

$$f(t) = \frac{1}{t \sigma \sqrt{2\pi}} e^{-(\ln \lambda t)^2 / 2 \sigma^2}, \quad t > 0; \lambda, \sigma > 0 \quad (f(t)=0 \text{ for } t \leq 0). \quad (\text{A6.111})$$

The *failure rate* is calculated from $\lambda(t)=f(t)/(1-F(t))$, see Table A6.1 for an example. The *mean* and *variance* of τ are (Eqs.(A6.37), (A6.111), (A6.41), (A6.45), Poisson integral (p. 566), Problem A6.8 in Appendix A11)

$$E[\tau] = e^{\sigma^2/2} / \lambda \quad (\text{A6.112})$$

and

$$\text{Var}[\tau] = (e^{2\sigma^2} - e^{\sigma^2}) / \lambda^2, \quad (\text{A6.113})$$

respectively. The density of the lognormal distribution is practically zero for some t at the origin, increases rapidly to a maximum and decreases quickly (Fig. 4.2). It applies often as model for *repair times* (Section 4.1) or for lifetimes in *accelerated reliability tests* (Section 7.4) and appears when a large number of independent random variables are combined in a *multiplicative way* (*additive* for $\eta = \ln \tau$, i.e. for normal distribution). Notation with m or $a = -\ln(\lambda)$ is often used. It must also be noted that $\sigma^2 = \text{Var}[\ln \tau]$ and $m = \ln(1/\lambda) = E[\ln \tau]$ (Example A6.18).

Example A6.18

Show that the logarithm of a lognormally distributed random variable is normally distributed.

Solution

For

$$f_{\tau}(t) = \frac{1}{t \sigma \sqrt{2\pi}} e^{-(\ln t + \ln \lambda)^2 / 2 \sigma^2}$$

and $\eta = \ln \tau$, Equation (A6.31) yields ($u(t) = \ln t$ and $u^{-1}(t) = e^t$)

$$f_{\eta}(t) = \frac{1}{e^t \sigma \sqrt{2\pi}} e^{-(t + \ln \lambda)^2 / 2 \sigma^2} e^t = \frac{1}{\sigma \sqrt{2\pi}} e^{-(t + \ln \lambda)^2 / 2 \sigma^2} = \frac{1}{\sigma \sqrt{2\pi}} e^{-(t-m)^2 / 2 \sigma^2},$$

with $m = \ln(1/\lambda)$; $\eta = \ln \tau$ is thus normally distributed with mean $m = \ln(1/\lambda)$ and variance σ^2 .

Supplementary results (considering Eqs.(A6.31),(A6.106)&(A6.111),(A6.90)&(A6.82),(A6.114):

- (i) $u(t) = e^t$; $u^{-1}(t) = \ln(t)$: Normal distribution \rightarrow Lognormal distribution,
- (ii) $u(t) = \ln(t)$; $u^{-1}(t) = e^t$: Lognormal distribution \rightarrow Normal distribution,
- (iii) $u(t) = \lambda^{\beta-1} t^{\beta}$; $u^{-1}(t) = \sqrt[\beta]{t/\lambda^{\beta-1}}$: Weibull distribution \rightarrow Exponential distribution,
- (iv) $u(t) = \sqrt[\beta]{t/\lambda^{\beta-1}}$; $u^{-1}(t) = \lambda^{\beta-1} t^{\beta}$: Exponential distribution \rightarrow Weibull distribution,
- (v) $u(t) = F_{\eta}^{-1}(t)$; $u^{-1}(t) = F_{\eta}(t)$: Uniform distribution on (0, 1) \rightarrow $F_{\eta}(t)$,
- (vi) $u(t) = F_{\tau}(t)$; $u^{-1}(t) = F_{\tau}^{-1}(t)$: $F_{\tau}(t)$ \rightarrow Uniform distribution on (0, 1),
- (vii) $u(t) = C \cdot t$; $u^{-1}(t) = t/C$: $F_{\eta}(t) = F_{\tau}(t/C)$ and $f_{\eta}(t) = f_{\tau}(t/C)/C$,
 $u(t) = t - C$; $u^{-1}(t) = t + C$: $F_{\eta}(t) = F_{\tau}(t+C)$ and $f_{\eta}(t) = f_{\tau}(t+C)$

In *Monte Carlo simulations*, more elaborated algorithms than $F_{\eta}^{-1}(t)$ are often used.

A6.10.6 Uniform Distribution

A continuous random variable τ is *uniformly distributed* in the interval (a, b) if it has the distribution function

$$F(t) = \Pr\{\tau \leq t\} = \begin{cases} 0 & \text{if } t \leq a \\ \frac{t-a}{b-a} & \text{if } a < t < b \\ 1 & \text{if } t \geq b. \end{cases} \quad (\text{A6.114})$$

The *density* is then given by

$$f(t) = \frac{1}{b-a} \quad \text{for } a < t < b.$$

The uniform distribution is a particular case of the geometric probability introduced by Eq. (A6.3), for \mathcal{R}^1 instead of \mathcal{R}^2 .

Considering the property mentioned by case (V) of Example A6.18, the *uniform distribution* in the interval $[0,1)$ plays an important role in simulation problems (discrete random variables $\zeta_0, \zeta_1, \dots, \zeta_{2^n-1}$ with $p_i = 1/2^n$, for digital computers).

A6.10.7 Binomial Distribution

Consider a trial in which the only outcomes are either a given event A or its complement \bar{A} . These outcomes can be represented by a random variable of the form

$$\delta = \begin{cases} 1 & \text{if } A \text{ occurs} \\ 0 & \text{otherwise.} \end{cases} \quad (\text{A6.115})$$

δ is called a *Bernoulli variable*. If

$$\Pr\{\delta = 1\} = p \quad \text{and} \quad \Pr\{\delta = 0\} = 1 - p, \quad 0 < p < 1, \quad (\text{A6.116})$$

then

$$E[\delta] = 1 \cdot p + 0 \cdot (1 - p) = p, \quad (\text{A6.117})$$

and (Eq. (A6.45))

$$\text{Var}[\delta] = E[\delta^2] - E^2[\delta] = p - p^2 = p(1 - p). \quad (\text{A6.118})$$

An infinite sequence of independent Bernoulli variables

$$\delta_1, \delta_2, \dots$$

with the same probability $\Pr\{\delta_i = 1\} = p$, $i \geq 1$, is called a *Bernoulli model* or a *sequence of Bernoulli trials*. The sequence $\delta_1, \delta_2, \dots$ describes, for example, the model of the repeated sampling of a component from a lot of size N , with K defective components ($p = K/N$) such that the component is returned to the lot after testing (sample with replacement). The random variable

$$\zeta = \delta_1 + \dots + \delta_n \quad (\text{A6.119})$$

is the number of ones occurring in n Bernoulli trials. The distribution of ζ is given by

$$p_k = \Pr\{\zeta = k\} = \binom{n}{k} p^k (1-p)^{n-k}, \quad k=0, \dots, n, \quad 0 < p < 1. \quad (\text{A6.120})$$

Equation (A6.120) is the *binomial distribution*, see example A6.19 for an application. ζ is obviously a non-negative, *arithmetic random variable* taking on values in $\{0, 1, \dots, n\}$ with probabilities p_k . To prove Eq. (A6.120), consider that

$$p^k (1-p)^{n-k} = \Pr\{\delta_1 = 1 \cap \dots \cap \delta_k = 1 \cap \delta_{k+1} = 0 \cap \dots \cap \delta_n = 0\}$$

is the probability of the event A occurring in the first k trials and not occurring in the $n-k$ following trials; furthermore in n trials there are

$$\frac{n(n-1) \dots (n-k+1)}{k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

different possibilities of occurrence of k ones and $n-k$ zeros ($k!$ considers that the k ones can not be distinguished, yielding $k!$ identical possibilities). The addition theorem (Eq. (A6.11)) then leads to Eq. (A6.120), see example A6.19 for an application.

For the random variable ζ defined by Eq. (A6.119) it follows that (Example A6.20)

$$\Pr\{\zeta \leq k\} = \sum_{i=0}^k \binom{n}{i} p^i (1-p)^{n-i}, \quad k=0, \dots, n, \quad 0 < p < 1, \quad (\text{A6.121})$$

$$E[\zeta] = np, \quad (\text{A6.122})$$

$$\text{Var}[\zeta] = np(1-p). \quad (\text{A6.123})$$

Example A6.19

A populated printed circuit board (PCB) contains 30 ICs. These are taken from a shipment in which the probability of each IC being defective is constant and equal to 1%. What are the probabilities that the PCB contains (i) no defective ICs, (ii) exactly one defective IC, and (iii) more than one defective IC?

Solution

From Eq. (A6.120) with $p = 0.01$,

- (i) $p_0 = 0.99^{30} \approx 0.74$,
- (ii) $p_1 = 30 \cdot 0.01 \cdot 0.99^{29} \approx 0.224$,
- (iii) $p_2 + \dots + p_{30} = 1 - p_0 - p_1 \approx 0.036$.

Knowing p_i and assuming $C_i = \text{cost}$ for i repairs (because of i defective ICs) it is easy to calculate the *mean* C of the total cost caused by the defective ICs ($C = p_1 C_1 + \dots + p_{30} C_{30}$) and thus to develop a *test strategy* based on cost considerations (Section 8.4).

Example A6.20

Give mean and variance of a binomially distributed random variable with parameters n and p .

Solution

Considering the independence of $\delta_1, \dots, \delta_n$, the definition of ζ (Eq. (A6.119)), and from Eqs. (A6.117), (A6.118), (A6.68), and (A6.70) it follows that

$$E[\zeta] = E[\delta_1] + \dots + E[\delta_n] = np$$

and

$$\text{Var}[\zeta] = \text{Var}[\delta_1] + \dots + \text{Var}[\delta_n] = np(1-p).$$

A further demonstration follows, as for Example A6.21, by considering that

$$\sum_{k=1}^n k \binom{n}{k} p^k (1-p)^{n-k} = np \sum_{k=1}^n \binom{n-1}{k-1} p^{k-1} (1-p)^{n-k} = np \sum_{i=0}^m \binom{m}{i} p^i (1-p)^{m-i} = np.$$

For large n , the binomial distribution converges to the normal distribution (Eq. (A6.149), convergence good for $\min(np, n(1-p)) \geq 5$). For large n and small values of p the *Poisson approximation* (Eq. (A6.129)) can be used. Exact calculations of Eq. (A6.120) can be based upon the relationship between the binomial and the *Beta* or the *Fisher distribution* (Appendix A9.4).

Generalization of Eq. (A6.120) for the case where one of the events A_1, \dots, A_m can occur with probability p_1, \dots, p_m at every trial, leads to the *multinomial distribution*

$$\begin{aligned} & \Pr\{ \text{in } n \text{ trials } A_1 \text{ occurs } k_1 \text{ times, } \dots, A_m \text{ occurs } k_m \text{ times} \} \\ &= \frac{n(n-1)\dots(n-(k_1+\dots+k_{m-1})+1)}{k_1! \dots k_{m-1}!} p_1^{k_1} \dots p_m^{k_m} = \frac{n!}{k_1! \dots k_m!} p_1^{k_1} \dots p_m^{k_m}, \end{aligned} \quad (\text{A6.124})$$

with $k_1 + \dots + k_m = n$ and $p_1 + \dots + p_m = 1$ (the demonstration is similar to that for $\binom{n}{k}$ with Eq. (A6.120)).

A6.10.8 Poisson Distribution

A non-negative, arithmetic random variable ζ has a *Poisson distribution* if

$$p_k = \Pr\{\zeta = k\} = \frac{m^k}{k!} e^{-m}, \quad k = 0, 1, \dots, \quad m > 0, \quad (\text{A6.125})$$

and thus

$$\Pr\{\zeta \leq k\} = \sum_{i=0}^k \frac{m^i}{i!} e^{-m}, \quad k = 0, 1, \dots, \quad m > 0. \quad (\text{A6.126})$$

The *mean* and the *variance* of ζ are (Example A6.21)

$$E[\zeta] = m \tag{A6.127}$$

and

$$\text{Var}[\zeta] = m. \tag{A6.128}$$

The Poisson distribution often occurs in connection with *exponentially distributed failure-free times*. In fact, Eq. (A6.125) with $m = \lambda t$ gives the probability of k failures in the time interval $(0, t]$, given λ and t (Eq. (A7.41)).

The Poisson distribution is also used as an *approximation* of the binomial distribution for $n \rightarrow \infty$ and $p \rightarrow 0$ such that $np = m < \infty$. To prove this convergence, called the *Poisson approximation*, set $m = np$; Eq. (A6.120) then yields

$$\begin{aligned} p_k &= \frac{n!}{k!(n-k)!} \left(\frac{m}{n}\right)^k \left(1 - \frac{m}{n}\right)^{n-k} = \frac{n(n-1)\dots(n-k+1)}{n^k} \cdot \frac{m^k}{k!} \left(1 - \frac{m}{n}\right)^{n-k} \\ &= 1 \left(1 - \frac{1}{n}\right) \dots \left(1 - \frac{k-1}{n}\right) \cdot \frac{m^k}{k!} \left(1 - \frac{m}{n}\right)^{n-k}, \end{aligned}$$

from which (for $k < \infty$, $m = np < \infty$) it follows that (considering $\lim_{n \rightarrow \infty} (1 - m/n)^n = e^{-m}$)

$$\lim_{n \rightarrow \infty} p_k = \binom{n}{k} p^k (1-p)^{n-k} = \frac{m^k}{k!} e^{-m}, \quad m = np. \tag{A6.129}$$

Using partial integration one can show that

$$\sum_{i=0}^k \frac{m^i}{i!} e^{-m} = 1 - \frac{1}{k!} \int_0^m y^k e^{-y} dy = 1 - \frac{1}{k! 2^{k+1}} \int_0^{2m} x^k e^{-x/2} dx. \tag{A6.130}$$

The right-hand side of Eq. (A6.130) is a *chi-square distribution* (Eq. (A6.103)) with $v/2 = k+1$ and $t = 2m$. A table of the chi-square distribution can thus be used for a numerical evaluation of the Poisson distribution (Table A9.2).

Example A6.21

Give mean and variance of a Poisson-distributed random variable.

Solution

From Eqs. (A6.35) and (A6.125),

$$E[\zeta] = \sum_{k=0}^{\infty} k \frac{m^k}{k!} e^{-m} = \sum_{k=1}^{\infty} m \frac{m^{k-1}}{(k-1)!} e^{-m} = m \sum_{i=0}^{\infty} \frac{m^i}{i!} e^{-m} = m.$$

Similarly, from Eqs. (A6.45), (A6.41), (A6.125), and considering $k^2 = k(k-1) + k$,

$$\begin{aligned} \text{Var}[\zeta] &= \sum_{k=0}^{\infty} k^2 \frac{m^k}{k!} e^{-m} - m^2 = \sum_{k=0}^{\infty} [k(k-1) + k] \frac{m^k}{k!} e^{-m} - m^2 \\ &= \sum_{k=2}^{\infty} m^2 \frac{m^{k-2}}{(k-2)!} e^{-m} + m - m^2 = m^2 \sum_{i=0}^{\infty} \frac{m^i}{i!} e^{-m} + m - m^2 = m. \end{aligned}$$

A6.10.9 Geometric Distribution

Let $\delta_1, \delta_2, \dots$ be a sequence of independent *Bernoulli variables* resulting from Bernoulli trials. The positive arithmetic random variable ζ defining the number of trials to the *first occurrence* of the event A has a *geometric distribution*

$$p_k = \Pr\{\zeta = k\} = p(1-p)^{k-1}, \quad k=1,2,\dots, \quad 0 < p < 1. \quad (\text{A6.131})$$

Equation (A6.131) follows from the definition of Bernoulli variables δ_i (Eq. (A6.115))

$$p_k = \Pr\{\zeta = k\} = \Pr\{\delta_1 = 0 \cap \dots \cap \delta_{k-1} = 0 \cap \delta_k = 1\} = (1-p)^{k-1} p.$$

The geometric distribution is the only discrete distribution which exhibits the *memoryless property*, as does the exponential distribution for the continuous case. In fact, from $\Pr\{\zeta > k\} = \Pr\{\delta_1 = 0 \cap \dots \cap \delta_k = 0\} = (1-p)^k$ and, for any k and $j > 0$, it follows that

$$\Pr\{\zeta > k+j \mid \zeta > k\} = \frac{(1-p)^{k+j}}{(1-p)^k} = (1-p)^j = \Pr\{\zeta > j\}.$$

The *failure rate* (p. 428) is time independent and given by (considering Eqs. (A6.131) & (A6.133))

$$\lambda(k) = \Pr\{\zeta = k \mid \zeta > k-1\} = \frac{p(1-p)^{k-1}}{(1-p)^{k-1}} = p, \quad k=1,2,\dots, \quad 0 < p < 1. \quad (\text{A6.132})$$

For the distribution function of the random variable ζ defined by Eq. (A6.131) one obtains

$$\Pr\{\zeta \leq k\} = \sum_{i=1}^k p_i = 1 - \Pr\{\zeta > k\} = 1 - (1-p)^k. \quad (\text{A6.133})$$

Mean and variance are (considering $\sum_{n=1}^{\infty} nx^n = x/(1-x)^2$, $\sum_{n=1}^{\infty} n^2x^n = x(1+x)/(1-x)^3$, $x < 1$)

$$E[\zeta] = \frac{1}{p} \quad (\text{A6.134})$$

and

$$\text{Var}[\zeta] = \frac{1-p}{p^2}. \quad (\text{A6.135})$$

If Bernoulli trials are carried out at regular intervals Δt , then Eq. (A6.133) provides the distribution function of the *number of time units Δt between successive occurrences of the event A under consideration*; for example, breakdown of a capacitor, interference pulse in a digital network, etc.

Often the geometric distribution is considered with $p_k = p(1-p)^k$, $k=0,1,\dots$, in this case $E[\zeta] = (1-p)/p$ and $\text{Var}[\zeta] = (1-p)/p^2$.

A6.10.10 Hypergeometric Distribution

The *hypergeometric distribution* describes the model of a *random sample without replacement*. For example, if it is known that there are exactly K defective components in a lot of size N , then the probability of finding k defective components in a random sample of size n is given by (Eq. (A6.2), [A6.6 (Vol 1)])

$$p_k = \Pr\{\zeta = k\} = \frac{\binom{K}{k} \binom{N-K}{n-k}}{\binom{N}{n}}, \quad k = 0, 1, \dots, \min(K, n). \quad (\text{A6.136})$$

Equation (A6.136) defines the *hypergeometric distribution*. Since for fixed n and k ($0 \leq k \leq n$)

$$\lim_{N \rightarrow \infty} \Pr\{\zeta = k\} = \binom{n}{k} p^k (1-p)^{n-k}, \quad \text{with } p = \frac{K}{N},$$

the hypergeometric distribution can, for large N , be approximated by the binomial distribution with $p = K/N$. For the random variable ζ defined by Eq. (A6.136) it holds that

$$\Pr\{\zeta \leq k\} = \sum_{i=0}^k \frac{\binom{K}{i} \binom{N-K}{n-i}}{\binom{N}{n}}, \quad k = 0, 1, \dots, \min(K, n), \quad (\text{A6.137})$$

$$E[\zeta] = n \frac{K}{N}, \quad (\text{A6.138})$$

and (see e. g. [A9.1])

$$\text{Var}[\zeta] = \frac{K n (N-K)(N-n)}{N^2 (N-1)}. \quad (\text{A6.139})$$

A6.11 Limit Theorems

Limit theorems are of great importance in practical applications because they can be used to find *approximate expressions* with the help of known (tabulated) distributions. Two important cases will be discussed in this section, the *laws of large numbers* and the *central limit theorem*. The laws of large numbers provide additional justification for the construction of probability theory on the basis of

relative frequencies. The central limit theorem shows that the normal distribution can be used as an approximation in many practical situations.

A6.11.1 Laws of Large Numbers

Two notions used with the laws of large numbers are *convergence in probability* and *convergence with probability one*. Let ξ_1, ξ_2, \dots , and ξ be random variables on a probability space $[\Omega, \mathcal{F}, \Pr]$. ξ_n converge in probability to ξ if for arbitrary $\varepsilon > 0$

$$\lim_{n \rightarrow \infty} \Pr\{ |\xi_n - \xi| > \varepsilon \} = 0, \quad \varepsilon > 0, \tag{A6.140}$$

holds. ξ_n converge to ξ with probability one if

$$\Pr\{ \lim_{n \rightarrow \infty} \xi_n = \xi \} = 1. \tag{A6.141}$$

The convergence with probability one is also called *convergence almost sure* (a.s.). An equivalent condition for Eq. (A6.141) is

$$\lim_{n \rightarrow \infty} \Pr\{ \sup_{k \geq n} |\xi_k - \xi| > \varepsilon \} = 0, \quad \varepsilon > 0. \tag{A6.142}$$

This clarifies the difference between Eq. (A6.140) and the stronger condition given by Eq. (A6.141).

Let us now consider an infinite sequence of *Bernoulli trials* (Eqs. (A6.115), (A6.119), and (A6.120)), with parameter $p = \Pr\{A\}$, and let S_n (ζ in Eq. (A6.119)) be the number of occurrences of the event A in n trials

$$S_n = \delta_1 + \dots + \delta_n. \tag{A6.143}$$

The quantity S_n/n is the *relative frequency* of the occurrence of A in n Bernoulli trials. The *weak law of large numbers* states that for every $\varepsilon > 0$,

$$\lim_{n \rightarrow \infty} \Pr\{ \left| \frac{S_n}{n} - p \right| > \varepsilon \} = 0, \quad \varepsilon > 0. \tag{A6.144}$$

Equation (A6.144) is a consequence of Chebyshev's inequality (Eq. (A6.49) with $E[S_n/n] = p$ & $\text{Var}[S_n/n] = p(1-p)/n$ per Eqs. (A6.122), (A6.123), (A6.40), (A6.46)). Similarly, for a sequence of *independent identically distributed* random variables τ_1, \dots, τ_n , with mean $E[\tau_i] = a$ & variance $n \text{Var}[\tau_i] = n\sigma^2$ ($i=1, \dots, n$),

$$\lim_{n \rightarrow \infty} \Pr\{ \left| \left(\frac{1}{n} \sum_{i=1}^n \tau_i \right) - a \right| > \varepsilon \} = 0, \quad \varepsilon > 0. \tag{A6.145}$$

According to Eq. (A6.144), the sequence S_n/n converges in probability to $p = \Pr\{A\}$. Moreover, according to the Eq. (A6.145), the *arithmetic mean* $(t_1 + \dots + t_n)/n$ of n independent observations of the random variable τ (with a

finite variance) *converges in probability* to $E[\tau]$. Therefore, $\hat{p} = S_n/n$ and $\hat{a} = (t_1 + \dots + t_n)/n$ are *consistent estimates* of $p = \Pr\{A\}$ and $a = E[\tau]$, respectively (Eq. (A8.19)). Equation (A6.145) is also a consequence of Chebyshev's inequality (Eq. (A6.49)).

A firmer statement than the weak law of large numbers is given by the *strong law of large numbers*,

$$\Pr\left\{\lim_{n \rightarrow \infty} \frac{S_n}{n} = p\right\} = 1. \quad (\text{A6.146})$$

According to Eq. (A6.146), the relative frequency S_n/n *converges with probability one* (a. s.) to $p = \Pr\{A\}$. Similarly, for a sequence of independent identically distributed random variables τ_1, \dots, τ_n , with mean $E[\tau_i] = a < \infty$ and variance $n \text{Var}[\tau_i] = n\sigma^2$ ($i = 1, 2, \dots$),

$$\Pr\left\{\lim_{n \rightarrow \infty} \left(\frac{1}{n} \sum_{i=1}^n \tau_i\right) = a\right\} = 1. \quad (\text{A6.147})$$

The proof of the strong law of large numbers (A6.146) and (A6.147) is more laborious than that of the weak law of large numbers, see e. g. [A6.6 (vol. II), A6.7].

A6.11.2 Central Limit Theorem

Let τ_1, τ_2, \dots be *independent identically distributed* random variables with mean $E[\tau_i] = a < \infty$ and variance $n \text{Var}[\tau_i] = n\sigma^2$, $i = 1, 2, \dots$; for every $t < \infty$ it holds that (see e. g. [A6.6 (vol. II), A6.7, A8.8])

$$\lim_{n \rightarrow \infty} \Pr\left\{\frac{(\sum_{i=1}^n \tau_i) - na}{\sigma \sqrt{n}} \leq t\right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^t e^{-x^2/2} dx. \quad (\text{A6.148})$$

Equation (A6.148) is the *central limit theorem*. It says that for large values of n , the distribution function of the sum $\tau_1 + \dots + \tau_n$ of *independent identically distributed* random variables τ_i can be approximated by the normal distribution with mean $E[\tau_1 + \dots + \tau_n] = nE[\tau_i] = na$ and variance $\text{Var}[\tau_1 + \dots + \tau_n] = n \text{Var}[\tau_i] = n\sigma^2$. The central limit theorem is of great theoretical and practical importance, in probability theory and mathematical statistics. It includes the *integral Laplace theorem* (De Moivre-Laplace) for the case where $\tau_i = \delta_i$ are Bernoulli variables,

$$\lim_{n \rightarrow \infty} \Pr\left\{\frac{(\sum_{i=1}^n \delta_i) - np}{\sqrt{np(1-p)}} \leq t\right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^t e^{-x^2/2} dx. \quad (\text{A6.149})$$

$\sum \delta_i$ is the random variable ζ in Eq. (A6.119) for the binomial distribution, i.e., it is the total number of occurrences of the event considered in n Bernoulli trials.

From Eq. (A6.149) it follows that for $n \rightarrow \infty$ and $\delta = t \sqrt{np(1-p)} / n$

$$\Pr\left\{\left(\frac{\sum_{i=1}^n \delta_i}{n} - p\right) \leq \delta\right\} \rightarrow \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{n\delta}{\sqrt{np(1-p)}}} e^{-x^2/2} dx, \quad n \rightarrow \infty,$$

or, for arbitrary $\varepsilon > 0$,

$$\Pr\left\{\left|\frac{\sum_{i=1}^n \delta_i}{n} - p\right| \leq \varepsilon\right\} \rightarrow \frac{2}{\sqrt{2\pi}} \int_0^{\frac{n\varepsilon}{\sqrt{np(1-p)}}} e^{-x^2/2} dx, \quad n \rightarrow \infty, \varepsilon > 0. \quad (\text{A6.150})$$

Setting the right-hand side of Eq. (A6.150) equal to γ allows determination of the number of trials n for given γ, p , and ε which are necessary to fulfill the inequality $|\delta_1 + \dots + \delta_n / n - p| \leq \varepsilon$ with a probability γ . This result is important for reliability investigations using *Monte Carlo simulations*, see Eq. (A6.152).

The central limit theorem can be generalized under weak conditions to the sum of independent random variables with different distribution functions (see e.g. [A6.6 (Vol. II), A6.7, A8.8]), the meaning of these conditions being that each individual standardized random variable $(\tau_i - E[\tau_i]) / \sqrt{\text{Var}[\tau_i]}$ provides a small contribution to the standardized sum (Lindeberg conditions).

Examples 6.22-6.24 give some applications of the central limit theorem.

Example A6.22

The series production of a given assembly requires 5,000 ICs of a particular type. 0.5% of these ICs are defective. How many ICs must be bought in order to be able to produce the series with a probability of $\gamma = 0.99$?

Solution

Setting $p = \Pr\{\text{IC defective}\} = 0.005$, the minimum value of n satisfying

$$\Pr\left\{n - \sum_{i=1}^n \delta_i \geq 5,000\right\} = \Pr\left\{\sum_{i=1}^n \delta_i \leq n - 5,000\right\} \geq 0.99 = \gamma$$

must be found. Rearranging Eq. (A6.149) and considering $t = t_\gamma$ leads to

$$\lim_{n \rightarrow \infty} \Pr\left\{\sum_{i=1}^n \delta_i \leq t_\gamma \sqrt{np(1-p)} + np\right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t_\gamma} e^{-x^2/2} dx = \gamma,$$

where t_γ denotes the γ quantile of the standard normal distribution $\Phi(t)$ given by Eq. (A6.109) or Table A9.1. For $\gamma = 0.99$ one obtains from Table A9.1 $t_\gamma = t_{0.99} = 2.33$. With $p = 0.005$, it follows that

$$\sum_{i=1}^n \delta_i = n - 5,000 \leq 2.33 \sqrt{n \cdot 0.005 \cdot 0.995} + 0.005 \cdot n.$$

Thus, $n = 5,036$ ICs must be bought ($5,025 = 5,000 + 5,000 \cdot 0.005$ ICs would lead to $\gamma \approx 0.5$).

Example A6.23

Electronic components are delivered with a defective probability $p = 0.1\%$. (i) How large is the probability of having exactly 8 defective components in a (homogeneous) lot of size $n = 5,000$? (ii) In which interval $[k_1, k_2]$ around the mean value $np = 5$ will the number of defective components lie in a lot of size $n = 5,000$ with a probability γ as near as possible to 0.95 ?

Solution

(i) The use of the Poisson approximation (Eq. (A6.129)) leads to

$$p_8 \approx \frac{5^8}{8!} e^{-5} \approx 0.06528,$$

the exact value (obtained with Eq. (A6.120)) being 0.06527. For comparison, the following are the values of p_k obtained with the Poisson approximation (Eq. (A6.129)) in the first row and the exact values from Eq. (A6.120) in the second row

$k =$	0	1	2	3	4	5	6	7	8	9
$p_k \approx$	0.00674	0.03369	0.08422	0.14037	0.17547	0.17547	0.14622	0.10444	0.06528	0.03627
$p_k \approx$	0.00672	0.03364	0.08401	0.14036	0.17552	0.17570	0.14630	0.10448	0.06527	0.03624

(ii) From the above table one recognizes that the interval $[k_1, k_2] = [1, 9]$ is centered on the mean value $np=5$ and satisfy the condition " γ as near as possible to 0.95 " ($\gamma = p_1 + p_2 + \dots + p_9 \approx 0.96$). A good approximation for k_1 and k_2 can also be obtained using Eq. (A6.151) to determine $\varepsilon = (k_2 - k_1) / 2n$ by given p, n , and $t_{(1+\gamma)/2}$

$$\varepsilon = \frac{k_2 - k_1}{2n} = \frac{\sqrt{np(1-p)}}{n} t_{(1+\gamma)/2}, \tag{A6.151}$$

where $t_{(1+\gamma)/2}$ is the $(1 + \gamma) / 2$ quantile of the standard normal distribution (Eq. (A6.109), Appendix A9.1). Equation (A6.151) is a consequence of Eq. (A6.150), considering that

$$\frac{2}{\sqrt{2\pi}} \int_0^A e^{-x^2/2} dx = \gamma \quad \text{yields} \quad \frac{1}{\sqrt{2\pi}} \int_{-\infty}^A e^{-x^2/2} dx = 0.5 + \gamma/2 = \frac{1+\gamma}{2},$$

(i. e. $A = t_{(1+\gamma)/2}$), and

$$\begin{aligned} \Pr \left\{ \left| \frac{\sum_{i=1}^n \delta_i}{n} - p \right| \leq \varepsilon \right\} &= \Pr \left\{ \left| \sum_{i=1}^n \delta_i - np \right| \leq n\varepsilon \right\} = \Pr \left\{ -n\varepsilon \leq \sum_{i=1}^n \delta_i - np \leq n\varepsilon \right\} \\ &= \Pr \left\{ np - n\varepsilon \leq \sum_{i=1}^n \delta_i \leq np + n\varepsilon \right\} = \Pr \left\{ k_1 \leq \sum_{i=1}^n \delta_i \leq k_2 \right\}, \end{aligned}$$

with $k_1 = n(p - \varepsilon)$ and $k_2 = n(p + \varepsilon)$; from which (Eq. (A6.150))

$$A = t_{(1+\gamma)/2} = n\varepsilon / \sqrt{np(1-p)} \quad \text{or} \quad \varepsilon = (k_2 - k_1) / 2n = t_{(1+\gamma)/2} \sqrt{np(1-p)} / n.$$

With $\gamma = 0.95$, $t_{(1+\gamma)/2} = t_{0.975} = 1.96$ (Table A9.1), $n = 5,000$, and $p = 0.001$ one obtains $n\varepsilon = 4.38$, yielding $k_1 = np - n\varepsilon = 0.62$ (≥ 0) and $k_2 = np + n\varepsilon = 9.38$ ($\leq n$). The same solution is also given by Eq. (A8.45)

$$k_{12} = np \pm b\sqrt{np(1-p)}, \quad \text{i. e.} \quad k_2 - k_1 = 2b\sqrt{np(1-p)} = 2n\varepsilon,$$

considering $b = t_{(1+\gamma)/2}$.

Example A6.24

As an example belonging to both probability theory and statistics, determine the number n of trials necessary to estimate an unknown probability p within a given interval $\pm \epsilon$ at a given probability γ (e.g. for a Monte Carlo simulation).

Solution

From Eq. (A6.150) it follows that for $n \rightarrow \infty$

$$\Pr\left\{ \left| \frac{\sum_{i=1}^n \delta_i}{n} - p \right| \leq \epsilon \right\} \approx \frac{2}{\sqrt{2\pi}} \int_0^{\frac{n\epsilon}{\sqrt{np(1-p)}}} e^{-x^2/2} dx = \gamma.$$

Therefore,

$$\frac{1}{\sqrt{2\pi}} \int_0^{\frac{n\epsilon}{\sqrt{np(1-p)}}} e^{-x^2/2} dx = \frac{\gamma}{2} \quad \text{yields} \quad \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{n\epsilon}{\sqrt{np(1-p)}}} e^{-x^2/2} dx = 0.5 + \frac{\gamma}{2} = \frac{1+\gamma}{2},$$

and thus $n\epsilon / \sqrt{np(1-p)} = t_{(1+\gamma)/2}$, from which

$$n = \left(\frac{t_{(1+\gamma)/2}}{\epsilon} \right)^2 p(1-p), \tag{A6.152}$$

where $t_{(1+\gamma)/2}$ is the $(1+\gamma)/2$ quantile of the standard normal distribution $\Phi(t)$ (Eq. (A6.109), Appendix A9.1). The number of trials n depend on the value of p and is a maximum (n_{\max}) for $p = 0.5$. The following table gives n_{\max} for different values of ϵ and γ

ϵ	0.05 ($2\epsilon = 0.1$)			0.025 ($2\epsilon = 0.05$)		
γ	0.8	0.9	0.95	0.8	0.9	0.95
$t_{(1+\gamma)/2}$	1.282	1.645	1.960	1.282	1.645	1.960
n_{\max}	164	271	384	657	1,082	1,537

Equation (A6.152) has been established by assuming that p is known. Thus, ϵ refers to the number of observations in n trials ($2\epsilon n = k_2 - k_1$ as per Eqs. (A6.151) and (A6.152) or Eq. (A8.45) with $b = t_{(1+\gamma)/2}$). However, the role of p and k/n can be reversed by assuming that the number k of realizations in n trials is known. In this case, for n large and p or $(1-p)$ not very small ($\min(np, n(1-p)) \geq 5$), ϵ refers to the width of the confidence interval for p ($2\epsilon = \hat{p}_u - \hat{p}_l$ as per Eq. (A8.43) with $k(1-k/n) \gg b^2/4$ and $n \gg b^2$). The two interpretations of ϵ ($\epsilon = (k_2 - k_1)/2n$ per Eq. (A6.151) or (A6.152) and $\epsilon = (\hat{p}_u - \hat{p}_l)/2$ per Eq. (A8.43)) are basically different (probability theory and statistics) and agree only because of $n \rightarrow \infty$ (see also pp. 530, 542, 543-544). For n small, or $p(1-p)$ very small, the binomial distribution has to be used (Eqs. (A6.121), (A8.37), (A8.38)).

A7 Basic Stochastic - Processes Theory

Stochastic processes are a powerful tool for investigating reliability and availability of repairable equipment and systems. A stochastic process can be considered as a family of time-dependent random variables or as a random function in time, and thus has a theoretical foundation based on *probability theory* (Appendix A6.7). The use of stochastic processes allows analysis of the influence of the failure-free and repair time distributions of elements, as well as of the system's structure, repair strategy, and logistic support, on the reliability and availability of a given system. Considering applications given in Chapter 6, this appendix mainly deals with *regenerative stochastic processes with a finite state space*, to which belong *renewal processes, Markov processes, semi-Markov processes, and semi-regenerative processes*, including reward and frequency/duration aspects. However, because of their importance in reliability investigations, some nonregenerative processes (in particular the nonhomogeneous Poisson process) are introduced in Appendix A7.8. This appendix is a compendium of the theory of stochastic processes, consistent from a mathematical point of view but still with reliability engineering applications in mind (demonstration of established theorems is referred, and for all other propositions or equations, sufficient details for complete demonstration are given). To simplify the notation, *mean* is used for *expected value*, and *independent* for *totally* (mutually, statistically, stochastically) *independent* (p. 419). Selected examples illustrate the practical aspects.

A7.1 Introduction

Stochastic processes are mathematical models for random phenomena evolving over time, such as the time behavior of a repairable system or the noise voltage of a diode. They are designated hereafter by Greek letters $\xi(t)$, $\zeta(t)$, $\eta(t)$, $\nu(t)$ etc.

To introduce the concept of stochastic process, consider the time behavior of a system subject to random influences and let T be the time interval of interest, e. g. $T = [0, \infty)$. The set of possible states of the system, i. e. the *state space*, is assumed to be a subset of the set of real numbers. The state of the system at a given time t_0 is thus a *random variable* $\xi(t_0)$. The random variables $\xi(t)$, $t \in T$, may be arbitrarily coupled together. However, for any $n = 1, 2, \dots$, and arbitrary values $t_1, \dots, t_n \in T$, the existence of the *n-dimensional distribution function* (Eq. (A6.51))

$$F(x_1, \dots, x_n, t_1, \dots, t_n) = \Pr\{\xi(t_1) \leq x_1, \dots, \xi(t_n) \leq x_n\}, \quad (\text{A7.1})$$

is assumed, where $\xi(t_1) \leq x_1, \dots, \xi(t_n) \leq x_n \equiv \xi(t_1) \leq x_1 \cap \dots \cap \xi(t_n) \leq x_n$ is used.

$\xi(t_1), \dots, \xi(t_n)$ are thus the components of a *random vector* $\vec{\xi}(t)$. It can be shown that the family of n -dimensional distribution functions (Eq. (A7.1)) satisfies the *consistency condition*

$$F(x_1, \dots, x_k, \infty, \dots, \infty, t_1, \dots, t_k, t_{k+1}, \dots, t_n) = F(x_1, \dots, x_k, t_1, \dots, t_k), \quad k < n$$

and the *symmetry condition*

$$F(x_{i_1}, \dots, x_{i_n}, t_{i_1}, \dots, t_{i_n}) = F(x_1, \dots, x_n, t_1, \dots, t_n),$$

$$i_i \in \{1, \dots, n\}, \quad i_j \neq i_i \text{ for } j \neq i.$$

Conversely, if a family of distribution functions $F(x_1, \dots, x_n, t_1, \dots, t_n)$ satisfying the above consistency and symmetry conditions is given, then according to a theorem of A.N. Kolmogorov [A6.10], a *distribution law* on a suitable event field \mathcal{B}^T of the space \mathcal{R}^T consisting of all real functions on T exists. This distribution law is the distribution of a *random function* $\xi(t)$, $t \in T$, usually referred to as a *stochastic process*. The time function resulting from a particular experiment is called a *sample path* or *realization* of the stochastic process. All sample paths are in \mathcal{R}^T , however the set of sample paths for a particular stochastic process can be significantly smaller than \mathcal{R}^T , e.g. consisting only of increasing step functions. In the case of discrete time, the notion of a *sequence of random variables* ξ_n , $n \in T$ is generally used. The concept of a stochastic process generalizes the concept of a random variable introduced in Appendix A6.5. If the random variables $\xi(t)$ are defined as measurable functions $\xi(t) = \xi(t, \omega)$, $t \in T$, on a given probability space $[\Omega, \mathcal{F}, \Pr]$ then

$$F(x_1, \dots, x_n, t_1, \dots, t_n) = \Pr\{\omega : \xi(t_1, \omega) \leq x_1, \dots, \xi(t_n, \omega) \leq x_n\},$$

and the consistency and symmetry conditions are fulfilled. ω represents the random influence. The function $\xi(t, \omega)$, $t \in T$, is for a given ω a *realization of the stochastic process*.

The Kolmogorov theorem assures the *existence* of a stochastic process. However, the determination of all n -dimensional distribution functions is practically impossible, in general. Sufficient for many applications are often some specific parameters of the stochastic process involved, such as state probabilities or stay (sojourn) times. The problem considered, and the model assumed, generally allow determination of

- the time domain T (continuous, discrete, finite, infinite)
- the structure of the state space (continuous, discrete)
- the dependency structure of the process under consideration (e.g. memoryless)
- invariance properties with respect to time shifts (time-homogeneous, stationary).

The simplest process in discrete time is a *sequence of independent random variables* ξ_1, ξ_2, \dots . Also easy to describe are *processes with independent increments*, for instance Poisson processes (Appendices A7.2.5 & A7.8.2), for which

$$\Pr\{\xi(t_0) \leq x_0, \xi(t_1) - \xi(t_0) \leq x_1, \dots, \xi(t_n) - \xi(t_{n-1}) \leq x_n\} = \Pr\{\xi(t_0) \leq x_0\} \prod_{i=1}^n \Pr\{\xi(t_i) - \xi(t_{i-1}) \leq x_i\} \quad (\text{A7.2})$$

holds for arbitrary $n = 1, 2, \dots$, x_1, \dots, x_n , and $t_0 < \dots < t_n \in T$.

For reliability investigations, processes with *continuous time parameter* $t \geq 0$ and *discrete state space* $\{Z_0, \dots, Z_m\}$ are important. Among these, following processes will be discussed in the following sections (see Table 6.1 for a comparison)

- renewal processes
- alternating renewal processes
- Markov processes
- semi-Markov processes
- semi-regenerative processes (processes with an embedded semi-Markov process)
- regenerative processes with just one regeneration state
- particular nonregenerative processes (e. g. nonhomogeneous Poisson processes).

Markov processes represent a straightforward generalization of sequences of independent random variables. They are processes *without aftereffect*. With this, *the evolution of the process after an arbitrary time point t only depends on t and on the state occupied at t , not on the evolution of the process before t* . For time-homogeneous Markov processes, the dependence on t also disappears (*memoryless property*). Markov processes are very simple *regenerative stochastic processes*. They are regenerative with respect to every state and, if time-homogeneous, also with respect to any time t . *Semi-Markov processes* have the Markov property at the time points of any *state change*; i. e., all states of a Semi-Markov process are regeneration states. In a *semi-regenerative process*, a subset $\{Z_0, \dots, Z_k\}$, $0 < k < m$, of the state space $\{Z_0, \dots, Z_m\}$ are regeneration states and constitute an *embedded semi-Markov process*. Quite generally,

at the occurrence of a regeneration state the process forgets its foregoing evolution and restarts anew with respect to the regeneration state considered; successive occurrence points of a regeneration state Z_i constitute thus a renewal process embedded in the original process (see Figs. A7.3, A7.11-A7.13 and pp. 478-79 & 514).

Nonregenerative processes occur in particular with reliability data analysis.

In order to describe the time behavior of systems which are in statistical equilibrium (*steady-state*), stationary and time-homogeneous processes are suitable. The process $\xi(t)$ is *stationary* (strictly stationary) if for arbitrary $n = 1, 2, \dots$, t_1, \dots, t_n , and time span a ($t_i, t_i + a \in T$, $i = 1, \dots, n$)

$$F(x_1, \dots, x_n, t_1 + a, \dots, t_n + a) = F(x_1, \dots, x_n, t_1, \dots, t_n). \quad (\text{A7.3})$$

For $n = 1$, Eq. (A7.3) shows that the distribution function of the random variable $\xi(t)$ is independent of t . Hence, $E[\xi(t)]$, $\text{Var}[\xi(t)]$, and all other moments are

independent of time. For $n = 2$, the distribution function of the two-dimensional random variable $(\xi(t), \xi(t+u))$ is only a function of u . From this it follows that the *correlation coefficient* between $\xi(t)$ and $\xi(t+u)$ is also only a function of u

$$\begin{aligned} \rho_{\xi\xi}(t, t+u) &= \frac{E[(\xi(t+u) - E[\xi(t+u)])(\xi(t) - E[\xi(t)])]}{\sqrt{\text{Var}[\xi(t+u)] \text{Var}[\xi(t)]}} \\ &= \frac{E[\xi(t)\xi(t+u)] - E^2[\xi(t)]}{\text{Var}[\xi(t)]} = \rho_{\xi\xi}(u). \end{aligned} \tag{A7.4}$$

Besides stationarity in the *strict sense*, stationarity is also defined in the wide sense. The process $\xi(t)$ is *stationary in the wide sense* if the mean $E[\xi(t)]$ the variance $\text{Var}[\xi(t)]$, and the correlation coefficient $\rho_{\xi\xi}(t, t+u)$ are finite and independent of t . Stationarity in the strict sense of a process having a finite variance implies stationarity in the wide sense. The contrary is true only in some particular cases, e.g. for the *normal process* (process for which all n -dimensional distribution functions (Eq. (A7.1) are n -dimensional normal distribution functions, see Example A6.17).

A process $\xi(t)$ is *time-homogeneous* if it has *stationary increments*, i.e., if for arbitrary $n = 1, 2, \dots$, values x_1, \dots, x_n , disjoint intervals (t_i, b_i) , and time span a $(t_i, t_i+a, b_i, b_i+a \in T, i = 1, \dots, n)$

$$\begin{aligned} \Pr\{\xi(t_1+a) - \xi(b_1+a) \leq x_1, \dots, \xi(t_n+a) - \xi(b_n+a) \leq x_n\} \\ = \Pr\{\xi(t_1) - \xi(b_1) \leq x_1, \dots, \xi(t_n) - \xi(b_n) \leq x_n\}. \end{aligned} \tag{A7.5}$$

If $\xi(t)$ is stationary, it is also time-homogeneous. The contrary is not true, in general. However, time-homogeneous Markov Processes become stationary as $t \rightarrow \infty$.

The stochastic processes discussed in this appendix evolve in time, and their state space is a subset of natural numbers.

A7.2 Renewal Processes

In reliability theory, *renewal processes* describe the model of an item in continuous operation which is replaced at every failure, in a negligible amount of time, by a new, statistically identical item. Results for renewal processes are basic and useful in practical applications.

To define the renewal process, let τ_0, τ_1, \dots be (stochastically) independent and non-negative random variables distributed according to

$$F_A(x) = \Pr\{\tau_0 \leq x\}, \quad x \geq 0, \tag{A7.6}$$

and

$$F(x) = \Pr\{\tau_i \leq x\}, \quad i = 1, 2, \dots, x \geq 0. \tag{A7.7}$$

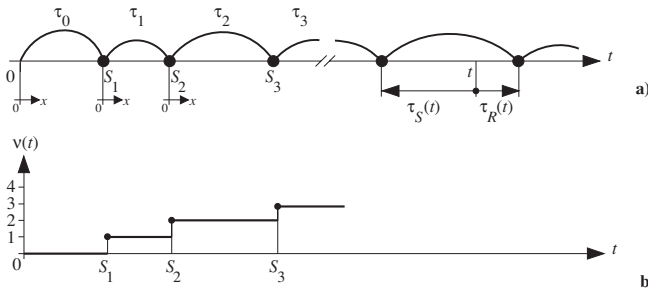


Figure A7.1 a) Possible time schedule for a *renewal process*; b) Corresponding *count function* $v(t)$ (S_1, S_2, \dots are *renewal points* ⁺), x start by 0 at $t=0$ and at every renewal point)

The random variables

$$S_n = \sum_{i=0}^{n-1} \tau_i, \quad n = 1, 2, \dots, \tag{A7.8}$$

or equivalently the sequence τ_0, τ_1, \dots constitutes a *renewal process*. The points S_1, S_2, \dots on the time axis are *renewal points*, and at these points the process *restarts anew*, as a whole ⁺. The renewal process is thus a particularly simple *point process*. The arcs relating the time points $0, S_1, S_2, \dots$ on Fig.A7.1a help to visualize the underlying point process. A *count function*

$$v(t) = \begin{cases} 0 & \text{for } t < \tau_0 \\ n & \text{for } S_n \leq t < S_{n+1}, \quad n=1, 2, \dots, v(t)=0 \text{ for } t \leq 0, \end{cases}$$

can be associated to a renewal process, giving the number of renewal points in the interval $(0, t]$ (Fig. A7.1b). Renewal processes are *ordinary* for $F_A(x) = F(x)$, otherwise they are *modified* (*stationary* for $F_A(x)$ as in Eq. (A7.35)). For $F_A(x) = F(x) = 1 - e^{-\lambda x}$, the renewal process is a *homogeneous Poisson process* (p. 472).

To simplify investigations, let us assume in the following that

$$F_A(x) = F(x) = 0 \quad \text{for } x \leq 0, \tag{A7.9}$$

$$f_A(x) = \frac{dF_A(x)}{dx}, \quad f(x) = \frac{dF(x)}{dx} \quad \text{exist,} \quad x > 0, f_A(x) = f(x) = 0 \text{ for } x \leq 0, \tag{A7.10}$$

$$MTTF_A = E[\tau_0] < \infty, \quad MTTF = E[\tau_i] = \int_0^\infty (1 - F(x)) dx < \infty, \quad i \geq 1, \tag{A7.11}$$

$$\sigma_A^2 = \text{Var}[\tau_0] < \infty, \quad \sigma^2 = \text{Var}[\tau_i] < \infty, \quad i \geq 1.$$

As $\tau_0 > 0, \tau_1 > 0, \dots$ are *interarrival times*, the variable x starting by 0 at $t=0$ and at every renewal point S_1, S_2, \dots (*arrival times*) is used instead of t (Fig. A7.1a).

⁺ *Regeneration point* instead of *renewal point* will be used when the process restarts anew with respect to a specific state (see e.g. Fig. A7.3 on p. 475 and Figs. A7.11-A7.13 on pp. 511-513).

A7.2.1 Renewal Function, Renewal Density

Consider first the distribution function of the number of renewal points $v(t)$ in the time interval $(0, t]$. From Fig. A7.1,

$$\begin{aligned} \Pr\{v(t) \leq n-1\} &= \Pr\{S_n > t\} = 1 - \Pr\{S_n \leq t\} \\ &= 1 - \Pr\{\tau_0 + \dots + \tau_{n-1} \leq t\} = 1 - F_n(t), \quad n=1, 2, \dots \end{aligned} \quad (A7.12)$$

The functions $F_n(t)$ can be calculated recursively (Eq. A6.73))

$$\begin{aligned} F_1(t) &= F_A(t), \quad t > 0, \quad F_1(t) = F_A(t) = 0 \text{ for } t \leq 0, \\ F_{n+1}(t) &= \int_0^t F_n(t-x)f(x)dx, \quad n=1, 2, \dots, \quad t > 0, \quad F_{n+1}(t) = 0 \text{ for } t \leq 0. \end{aligned} \quad (A7.13)$$

From Eq. (A7.12) it follows that

$$\Pr\{v(t) = n\} = \Pr\{v(t) \leq n\} - \Pr\{v(t) \leq n-1\} = F_n(t) - F_{n+1}(t), \quad n=1, 2, \dots, \quad (A7.14)$$

and thus, for the expected value (mean) of $v(t)$,

$$E[v(t)] = \sum_{n=1}^{\infty} n[F_n(t) - F_{n+1}(t)] = \sum_{n=1}^{\infty} F_n(t) = H(t), \quad t > 0, \quad H(t) = 0 \text{ for } t \leq 0, \quad (A7.15)$$

The function $H(t)$ defined by Eq. (A7.15) is the *renewal function*. Due to $F_A(0) = F(0) = 0$ one has $H(0) = 0$. The distribution functions $F_n(t)$ have densities

$$f_1(t) = f_A(t) \quad \text{and} \quad f_n(t) = \int_0^t f(x)f_{n-1}(t-x)dx, \quad f_1(t) = f_n(t) = 0 \text{ for } t \leq 0, \quad n=2, 3, \dots, \quad t > 0, \quad (A7.16)$$

and are thus the *convolutions* of $f(x)$ with $f_{n-1}(x)$. Changing the order of summation and integration one obtains from Eq. (A7.15)

$$H(t) = \sum_{n=1}^{\infty} \int_0^t f_n(x)dx = \int_0^t \sum_{n=1}^{\infty} f_n(x)dx, \quad t > 0, \quad H(t) = 0 \text{ for } t \leq 0. \quad (A7.17)$$

The function

$$h(t) = \frac{dH(t)}{dt} = \sum_{n=1}^{\infty} f_n(t), \quad t > 0, \quad h(t) = 0 \text{ for } t \leq 0, \quad (A7.18)$$

is the *renewal density*, or *renewal points frequency*. $h(t)$ is the *failure intensity* $z(t)$ (Eq. (A7.228)) for the case in which failures of a repairable item (system) with negligible repair times can be described by a renewal process (see also Eqs. (A7.24) and (A7.229)).

$H(t)$ and $h(t)$ per Eqs. (A7.15) and (A7.18) satisfy

$$H(t) = F_A(t) + \int_0^t H(x) f(t-x) dx \quad \text{and} \quad h(t) = f_A(t) + \int_0^t h(x) f(t-x) dx. \quad (\text{A7.19})$$

Equations (A7.19), known as *renewal equations*, have a solution with Laplace transforms (Appendix A9.7) [A7.9(1941)]

$$\tilde{H}(s) = \frac{\tilde{F}_A(s)}{1 - \tilde{f}(s)} = \frac{\tilde{f}_A(s)}{s(1 - \tilde{f}(s))} \quad \text{and} \quad \tilde{h}(s) = \frac{\tilde{f}_A(s)}{1 - \tilde{f}(s)}. \quad (\text{A7.20})$$

Furthermore, for $H(t)$ it can be shown that

$$H(t) \geq \frac{t}{MTTF} - 1, \quad (\text{A7.21})$$

with $MTTF$ as per Eq. (A7.11) (see e. g. [2.34 (1965)] for a two sided bound).

For an ordinary renewal process ($F_A(x) = F(x)$) it holds that

$$\tilde{h}_o(s) = \tilde{f}(s) / (1 - \tilde{f}(s)). \quad (\text{A7.22})$$

Thus, an ordinary renewal process is *completely characterized* by its renewal density $h_o(t)$ or renewal function $H_o(t)$ (the index o referring to an ordinary renewal process). In particular, it can be shown (see e. g. [6.3 (1983)]) that

$$\text{Var}[v_o(t)] = H_o(t) + 2 \int_0^t h_o(x) H_o(t-x) dx - (H_o(t))^2. \quad (\text{A7.23})$$

It is not difficult to recognize that $H(t) = E[v(t)]$ and $\text{Var}[v(t)]$ are finite for all $t < \infty$.

The renewal density $h(t)$ has the following important meaning:

Due to the assumption $F_A(0) = F(0) = 0$, it follows that

$$\lim_{\delta t \downarrow 0} \frac{1}{\delta t} \Pr\{v(t+\delta t) - v(t) > 1\} = 0, \quad t > 0,$$

and thus, for $\delta t \downarrow 0$,

$$\Pr\{\text{any one of the renewal points } S_1 \text{ or } S_2 \text{ or } \dots \text{ lies in } (t, t+\delta t)\} = h(t)\delta t + o(\delta t). \quad (\text{A7.24})$$

Equation (A7.24) gives the *unconditional* probability for *one* renewal point in $(t, t+\delta t]$. $h(t)$ corresponds thus to the *failure intensity* $z(t)$ for an arbitrary point process (Eq. (A7.228)) or the intensity $m(t)$ for a Poisson process (homogeneous (Eq. (A7.42)) or nonhomogeneous (Eq. (A7.193))), but *differs basically* from the *failure rate* $\lambda(t)$ defined by Eq. (A6.25), which gives (for $\lambda(t)\delta t$) the *conditional* probability for a failure in $(t, t+\delta t]$ *given item new at $t=0$ and no failure in $(0, t]$* . $\lambda(t)$ can thus be used, as a function of t only for τ_0 . This distinction is important

also for the case of a *homogeneous Poisson process* ($F_A(x) = F(x) = 1 - e^{-\lambda x}$, p. 472), for which $\lambda(x) = \lambda$ holds for *all interarrival times* (with x starting by 0 at every renewal point) and $h(t) = \lambda$ holds for the whole process (see also pp. 378 and 426). Misuses are known, see e. g. [6.1].

Example A7.1 discusses the shape of $H(t)$ for some practical applications.

Example A7.1

Give the renewal function $H(t)$, analytically for

- (i) $f_A(x) = f(x) = \lambda e^{-\lambda x}$ (Exponential)
- (ii) $f_A(x) = f(x) = 0.5\lambda(\lambda x)^2 e^{-\lambda x}$ (Erlang with $n = 3$)
- (iii) $f_A(x) = f(x) = \lambda(\lambda x)^{\beta-1} e^{-\lambda x} / \Gamma(\beta)$ (Gamma),

and numerically for $\lambda(x) = \lambda$ for $0 < x \leq \Psi$ and $\lambda(x) = \lambda + \beta \lambda_w^\beta (x - \Psi)^{\beta-1}$ for $x > \Psi$, i.e. for

$$(iv) F_A(x) = F(x) = \int_0^x f(y) dy = \begin{cases} 1 - e^{-\lambda x} & \text{for } 0 < x \leq \Psi \\ 1 - e^{-(\lambda x + \lambda_w^\beta (x - \Psi)^\beta)} & \text{for } x > \Psi \end{cases}$$

with $\lambda = 4 \cdot 10^{-6} \text{ h}^{-1}$, $\lambda_w = 10^{-5} \text{ h}^{-1}$, $\beta = 5$, $\Psi = 2 \cdot 10^5 \text{ h}$ (wear-out), and for

- (v) $F_A(x) = F(x)$ as in case (iv) but with $\beta = 0.3$ and $\Psi = 0$ (early failures).

Give the solution in a graphical form for cases (iv) and (v) ($f_A(0) = f(0) = F_A(0) = F(0) = 0$).

Solution

The Laplace transformations of $f_A(t)$ and $f(t)$ for the cases (i) to (iii) are (Table A9.7b)

- (i) $\tilde{f}_A(s) = \tilde{f}(s) = \lambda / (s + \lambda)$
- (ii) $\tilde{f}_A(s) = \tilde{f}(s) = \lambda^3 / (s + \lambda)^3$
- (iii) $\tilde{f}_A(s) = \tilde{f}(s) = \lambda^\beta / (s + \lambda)^\beta$,

$\tilde{h}(s) = \tilde{h}_o(s)$ follows from Eq. (A7.22) yielding $h(t) = h_o(t)$ and $H(t) = H_o(t) = \int_0^t h(x) dx$

- (i) $\tilde{h}(s) = \lambda / s$ and $H(t) = \lambda t$
- (ii) $\tilde{h}(s) = \lambda^3 / s(s^2 + 3\lambda s + 3\lambda^2) = \lambda^3 / s[(s + \frac{3}{2}\lambda)^2 + \frac{3}{4}\lambda^2]$
 and $H(t) = \frac{1}{3}[\lambda t - 1 + \frac{2}{\sqrt{3}} e^{-3\lambda t/2} \sin(\sqrt{3}\lambda t/2 + \frac{\pi}{3})]$ (using $d^2 H(t) dt^2 = s \tilde{h}(s)$)
- (iii) $\tilde{h}(s) = \frac{\lambda^\beta / (s + \lambda)^\beta}{1 - \lambda^\beta / (s + \lambda)^\beta} = \sum_{n=1}^\infty [\lambda^\beta / (s + \lambda)^\beta]^n = \sum_{n=1}^\infty \frac{\lambda^{n\beta}}{(s + \lambda)^{n\beta}}$
 and $H(t) = \sum_{n=1}^\infty \int_0^t \frac{\lambda^{n\beta} x^{n\beta-1}}{\Gamma(n\beta)} e^{-\lambda x} dx$.

Cases (iv) and (v) can only be solved numerically or by simulation. Figure A7.2 gives the results for these two cases in a graphical form (see Eq. (A7.28) for the asymptotic behavior of $H(t)$, dashed line in Fig. A7.2a). Figure A7.2 shows that the convergence of $H(t)$ to its asymptotic value is reasonably fast. The shape of $H(t)$ allows recognition of the presence of wear-out (case iv) or early failures (case v), but *can not* deliver valid indications on the failure rate shape (see Section 7.6.3.3 & Problem A7.2 in Appendix A11). Cases iv & v are also discussed on pp. 7, 337-8, 355-6; see also Section 7.6 for considerations with nonhomogeneous Poisson processes.

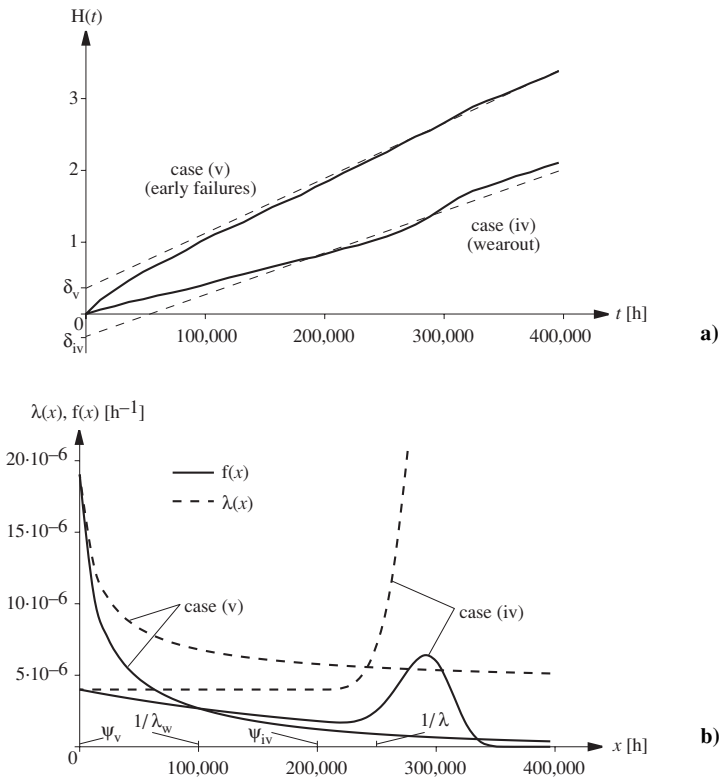


Figure A7.2 a) Renewal function $H(t)$ and b) Failure rate $\lambda(x)$ and density $f(x)$ for cases (iv) & (v) in Example A7.1 ($H(t)$ was obtained empirically, simulating 1000 failure-free times and plotting $H(t)$ as a continuous curve; $\delta = [(\sigma / MTTF)^2 - 1] / 2$ per Eq.(A7.28))

A7.2.2 Recurrence Times

Consider now the distribution functions of the forward recurrence time $\tau_R(t)$ and the backward recurrence time $\tau_S(t)$. As shown in Fig. A7.1a, $\tau_R(t)$ and $\tau_S(t)$ are the time intervals from an arbitrary time point t forward to the next renewal point and backward to the last renewal point (or to the time origin), respectively. It follows from Fig. A7.1a that the event $\tau_R(t) > x$ occurs with one of the following mutually exclusive events

$$A_0 = \{S_1 > t + x\}$$

$$A_n = \{(S_n \leq t) \cap (\tau_n > t + x - S_n)\}, \quad n = 1, 2, \dots$$

Obviously, $\Pr\{A_0\} = 1 - F_A(t + x)$. The event A_n means that exactly n renewal points have occurred before t and the $(n+1)$ th renewal point occurs after $t + x$. Considering that S_n and τ_n are independent, it follows that

$$\Pr\{A_n \mid S_n = y\} = \Pr\{\tau_n > t + x - y\}, \quad n = 1, 2, \dots,$$

and thus, from the theorem of total probability (Eq. (A6.17))

$$\Pr\{\tau_R(t) > x\} = 1 - F_A(t + x) + \int_0^t h(y)(1 - F(t + x - y))dy, \quad t, x > 0,$$

yielding finally, for the *forward recurrence time* $\tau_R(t)$,

$$\Pr\{\tau_R(t) \leq x\} = F_A(t + x) - \int_0^t h(y)(1 - F(t + x - y))dy, \quad t, x > 0. \quad (A7.25)$$

The distribution function of the *backward recurrence time* $\tau_S(t)$ can be obtained as

$$\Pr\{\tau_S(t) \leq x\} = \begin{cases} \int_{t-x}^t h(y)(1 - F(t - y))dy & \text{for } 0 < x < t \\ 1 & \text{for } x \geq t > 0. \end{cases} \quad (A7.26)$$

Since $\Pr\{S_0 > t\} = 1 - F_A(t)$, the distribution function of $\tau_S(t)$ makes a jump of height $1 - F_A(t)$ at the point $x = t$.

A7.2.3 Asymptotic Behavior

Asymptotic behavior of a renewal process (generally of a stochastic process) is understood to be the behavior of the process for $t \rightarrow \infty$. The following theorems hold with *MTTF* and σ as per Eq. (A7.11) (some of these theorems can be proved with less restrictive assumptions as conditions (A7.9) - (A7.11)):

1. *Elementary Renewal Theorems* [A7.9 (1941), A7.24 (1954)]: If conditions (A7.9) - (A7.11) are fulfilled, then

$$\begin{aligned} \lim_{t \rightarrow \infty} (E[v(t)] / t) &= \lim_{t \rightarrow \infty} (H(t) / t) = 1 / MTF, \\ \lim_{t \rightarrow \infty} (\text{Var}[v(t)] / t) &= \sigma^2 / MTF^2. \end{aligned} \quad (A7.27)$$

It can also be shown [6.17] that $\lim_{t \rightarrow \infty} (v(t) / t) = 1 / MTF$ holds with probability 1.

2. *Tightened Elementary Renewal Theorem* [A7.24 (1954)]: If conditions (A7.9) - (A7.11) are fulfilled, then

$$\lim_{t \rightarrow \infty} (H(t) - \frac{t}{MTF}) = \frac{\sigma^2}{2 MTF^2} - \frac{MTF_A}{MTF} + \frac{1}{2}. \quad (A7.28)$$

3. *Key Renewal Theorem* [A7.24 (1954)]: If conditions (A7.9) - (A7.11) are fulfilled, $U(z) \geq 0$ is bounded, nonincreasing, and Riemann integrable over the interval $(0, \infty)$, and $h(t)$ is a renewal density, then

$$\lim_{t \rightarrow \infty} \int_0^t U(t-y)h(y)dy = \frac{1}{MTTF} \int_0^\infty U(z)dz . \tag{A7.29}$$

For any $a > 0$, the key renewal theorem leads, with

$$U(z) = \begin{cases} 1 & \text{for } 0 < z < a \\ 0 & \text{otherwise,} \end{cases}$$

to the *Blackwell's Theorem* [A7.24 (1954)]

$$\lim_{t \rightarrow \infty} \frac{H(t+a) - H(t)}{a} = \frac{1}{MTTF} , \quad a > 0. \tag{A7.30}$$

4. *Renewal Density Theorem* [A7.9 (1941), A7.24 (1954)] : If conditions (A7.9) - (A7.11) are fulfilled, $f_A(x)$ & $f(x)$ go to 0 as $x \rightarrow \infty$, then

$$\lim_{t \rightarrow \infty} h(t) = \frac{1}{MTTF} . \tag{A7.31}$$

5. *Recurrence Time Limit Theorems*: Assuming $U(z) = 1 - F(x+z)$ in Eq. (A7.29) and considering $F_A(\infty) = 1$ & $MTTF = \int_0^\infty (1 - F(y))dy$, Eq. (A7.25) yields

$$\lim_{t \rightarrow \infty} \Pr\{\tau_R(t) \leq x\} = 1 - \frac{1}{MTTF} \int_0^\infty (1 - F(x+z))dz = \frac{1}{MTTF} \int_0^x (1 - F(y))dy . \tag{A7.32}$$

For $t \rightarrow \infty$, the density of the *forward recurrence time* $\tau_R(t)$ is thus given by $f_{\tau_R}(x) = (1 - F(x)) / MTTF$. Considering $E[\tau_i] = MTTF < \infty$, $\sigma^2 = \text{Var}[\tau_i] < \infty$ ($i \geq 1$), and $E[\tau_R(t)] < \infty$, it follows that $\lim_{x \rightarrow \infty} (x^2(1 - F(x))) = 0$ (supplementary results in Example A6.9 ($c > 1$), p.432). Integration by parts and Eq. (A6.45) lead to

$$\lim_{t \rightarrow \infty} E[\tau_R(t)] = \frac{1}{MTTF} \int_0^\infty x(1 - F(x))dx = \frac{MTTF}{2} + \frac{\sigma^2}{2 MTTF} . \tag{A7.33}$$

The result of Eq. (A7.33) is important to clarify the *waiting time paradox*:

- (i) $\lim_{t \rightarrow \infty} E[\tau_R(t)] = MTTF / 2$ holds for $\sigma^2 = 0$, i.e. for $\tau_i = MTTF$, $i \geq 0$, and
- (ii) $\lim_{t \rightarrow \infty} E[\tau_R(t)] = E[\tau_i] = 1/\lambda = MTTF$, $i \geq 0$, holds for $F_A(x) = F(x) = 1 - e^{-\lambda x}$.

Similar is for $\tau_S(t)$. For a *simultaneous* observation of $\tau_R(t)$ and $\tau_S(t)$, it must be noted that in this cases $\tau_R(t)$ and $\tau_S(t)$ belong to the same τ_i and are independent only for case (ii). Considering Eqs. (A7.37) & (A7.32), Eq. (A7.33) holds for any $t > 0$ in the case of a *stationary renewal process*.

6. *Central Limit Theorem for Renewal Processes* ([A6.6 (Vol. II), A7.24 (1955), A7.29 (1956)]): If conditions (A7.9) - (A7.11) are fulfilled, then

$$\lim_{t \rightarrow \infty} \Pr \left\{ \frac{v(t) - t/MTTF}{\sigma \sqrt{t/MTTF^3}} \leq x \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-y^2/2} dy. \tag{A7.34}$$

Equation (A7.34) is a consequence of the central limit theorem (Eq. (A6.148)); it shows that $v(t)$ is for $t \rightarrow \infty$ normally distributed with mean $t/MTTF$ and variance $\sigma^2 t/MTTF^3$,

Equations (A7.27) - (A7.34) show that renewal processes encountered in practical applications converge to a *statistical equilibrium (steady-state)* as $t \rightarrow \infty$, see Appendix A7.2.4 for a discussion on stationary renewal processes.

A7.2.4 Stationary Renewal Processes

The results of Appendix A7.2.3 allow a *stationary renewal process* to be defined as follows:

A renewal process is stationary (in steady-state) if for all $t > 0$ the distribution function of $\tau_R(t)$ in Eq. (A7.25) does not depend on t .

It is intuitively clear that such a situation can only occur if a particular relationship exists between the distribution functions $F_A(x)$ and $F(x)$ given by Eqs. (A7.6) and (A7.7). Assuming, as *initial distribution* at $t=0$,

$$F_A(x) = \frac{1}{MTTF} \int_0^x (1 - F(y)) dy, \quad x > 0, \quad F(x) = F_A(x) = 0 \text{ for } x \leq 0, \tag{A7.35}$$

it follows that $f_A(x) = (1 - F(x)) / MTTF$, $\tilde{f}_A(s) = (1 - \tilde{f}(s)) / (s \cdot MTTF)$, and thus from Eq. (A7.20)

$$\tilde{h}(s) = \frac{1}{s \cdot MTTF},$$

yielding

$$h(t) = \frac{1}{MTTF}, \quad t > 0, \quad h(t) = 0 \text{ for } t \leq 0. \tag{A7.36}$$

With $F_A(x)$ & $h(x)$ from Eqs. (A7.35) & (A7.36), Eq. (A7.25) yields for any $t, x > 0$

$$\Pr\{\tau_R(t) \leq x\} = \frac{1}{MTTF} \left[\int_0^{t+x} (1 - F(y)) dy - \int_0^t (1 - F(t+x-y)) dy \right] = \frac{1}{MTTF} \int_0^x (1 - F(y)) dy, \tag{A7.37}$$

as for Eq. (A7.32).

Equation (A7.35) is thus a *necessary and sufficient* condition for stationarity of the renewal process with $\Pr\{\tau_i \leq x\} = F(x), i \geq 1, x > 0, F(x) = 0$ for $x \leq 0$.

It is not difficult to show that the count process $v(t)$ given in Fig. 7.1b, belonging to a *stationary renewal process*, is a *process with stationary increments*. For any $t, a > 0$, and $n = 1, 2, \dots$ it follows that

$$\Pr\{v(t+a) - v(t) = n\} = \Pr\{v(a) = n\} = F_n(a) - F_{n+1}(a),$$

with $F_{n+1}(a)$ as in Eq. (A7.13) and $F_A(x)$ as in Eq. (A7.35). Moreover, for a stationary renewal process, $H(t) = t / MTTF$ and the mean number of renewals within an arbitrary interval $(t, t + a]$ is

$$H(t+a) - H(t) = a / MTTF.$$

Comparing Eqs. (A7.32) and (A7.37) it follows that under weak conditions, as $t \rightarrow \infty$ each renewal process becomes stationary. For reliability applications,

a stationary renewal process can thus be regarded as a renewal process with arbitrary initial condition ($F_A(x)$) which has been started at $t = -\infty$ and will only be considered for $t \geq 0$ ($t = 0$ being an arbitrary time point);

in other words,

for reliability applications, asymptotic & steady-state can be used as a synonym for stationary (see e.g. also pp. 187-188, 477, 479, 498, 509, 514).

It can be noted that for a *stationary renewal process*, Eq.(A7.33) holds for $t \geq 0$. The important properties of stationary renewal processes are summarized in Table A7.1.

A7.2.5 Homogeneous Poisson Processes (HPP)

The renewal process, defined by Eq. (A7.8), with

$$F_A(x) = F(x) = 1 - e^{-\lambda x}, \quad x > 0, \lambda > 0 \quad (F_A(x) = F(x) = 0 \text{ for } x \leq 0). \quad (\text{A7.38})$$

is a *homogeneous Poisson process* (HPP), and the contrary is true. $F_A(x)$ per Eq.(A7.38) fulfills Eq.(A7.35) and thus, the Poisson process is stationary. From Appendices A7.2.1 to A7.2.3 it follows that (see also Example A6.21)

$$\Pr\{\tau_0 + \dots + \tau_{n-1} \leq t\} = F_n(t) = 1 - \sum_{i=0}^{n-1} \frac{(\lambda t)^i}{i!} e^{-\lambda t} = \int_0^{\lambda t} \frac{x^{n-1}}{(n-1)!} e^{-x} dx, \quad n = 1, 2, \dots, \quad (\text{A7.39})$$

$$f_n(t) = dF_n(t)/dt = \lambda e^{-\lambda t} (\lambda t)^{n-1} / (n-1)!, \quad n = 1, 2, \dots, \quad (\text{A7.40})$$

$$\Pr\{v(t) = k\} = F_k(t) - F_{k+1}(t) = \frac{(\lambda t)^k}{k!} e^{-\lambda t}, \quad k = 0, 1, 2, \dots, F_0(t) \equiv 1, \quad (\text{A7.41})$$

$$H(t) = E[v(t)] = \lambda t, \quad h(t) = \lambda, \quad \text{Var}[v(t)] = \lambda t, \tag{A7.42}$$

$$\Pr\{\tau_R(t) \leq x\} = 1 - e^{-\lambda x}, \quad t, x > 0, \tag{A7.43}$$

$$\Pr\{\tau_S(t) \leq x\} = \begin{cases} 1 - e^{-\lambda x} & \text{for } 0 < x < t \\ 1 & \text{for } x \geq t > 0. \end{cases} \tag{A7.44}$$

As a result of the *memoryless property* of the exponential distribution, the count function $v(t)$ (as in Fig A7.1b) has *independent increments* (Eq. (A7.2)). Quite generally, a point process is a *homogeneous Poisson process* (HPP), with intensity λ , if the associated count function $v(t)$ has *stationary independent increments and satisfy* Eq. (A7.41). Alternatively, a renewal process satisfying Eq.(A7.38) is an HPP.

Substituting for λt in Eq.(A7.41) a nondecreasing function $M(t) > 0$, a *non-homogeneous Poisson process* (NHPP) is obtained (Appendix A7.8.2). The NHPP is a point process with *independent Poisson distributed increments*. Because of independent increments, the NHPP is a process *without aftereffect* (*memoryless* if HPP) and the sum of Poisson processes is a Poisson process (Eq. (7.27) for HPP). Moreover, the sum of n independent renewal processes with low occurrence converge for $n \rightarrow \infty$ to an NHPP, to an HPP in the case of stationary independent renewal processes (Appendix A7.8.3). However, despite its intrinsic simplicity, the NHPP is *not* a regenerative process, and in statistical data analysis, the property of independent increments is often difficult to be proven. Nonhomogeneous Poisson processes are introduced in Appendix A7.8.2 and used in Sections 7.6&7.7 for reliability tests.

Table A7.1 Main properties of a stationary renewal process

	Expression	Comments, assumptions
1. Distribution function of τ_0	$F_A(x) = \frac{1}{MTTF} \int_0^x (1 - F(y)) dy$	$x > 0^*$, $f_A(x) = dF_A(x)/dx$ $MTTF = E[\tau_i]$, $i \geq 1$
2. Distribution function of $\tau_i, i \geq 1$	$F(x) \quad x > 0^*$	$f(x) = dF(x)/dx$
3. Renewal function	$H(t) = \frac{t}{MTTF}, \quad t > 0^*$	$H(t) = E[v(t)] = E[\text{number of renewal points in } (0, t)]$
4. Renewal density	$h(t) = \frac{1}{MTTF}, \quad t > 0^*$	$h(t) = \frac{dH(t)}{dt}$, $h(t)\delta t \approx \lim_{\delta t \rightarrow 0} \Pr\{S_1 \text{ or } S_2 \text{ or } \dots \text{ lies in } (t, t + \delta t]\}$
5. Distribution function & mean of the forward recurrence time	$\Pr\{\tau_R(t) \leq x\} = F_A(x), \quad t > 0$ $E[\tau_R(t)] = T/2 + \text{Var}[\tau_i]/2T$	$F_A(x)$ as in point 1, similar for $\tau_S(t)$ $T = MTTF = E[\tau_i]$, $i \geq 1$

* $F(x) = F_A(x) = f(x) = f_A(x) = H(t) = h(t) = 0$ for $x, t \leq 0$

A7.3 Alternating Renewal Processes

Generalization of the renewal process given in Fig. A7.1a by introducing a positive random replacement time ($\tau' > 0$), distributed according to $G(x)$, leads to the *alternating renewal process*. An alternating renewal process is a process with two states, which alternate from one state to the other after a stay (sojourn) time distributed according to $F(x)$ and $G(x)$, respectively (it is a 2 states semi-Markov process, see Appendices A7.6 & A7.7 and the footnote on p. 505). Considering the reliability and availability analysis of a repairable item in Section 6.2 and in order to simplify the notation, these two states will be referred to as the *up state* and the *down state*, abbreviated as u and d , respectively.

To define an alternating renewal process, consider two *independent* renewal processes $\{\tau_i\}$ and $\{\tau'_i\}$, $i = 0, 1, \dots$. For reliability applications, τ_i denotes the i th *failure-free time* and τ'_i the i th *repair (restoration) time*. These random variables are distributed according to

$$F_A(x) \text{ for } \tau_0 \text{ and } F(x) \text{ for } \tau_i, i \geq 1, \quad x > 0, F_A(x) = F(x) = 0 \text{ for } x \leq 0, \quad (\text{A7.45})$$

$$G_A(x) \text{ for } \tau'_0 \text{ and } G(x) \text{ for } \tau'_i, i \geq 1, \quad x > 0, G_A(x) = G(x) = 0 \text{ for } x \leq 0, \quad (\text{A7.46})$$

with densities $f_A(x)$, $f(x)$, $g_A(x)$, $g(x)$, and means

$$MTTF = E[\tau_i] = \int_0^\infty (1 - F(x)) dx, \quad i \geq 1, \quad MTTF_A = E[\tau_0], \quad (\text{A7.47})$$

and

$$MTTR = E[\tau'_i] = \int_0^\infty (1 - G(x)) dx, \quad i \geq 1, \quad MTTR_A = E[\tau'_0], \quad (\text{A7.48})$$

where $MTTF$ and $MTTR$ are used for *mean time to failure* and *mean time to repair* (restoration). $E[\tau_i]$, $E[\tau'_i]$, $\text{Var}[\tau_i]$, $\text{Var}[\tau'_i]$, $i \geq 0$, are assumed $< \infty$. The sequences

$$\tau_0, \tau'_1, \tau_1, \tau'_2, \tau_2, \tau'_3, \dots \quad \text{and} \quad \tau'_0, \tau_1, \tau'_1, \tau_2, \tau'_2, \tau_3, \dots \quad (\text{A7.49})$$

form two modified *alternating renewal processes*, starting at $t = 0$ with τ_0 and τ'_0 , respectively. Figure A7.3 shows a possible time schedule of these two alternating renewal processes (repair times greatly exaggerated). *Embedded* in every one of these processes are two renewal processes with renewal points S_{udu_i} or S_{udd_i} marked with \blacktriangle and S_{duu_i} or S_{dud_i} marked with \bullet , where udu denotes a *transition from up to down given up at $t = 0$* , i.e.,

$$S_{udu_1} = \tau_0 \quad \text{and} \quad S_{udu_i} = \tau_0 + (\tau'_1 + \tau_1) + \dots + (\tau'_{i-1} + \tau_{i-1}), \quad i > 1.$$

These four *embedded renewal processes* are statistically identical up to the time intervals starting at $t = 0$ (τ_0 , $\tau_0 + \tau'_1$, $\tau'_0 + \tau_1$, τ'_0). The corresponding densities are

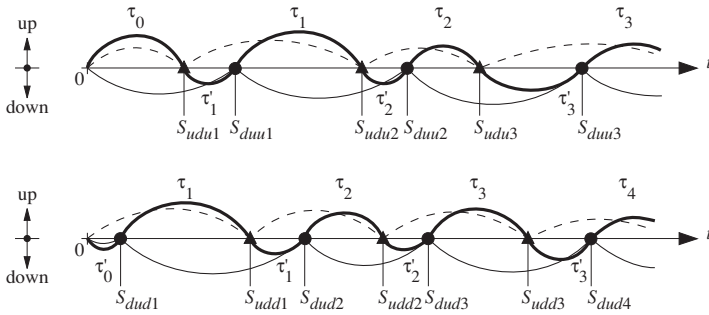


Figure A7.3 Possible time schedule for two *alternating renewal processes* starting at $t = 0$ with τ_0 and τ'_0 , respectively (shown also the 4 embedded renewal processes with *renewal points* ● & ▲, *regeneration points* for the states *up* & *down* of the alternating renewal process, see footnote on p.464)

$$f_A(x), f_A(x) * g(x), g_A(x) * f(x), g_A(x)$$

for the time interval starting at $t = 0$, and

$$f(x) * g(x)$$

for all others. The symbol $*$ denotes *convolution* (Eq. (A6.75)).

Results of Appendix A7.2 can be used to investigate the embedded renewal processes of Fig. A7.3. Equation (A7.20) yields Laplace transforms of the renewal densities $h_{udu}(t)$, $h_{duu}(t)$, $h_{udd}(t)$, and $h_{dud}(t)$

$$\begin{aligned} \tilde{h}_{udu}(s) &= \frac{\tilde{f}_A(s)}{1 - \tilde{f}(s)\tilde{g}(s)}, & \tilde{h}_{duu}(s) &= \frac{\tilde{f}_A(s)\tilde{g}(s)}{1 - \tilde{f}(s)\tilde{g}(s)}, \\ \tilde{h}_{udd}(s) &= \frac{\tilde{g}_A(s)\tilde{f}(s)}{1 - \tilde{f}(s)\tilde{g}(s)}, & \tilde{h}_{dud}(s) &= \frac{\tilde{g}_A(s)}{1 - \tilde{f}(s)\tilde{g}(s)}. \end{aligned} \tag{A7.50}$$

To describe the alternating renewal process defined above (Fig. A7.3), let us introduce the two-dimensional stochastic process $(\zeta(t), \tau_{R\zeta(t)}(t))$ where $\zeta(t)$ denotes the state of the process (repairable item in reliability application)

$$\zeta(t) = \begin{cases} u & \text{if the item is up at time } t \\ d & \text{if the item is down at time } t. \end{cases}$$

$\tau_{Ru}(t)$ and $\tau_{Rd}(t)$ are thus the forward recurrence times in the up and down states, respectively, provided that the item is *up* or *down* at the time t , see Fig. 6.3.

^{+) It can be noted that $f_A(x) = f(x) = \lambda e^{-\lambda x}$, i. e. constant failure rate λ , yields, for *item new at* $t=0$, $h_{udu}(t) = \lambda(\mu + \lambda e^{-(\lambda + \mu)t}) / (\lambda + \mu) = \lambda PA_{S_0}(t)$, as per Eq. (6.19); showing once more the *memoryless property* of exponentially distributed failure-free times.}

To investigate the general case, both alternating renewal processes of Fig. A7.3 must be combined. For this let

$$p = \Pr\{\text{item up at } t = 0\} \quad \text{and} \quad 1 - p = \Pr\{\text{item down at } t = 0\}. \quad (\text{A7.51})$$

In terms of the process $(\zeta(t), \tau_R \zeta(t)(t))$,

$$\begin{aligned} p &= \Pr\{\zeta(0) = u\}, & F_A(x) &= \Pr\{\tau_{Ru}(0) \leq x \mid \zeta(0) = u\}, \\ 1 - p &= \Pr\{\zeta(0) = d\}, & G_A(x) &= \Pr\{\tau_{Rd}(0) \leq x \mid \zeta(0) = d\}. \end{aligned}$$

Consecutive jumps from *up to down* form a renewal process with renewal density

$$h_{ud}(t) = ph_{udu}(t) + (1 - p)h_{udd}(t), \quad t > 0, \quad h_{udu}(t) = h_{udd}(t) = 0 \text{ for } t \leq 0. \quad (\text{A7.52})$$

Similarly, the renewal density for consecutive jumps from *down to up* is given by

$$h_{du}(t) = ph_{duu}(t) + (1 - p)h_{dud}(t), \quad t > 0, \quad h_{duu}(t) = h_{dud}(t) = 0 \text{ for } t \leq 0. \quad (\text{A7.53})$$

Using Eqs. (A7.52) and (A7.53), and considering Eq. (A7.25), it follows that $(\theta \geq 0)$

$$\begin{aligned} \Pr\{\zeta(t) = u \cap \tau_{Ru}(t) > \theta\} &= p(1 - F_A(t + \theta)) + \int_0^t h_{du}(x)(1 - F(t - x + \theta))dx \quad (\text{A7.54}) \end{aligned}$$

and

$$\begin{aligned} \Pr\{\zeta(t) = d \cap \tau_{Rd}(t) > \theta\} &= (1 - p)(1 - G_A(t + \theta)) + \int_0^t h_{ud}(x)(1 - G(t - x + \theta))dx. \quad (\text{A7.55}) \end{aligned}$$

Setting $\theta = 0$ in Eq. (A7.54) yields

$$\Pr\{\zeta(t) = u\} = p(1 - F_A(t)) + \int_0^t h_{du}(x)(1 - F(t - x))dx. \quad (\text{A7.56})$$

The probability $PA(t) = \Pr\{\zeta(t) = u\}$ is called the *point availability* and $IR(t, t + \theta) = \Pr\{\zeta(t) = u \cap \tau_{Ru}(t) > \theta\}$ the *interval reliability* of the given item (see Section 6.2 for further considerations).

An alternating renewal process, characterized by the parameters $p, F_A(x), F(x), G_A(x)$, and $G(x)$ is *stationary* if the two-dimensional process $(\zeta(t), \tau_R \zeta(t)(t))$ is stationary. As with the renewal process it can be shown that an alternating renewal process is *stationary* if and only if

$$p = \frac{MTTF}{MTTF + MTTR}, \quad F_A(x) = \frac{1}{MTTF} \int_0^x (1 - F(y))dy, \quad G_A(x) = \frac{1}{MTTR} \int_0^x (1 - G(y))dy, \quad (\text{A7.57})$$

hold as *initial condition/ distributions* at $t=0$, with *MTTF* & *MTTR* as in Eqs. (A7.47) & (A7.48). In particular, for $t \geq 0$ the following relationships apply for the *stationary alternating renewal process* (see Examples 6.3 & 6.4 for PA, Eq.(6.50) for $IR_S(\theta)$)

$$PA(t) = \Pr\{\text{item up at } t\} = \frac{MTTF}{MTTF + MTTR} = PA, \tag{A7.58}$$

$$\begin{aligned} IR(t, t+\theta) &= \Pr\{\text{item up at } t \text{ and remains up until } t+\theta\} \\ &= \frac{1}{MTTF + MTTR} \int_{\theta}^{\infty} (1 - F(y)) dy = IR_S(\theta). \end{aligned} \tag{A7.59}$$

Condition (A7.57) is equivalent to

$$h_{ud}(t) = h_{du}(t) = \frac{1}{MTTF + MTTR}, \quad t \geq 0. \tag{A7.60}$$

Moreover, application of the *key renewal theorem* (Eq. (A7.29)) to Eqs. (A7.54) - (A7.56) yields (for $\theta > 0$ given (fixed), see Example 6.3 for PA)

$$\lim_{t \rightarrow \infty} \Pr\{\zeta(t) = u \cap \tau_{Ru}(t) > \theta\} = \frac{1}{MTTF + MTTR} \int_{\theta}^{\infty} (1 - F(y)) dy, \tag{A7.61}$$

$$\lim_{t \rightarrow \infty} \Pr\{\zeta(t) = d \cap \tau_{Rd}(t) > \theta\} = \frac{1}{MTTF + MTTR} \int_{\theta}^{\infty} (1 - G(y)) dy, \tag{A7.62}$$

$$\lim_{t \rightarrow \infty} \Pr\{\zeta(t) = u\} = \lim_{t \rightarrow \infty} PA(t) = PA = \frac{MTTF}{MTTF + MTTR}. \tag{A7.63}$$

Under weak conditions, irrespective of its initial conditions p , $F_A(x)$, and $G_A(x)$, an alternating renewal process has for $t \rightarrow \infty$ an *asymptotic behavior* which is identical to the stationary state (*steady-state*). Thus, for reliability applications,

a stationary alternating renewal process can be regarded as an alternating renewal process with arbitrary initial conditions (p , $F_A(x)$, $G_A(x$)) which has been started at $t = -\infty$ and will only be considered for $t \geq 0$ ($t=0$ being an arbitrary time point);

in other words,

for reliability applications, asymptotic & steady-state can be used as a synonym for stationary (see e.g. also pp. 187-188, 472, 479, 498, 509, 514).

It can be noted that the results of this section remain valid even if independence between τ_i and τ'_i within a *cycle* (e. g. $\tau_0 + \tau'_1$, $\tau_1 + \tau'_2$, ...) is dropped; only independence between cycles is necessary. For *exponentially distributed* τ_i and τ'_i , i. e., for *constant failure rate* λ and *repair rate* μ in reliability applications, the *convergence* of $PA(t)$ towards PA stated by Eq. (A7.63) is of the form $PA(t) - PA = (\lambda / (\lambda + \mu)) e^{-(\lambda + \mu)t} \approx (\lambda / \mu) e^{-\mu t}$, see Eq. (6.20). The case of general repair rate is discussed at the end of Section 6.2.4.

A7.4 Regenerative Processes with a Finite Number of States

A *regenerative process* with a finite number of states Z_0, \dots, Z_m is characterized by the property that there is a sequence of random points on the time axis, *regeneration points*, at which the process

forgets its foregoing evolution and, from a probabilistic point of view, restarts anew with respect to the regeneration state considered.

The times at which a regenerative process restarts, occur when the process returns to some states defined as *regeneration states*. The sequence of these time points for a *specific regeneration state* is a *renewal process embedded in the original stochastic process*. For instance, a renewal process is a regenerative process with one state⁺, both states of an alternating renewal process (Fig. A7.3) and, assuming an irreducible embedded Markov chain, all states of a time-homogeneous Markov process & a semi-Markov process (Eqs. (A7.77), (A7.95) & (A7.158)) are regeneration states. However, in practical applications there are processes in discrete state space with only few (Figs. 6.10, A7.11-A7.13) or even with no regeneration states;

a regenerative process must have at least one regeneration state, and the set of regeneration states constitutes a semi-Markov process embedded in the original process.

A regenerative process with states space Z_0, \dots, Z_m and an embedded semi-Markov process on the regeneration states $Z_0, \dots, Z_k, 0 < k < m$, is (in this book) a *semi-regenerative process* (Appendix A7.7), and has $k+1$ *embedded renewal processes*.

In the following, a basic result for regenerative processes is given focusing on *an arbitrarily chosen regeneration state and the related embedded renewal process*. So considered, the process consists of *independent cycles* which describe the time behavior of the process *between two consecutive regeneration points*. The i th cycle is characterized by a positive random variable τ_{c_i} (duration of cycle i) and a stochastic process $\xi_i(x)$ defined for $0 \leq x < \tau_{c_i}$ (content of cycle). The pieces $\xi_n(x)$ ($n=0, 1, \dots, 0 \leq x < \tau_{c_n}$) are independent, and for $n \geq 1$ identically distributed cycles. The time points $S_1 = \tau_{c_0}, S_2 = \tau_{c_0} + \tau_{c_1}, \dots$ form a *renewal process*, for which we assume that τ_{c_0} and $\tau_{c_i}, i \geq 1$, have distribution functions $F_A(x)$ for τ_{c_0} & $F(x)$ for τ_{c_i} , densities $f_A(x)$ & $f(x)$, and finite means T_A & T_C and variances σ_A^2 & σ_C^2 , respectively ($F_A(x) = F(x) = f_A(x) = f(x) = 0$ for $x \leq 0$). $\xi(t)$ is then given by

$$\xi(t) = \begin{cases} \xi_0(t) & \text{for } 0 \leq t < S_1 \\ \xi_n(t - S_n) & \text{for } S_n \leq t < S_{n+1}, \quad n = 1, 2, \dots \end{cases}$$

The regenerative structure is *sufficient for the existence of an asymptotic behavior (limiting distribution) for the process as $t \rightarrow \infty$ (provided $T_A, T_C < \infty$)*. This

⁺ *Renewal point* instead of *regeneration point* is to use, because the *whole process restarts anew*.

limiting distribution is determined by the behavior of the process between *two consecutive regeneration points* (belonging to the same embedded renewal process) [A7.9 (1949 & Vol 2), A7.24, 6.3 (1983)]. Defining $h(t)$ as the renewal density of the *embedded renewal process*, and setting

$$U(x, B) = \Pr\{ \xi_i(x) \in B \cap \tau_{c_i} > x \}, \quad i = 1, 2, \dots, \quad B \subseteq \{Z_0, \dots, Z_m\},$$

it follows, similarly to Eq. (A7.25), that

$$\Pr\{ \xi(t) \in B \} = \Pr\{ \xi_0(t) \in B \cap \tau_{c_0} > t \} + \int_0^t h(x)U(t-x, B)dx. \quad (A7.64)$$

For any given distribution of the cycle $\xi_i(x)$, $0 \leq x < \tau_{c_i}$, $i \geq 1$, with $T_c = E[\tau_{c_i}] < \infty$, there exists a *stationary regenerative process* $\xi_e(t)$ with regeneration points S_{e_i} , $i \geq 1$. The cycles $\xi_{e_n}(x)$, $0 \leq x < \tau_{e_n}$, have for $n \geq 1$ the same distribution law as $\xi_i(x)$, $0 \leq x < \tau_{c_i}$. The distribution law of the starting cycle $\xi_{e_0}(x)$, $0 \leq x < \tau_{e_0}$, can be computed from the distribution law of $\xi_i(x)$, $0 \leq x < \tau_{c_i}$ (see e.g. Eq. (A7.57) for an alternating renewal process). In particular [A7.24 (1955), 6.3],

$$\Pr\{ \xi_e(0) \in B \} = \frac{1}{T_c} \int_0^\infty U(x, B)dx, \quad (A7.65)$$

with $T_c = E[\tau_{c_i}] < \infty$, $i \geq 1$. Furthermore, for $S_1 = 0$ and $g(x)$ non-negative, strictly increasing, and continuous, it holds that [6.3]

$$E[g(\xi_e(0))] = \frac{1}{T_c} E\left[\int_0^{\tau_{c_1}} g(\xi_1(x))dx \right]. \quad (A7.66)$$

Equation (A7.66) is known as the *stochastic mean value theorem* for regenerative processes, and can be extended to every non-negative function $g(x)$. Assuming, for instance, $\xi_i(x) = 1$ for item *up* & $\xi_i(x) = 0$ for item *down* for the alternating renewal process, and $g(x) = x$, Eq. (A7.66) yields $E[\xi_e(0)] = \Pr\{\xi_e(0) = 1\} = p$ (Eq. (A7.57)).

Since $T_c < \infty$ and $U(x, B)$ is ≥ 0 , nonincreasing and $\leq 1 - \Pr\{\tau_{c_i} \leq x\}$ for all $x > 0$, it follows from Eq. (A7.64) and the *key renewal theorem* (Eq. (A7.29)) that

$$\lim_{t \rightarrow \infty} \Pr\{ \xi(t) \in B \} = \frac{1}{T_c} \int_0^\infty U(x, B)dx \quad T_c = E[\tau_{c_i}] < \infty, \quad i \geq 1. \quad (A7.67)$$

Equations (A7.65), (A7.67) show that under weak conditions, as $t \rightarrow \infty$ a regenerative process becomes *stationary* (see Eqs. (A7.188) & (A7.188a) for a *semi-regenerative process*, and the example at the bottom of p. 514, as well as Eqs. (6.110) & (6.131), for practical applications). As for renewal (p. 472), alternating renewal (p. 477), Markov (p. 498), and semi-Markov (p. 509) processes, for reliability applications,

a stationary regenerative process can be considered as a regenerative process with arbitrary distribution of the starting cycle, which has been started at $t = -\infty$ and will only be considered for $t \geq 0$ ($t = 0$ being an arbitrary time point).

A7.5 Markov Processes with a Finite Number of States

Markov processes are processes *without aftereffect*. They are characterized by the property that for any (arbitrarily chosen) time point t their evolution after t depends on t and the state occupied at t , but not on the process evolution up to the time t . In the case of *time-homogeneous* Markov processes, *dependence on t also disappears*. In reliability theory, these processes describe the behavior of repairable systems with *constant failure and repair rates* for all elements. Constant rates are required during the stay (sojourn) time in every state, not necessarily at state changes (e.g. because of load sharing). After an introduction to *Markov chains*, time-homogeneous *Markov processes* with a finite number of states are introduced as basis for Chapter 6.

A7.5.1 Markov Chains with a Finite Number of States

Let ξ_0, ξ_1, \dots be a sequence random variables taking values on $\{Z_0, \dots, Z_m\}, 0 < m < \infty$, e.g. the sequence of *consecutively occurring states* of an arbitrary system. The sequence $\{\xi_n\}, n = 0, 1, \dots$ constitutes a *Markov chain with state space* $\{Z_0, \dots, Z_m\}, 0 < m < \infty$, if for $n = 0, 1, 2, \dots$ and arbitrary $i, j, i_0, \dots, i_{n-1} \in \{0, \dots, m\}$

$$\begin{aligned} \Pr\{\xi_{n+1} = Z_j \mid (\xi_n = Z_i \cap \xi_{n-1} = Z_{i_{n-1}} \cap \dots \cap \xi_0 = Z_{i_0})\} \\ = \Pr\{\xi_{n+1} = Z_j \mid \xi_n = Z_i\} = p_{ij}(n) \end{aligned} \quad (A7.68)$$

holds.^{*)} The quantities $p_{ij}(n)$ are the (one step) *transition probabilities of the Markov chain*. Investigation will be limited here to *time-homogeneous* Markov chains, for which the transition probabilities $p_{ij}(n)$ are independent of n

$$p_{ij}(n) = p_{ij} = \Pr\{\xi_{n+1} = Z_j \mid \xi_n = Z_i\}, \quad n = 0, 1, \dots \quad (A7.69)$$

For simplicity, *Markov chain* will be used in the following for *time-homogeneous Markov chains*. The probabilities p_{ij} satisfy the relationships

$$p_{ij} \geq 0 \quad \text{and} \quad \sum_{j=0}^m p_{ij} = 1, \quad i, j \in \{0, \dots, m\}. \quad (A7.70)$$

A matrix with elements p_{ij} as in Eq. (A7.70) is a *stochastic matrix*. The k -step transition probabilities are the elements of the k th power of the stochastic matrix with elements p_{ij} . For instance, $k=2$ leads to (Example A7.2, Eq. (A6.17))

$$\begin{aligned} p_{ij}^{(2)} &= \Pr\{\xi_{n+2} = Z_j \mid \xi_n = Z_i\} = \sum_{k=0}^m \Pr\{(\xi_{n+2} = Z_j \cap \xi_{n+1} = Z_k) \mid \xi_n = Z_i\} \\ &= \sum_{k=0}^m \Pr\{\xi_{n+1} = Z_k \mid \xi_n = Z_i\} \Pr\{\xi_{n+2} = Z_j \mid (\xi_n = Z_i \cap \xi_{n+1} = Z_k)\}, \end{aligned}$$

^{*)} ξ_0, ξ_1, \dots identify only *successive transitions* (in the same state for $p_{ii}(n) > 0$) without relation to the time axis; this is important when considering *Markov chains embedded* in stochastic processes.

Example A7.2

Assuming $\Pr\{C\} > 0$, prove that $\Pr\{(A \cap B) \mid C\} = \Pr\{B \mid C\} \Pr\{A \mid (B \cap C)\}$.

Solution

For $\Pr\{C\} > 0$ it follows that

$$\Pr\{(A \cap B) \mid C\} = \frac{\Pr\{A \cap B \cap C\}}{\Pr\{C\}} = \frac{\Pr\{B \cap C\} \Pr\{A \mid (B \cap C)\}}{\Pr\{C\}} = \Pr\{B \mid C\} \Pr\{A \mid (B \cap C)\}.$$

from which, considering the Markov property (Eqs. (A7.68)),

$$\mathcal{P}_{ij}^{(2)} = \sum_{k=0}^m \Pr\{\xi_{n+1} = Z_k \mid \xi_n = Z_i\} \Pr\{\xi_{n+2} = Z_j \mid \xi_{n+1} = Z_k\} = \sum_{k=0}^m \mathcal{P}_{ik} \mathcal{P}_{kj}. \quad (\text{A7.71})$$

Results for $k > 2$ follow by induction.

The *distribution law* of a Markov chain is completely given by the *initial distribution*

$$A_i = \Pr\{\xi_0 = Z_i\}, \quad i = 0, \dots, m, \quad (\text{A7.72})$$

with $\sum A_i = 1$, and the *transition probabilities* \mathcal{P}_{ij} . For arbitrary $i_0, \dots, i_n \in \{0, \dots, m\}$

$$\Pr\{\xi_0 = Z_{i_0} \cap \xi_1 = Z_{i_1} \cap \dots \cap \xi_n = Z_{i_n}\} = A_{i_0} \mathcal{P}_{i_0 i_1} \dots \mathcal{P}_{i_{n-1} i_n},$$

and the *state probability* (absolute probability) follows as (Eq. (A6.17))

$$\Pr\{\xi_n = Z_j\} = \sum_{i=0}^m A_i \mathcal{P}_{ij}^{(n)}, \quad n = 1, 2, \dots \quad (\text{A7.73})$$

A Markov chain with transition probabilities \mathcal{P}_{ij} is *stationary* (in steady-state) if and only if the state probabilities $\mathcal{P}_j = \Pr\{\xi_n = Z_j\}$, $j = 0, \dots, m$, are independent of n , i.e., if the initial distribution A_i (Eq. (A7.72)) is a solution (\mathcal{P}_j) of the system

$$\mathcal{P}_j = \sum_{i=0}^m \mathcal{P}_i \mathcal{P}_{ij}, \quad \text{with } \mathcal{P}_j \geq 0 \quad \text{and} \quad \sum_{j=0}^m \mathcal{P}_j = 1, \quad j = 0, \dots, m. \quad (\text{A7.74})$$

The system given by Eq. (A7.74) must be solved by replacing one (freely chosen) equation by $\sum \mathcal{P}_j = 1$. \mathcal{P}_j per Eq. (A7.74) expresses that

in steady-state, the probability to be in Z_j is equal to that to come in Z_j .

$\mathcal{P}_0, \dots, \mathcal{P}_m$ from Eq. (A7.74) define the *stationary distribution* of the Markov chain with transition probabilities \mathcal{P}_{ij} .

A Markov chain with transition probabilities \mathcal{P}_{ij} is *irreducible* if every state can be reached from every other state, i.e., if for each (i, j) there is an $n = n(i, j)$ such that

$$\mathcal{P}_{ij}^{(n)} > 0, \quad i, j \in \{0, \dots, m\}, \quad n \geq 1. \quad (\text{A7.75})$$

It can be shown that the system (A7.74) possesses (for $m < \infty$) a *unique solution* with

$$P_j > 0 \quad \text{and} \quad P_1 + P_2 + \dots + P_m = 1, \quad j = 0, \dots, m, \quad (A7.76)$$

only if the Markov chain is *irreducible*, see e. g. [A7.3, A7.9 (V.1)]. In this case, the stationary distribution is also an *ergodic distribution*, i. e. $P_j = \lim_{n \rightarrow \infty} P_{ij}^{(n)}$.

A7.5.2 Markov Processes with a Finite Number of States ⁺⁾

A stochastic process $\xi(t)$ with state space $\{Z_0, \dots, Z_m\}, 0 < m < \infty$, is a *Markov process* in continuous time ($t \geq 0$) with a finite number of states, if for $n = 0, 1, 2, \dots$, arbitrary time points $t+a > t > t_n > \dots > t_0 \geq 0$, and arbitrary $i, j, i_0, \dots, i_n \in \{0, \dots, m\}$

$$\begin{aligned} \Pr\{ \xi(t+a) = Z_j \mid (\xi(t) = Z_i \cap \xi(t_n) = Z_{i_n} \cap \dots \cap \xi(t_0) = Z_{i_0}) \} \\ = \Pr\{ \xi(t+a) = Z_j \mid \xi(t) = Z_i \} \end{aligned} \quad (A7.77)$$

holds. $\xi(t)$ ($t \geq 0$) is a jump function (jump process), as visualized in Fig. A7.10. The conditional state probabilities in Eq. (A7.77) are the *transition probabilities* of the Markov process and they will be designated by $P_{ij}(t, t+a)$

$$P_{ij}(t, t+a) = \Pr\{ \xi(t+a) = Z_j \mid \xi(t) = Z_i \}, \quad t \geq 0, a > 0. \quad (A7.78)$$

Equations (A7.77) and (A7.78) give the probability that $\xi(t+a)$ will be Z_j given that $\xi(t)$ was Z_i . Between t and $t+a$ the Markov process *can visit any other state* (this is not the case in Eq. (A7.95), in which Z_j is the *next state* visited after Z_i).

The Markov process is *time-homogeneous* if

$$P_{ij}(t, t+a) = P_{ij}(a), \quad t \geq 0, a > 0. \quad (A7.79)$$

In the following only time-homogeneous Markov processes in continuous time ($t \geq 0$) and with a finite number of states ($m+1$) is considered. Equation (A7.79) expresses the *memoryless property of the time-homogeneous Markov processes*. From these property, for arbitrary $t \geq 0$ and given $a > 0$, $P_{ij}(t+a)$ satisfy the *Chapman-Kolmogorov equations*

$$P_{ij}(t+a) = \sum_{k=0}^m P_{ik}(t)P_{kj}(a), \quad t \geq 0, a > 0, i, j \in \{0, \dots, m\}, \quad (A7.80)$$

whose demonstration is similar to $p_{ij}^{(2)}$ in Eq. (A7.71). Furthermore $P_{ij}(a)$ satisfy

$$P_{ij}(a) \geq 0 \quad \text{and} \quad \sum_{j=0}^m P_{ij}(a) = 1, \quad a \geq 0, i = 0, \dots, m, \quad (A7.81)$$

and thus form a *stochastic matrix*. Together with the *initial distribution*

$$P_i(0) = \Pr\{ \xi(0) = Z_i \}, \quad i = 0, \dots, m, \quad (A7.82)$$

⁺⁾ Continuous (parameter) Markov chain is often used in the literature. Use of Markov process should help to avoid confusion with Markov chains embedded in stochastic processes (footnote on p. 480).

the transition probabilities $P_{ij}(a)$ completely determine the distribution law of the Markov process. In particular, the *state probabilities*

$$P_j(t) = \Pr\{\xi(t) = Z_j\}, \quad t > 0, \quad j = 0, \dots, m, \quad (\text{A7.83})$$

follows as (theorem of total probability (Eq. (A6.17)) and Eq. (A7.82))

$$P_j(t) = \sum_{i=0}^m P_i(0)P_{ij}(t), \quad t > 0. \quad (\text{A7.84})$$

Setting

$$P_{ij}(0) = \delta_{ij} = \begin{cases} 0 & \text{for } i \neq j \\ 1 & \text{for } i = j \end{cases} \quad (\text{A7.85})$$

and assuming that the transition probabilities $P_{ij}(t)$ are *continuous* at $t=0$, it can be shown that $P_{ij}(t)$ are also differentiable at $t=0$ (see e. g. the discussion to Eqs. (A7.105)-(A7.106). Thus, the limiting values

$$\lim_{\delta t \downarrow 0} \frac{P_{ij}(\delta t)}{\delta t} = \rho_{ij}, \quad \text{for } i \neq j, \quad \text{and} \quad \lim_{\delta t \downarrow 0} \frac{1 - P_{ii}(\delta t)}{\delta t} = \rho_i, \quad (\text{A7.86})$$

exist and satisfy

$$\rho_i = \sum_{\substack{j=0 \\ j \neq i}}^m \rho_{ij}, \quad i = 0, \dots, m. \quad (\text{A7.87})$$

Equation (A7.86) can be written in the form

$$P_{ij}(\delta t) = \rho_{ij} \delta t + o(\delta t) \quad \text{and} \quad 1 - P_{ii}(\delta t) = \rho_i \delta t + o(\delta t), \quad (\text{A7.88})$$

where $o(\delta t)$ denotes a quantity having *an order higher than that of δt* , i. e.

$$\lim_{\delta t \downarrow 0} \frac{o(\delta t)}{\delta t} = 0. \quad (\text{A7.89})$$

Considering for any $t \geq 0$ and $\delta t > 0$

$$P_{ij}(\delta t) = \Pr\{\xi(t + \delta t) = Z_j \mid \xi(t) = Z_i\},$$

the following useful interpretation for ρ_{ij} and ρ_i can be obtained for arbitrary t and $\delta t \downarrow 0$

$$\begin{aligned} \Pr\{\text{jump from } Z_i \text{ to } Z_j \text{ in } (t, t + \delta t) \mid \xi(t) = Z_i\} &= \rho_{ij} \delta t + o(\delta t) \\ \Pr\{\text{leave } Z_i \text{ in } (t, t + \delta t) \mid \xi(t) = Z_i\} &= \rho_i \delta t + o(\delta t). \end{aligned} \quad (\text{A7.90})$$

It is thus reasonable to define ρ_{ij} and ρ_i as *transition rates* (for a Markov process, ρ_{ij} plays a similar role to that of the transition probability p_{ij} for a Markov chain).

Setting $a = \delta t$ in Eq. (A7.80) yields

$$P_{ij}(t + \delta t) = \sum_{\substack{k=0 \\ k \neq j}}^m P_{ik}(t) P_{kj}(\delta t) + P_{ij}(t) P_{jj}(\delta t)$$

or

$$\frac{P_{ij}(t + \delta t) - P_{ij}(t)}{\delta t} = \sum_{\substack{k=0 \\ k \neq j}}^m P_{ik}(t) \frac{P_{kj}(\delta t)}{\delta t} + P_{ij}(t) \frac{P_{jj}(\delta t) - 1}{\delta t},$$

and then, taking into account Eq. (A7.86), it follows that

$$\dot{P}_{ij}(t) = -P_{ij}(t)\rho_j + \sum_{\substack{k=0 \\ k \neq j}}^m P_{ik}(t)\rho_{kj}, \quad t > 0, i, j \in \{0, \dots, m\}. \quad (A7.91)$$

Equations (A7.91) are the *Kolmogorov's forward equations*. With initial conditions $P_{ij}(0) = \delta_{ij}$ as in Eq. (A7.85), they have a *unique solution* which satisfies Eq. (A7.81). In other words, the transition rates according to Eq. (A7.86) or Eq. (A7.90) *uniquely determine* the transition probabilities $P_{ij}(t)$. Setting $a = \delta t$ in Eq. (A7.80) and using $P_{ij}(t + \delta t) = \sum_{k \neq i} P_{ik}(\delta t) P_{kj}(t) + P_{ii}(\delta t) P_{ij}(t)$, $P_{ij}(t)$ also satisfy the *Kolmogorov's backward equations*

$$\dot{P}_{ij}(t) = -\rho_i P_{ij}(t) + \sum_{\substack{k=0 \\ k \neq i}}^m \rho_{ik} P_{kj}(t), \quad t > 0, i, j \in \{0, \dots, m\}, \quad (A7.92)$$

Equations (A7.91), (A7.92) can be written in matrix form $\dot{\mathbf{P}}(t) = \mathbf{P}(t)\mathbf{\Lambda}$ & $\dot{\mathbf{P}}(t) = \mathbf{\Lambda}\mathbf{P}(t)$ yielding, with $\mathbf{P}(0) = \mathbf{I}$ (Eq. (A7.85)), the (formal) solution $\mathbf{P}(t) = e^{\mathbf{\Lambda}t}$ ($\mathbf{\Lambda} = \|\rho_{ij}\|$).

The following description of the time-homogeneous Markov process, with initial distribution $P_i(0)$ and transition rates ρ_{ij} , $i, j \in \{0, \dots, m\}$, provides a better insight into the structure of a Markov process as a pure jump process (Fig. A7.10, [A7.2 (1985)]); it is the basis for investigations of Markov processes by means of integral equations (Section A7.5.3.2), and is the motivation for the introduction of semi-Markov processes (Section A7.6).

Let ξ_0, ξ_1, \dots be a sequence of random variables taking values in $\{Z_0, \dots, Z_m\}$ denoting the states *successively occupied* and η_0, η_1, \dots a sequence of positive random variables denoting the *stay times between two consecutive state transitions*. Define

$$p_{ij} = \frac{\rho_{ij}}{\rho_i}, \quad i \neq j \quad \text{and} \quad p_{ii} \equiv 0, \quad i, j \in \{0, \dots, m\}, \quad (A7.93)$$

(see the footnote on p. 487 for a discussion on $p_{ii} \equiv 0$). Assume furthermore that

$$\Pr\{\xi_0 = Z_i\} = P_i(0), \quad i = 0, \dots, m, \quad (A7.94)$$

and, for $n = 0, 1, 2, \dots$, arbitrary $i, j, i_0, \dots, i_{n-1} \in \{0, \dots, m\}$, and arbitrary $x, x_0, \dots, x_{n-1} > 0$,

$$\begin{aligned} & \Pr \{ (\xi_{n+1} = Z_j \cap \eta_n \leq x) \mid (\xi_n = Z_i \cap \eta_{n-1} = x_{n-1} \cap \dots \cap \xi_1 = Z_{i_1} \cap \eta_0 = x_0 \cap \xi_0 = Z_{i_0}) \} \\ & = \Pr \{ (\xi_{n+1} = Z_j \cap \eta_n \leq x) \mid \xi_n = Z_i \} = Q_{ij}(x) = \mathcal{P}_{ij} F_{ij}(x) = \mathcal{P}_{ij} (1 - e^{-\rho_i x}). \end{aligned} \tag{A7.95}$$

In Eq.(A7.95) (as well as in Eq. (A7.158)),

Z_j is the next state visited after Z_i ; this is not the case in Eq. (A7.77), see also the remark to Eq. (A7.106).

$Q_{ij}(x)$ is thus defined *only* for $j \neq i$ ($Q_{ii}(x) \equiv 0$). For Eq. (A7.95), it holds that

$$\begin{aligned} \mathcal{P}_{ij} &= \Pr \{ \xi_{n+1} = Z_j \mid \xi_n = Z_i \}, \quad \text{with } \mathcal{P}_{ii} \equiv 0, \\ F_{ij}(x) &= \Pr \{ \eta_n \leq x \mid (\xi_n = Z_i \cap \xi_{n+1} = Z_j) \}, \end{aligned} \tag{A7.96}$$

and the last part of Eq. (A7.95) is a consequence of the *memoryless property* of the time-homogeneous Markov process (see also Eq. (A7.102)). From these considerations it follows that ξ_0, ξ_1, \dots is a *Markov chain* with *initial distribution*

$$\mathcal{P}_i(0) = \Pr \{ \xi_0 = Z_i \}$$

and *transition probabilities* \mathcal{P}_{ij} , embedded in the original process. $Q_{ij}(x)$ is a *semi-Markov transition probability* and will as such be discussed in Section A7.6. Now, define (see e.g. Fig. A7.10)

$$\begin{aligned} S_0 &= 0, \quad S_n = \eta_0 + \dots + \eta_{n-1}, \quad n = 1, 2, \dots, \\ \xi(t) &= \xi_{n-1} \quad \text{for } S_{n-1} \leq t < S_n, \quad n = 1, 2, \dots \end{aligned} \tag{A7.97}$$

From Eq. (A7.97) and the *memoryless property* of the exponential distribution (Eq.(A6.87)) it follows that $\xi(t), t \geq 0$ is a *Markov process* with initial distribution

$$P_i(0) = \Pr \{ \xi(0) = Z_i \},$$

and *transition rates*

$$\begin{aligned} \rho_{ij} &= \lim_{\delta t \downarrow 0} \frac{1}{\delta t} \Pr \{ \text{jump from } Z_i \text{ to } Z_j \text{ in } (t, t + \delta t] \mid \xi(t) = Z_i \}, \quad j \neq i, \\ \rho_i &= \lim_{\delta t \downarrow 0} \frac{1}{\delta t} \Pr \{ \text{leave } Z_i \text{ in } (t, t + \delta t] \mid \xi(t) = Z_i \} = \sum_{\substack{j=0 \\ j \neq i}}^m \rho_{ij}. \end{aligned} \tag{A7.98}$$

The evolution of a *time-homogeneous Markov process* with transition rates ρ_{ij} and ρ_i can thus be described in the following way [A7.2 (1974 ETH, 1985)]:

If at $t=0$ the process enters the state Z_i , i.e. $\xi_0 = Z_i$, the next state to be entered, say Z_j ($j \neq i$) is selected according to the probability $\mathcal{P}_{ij} \geq 0$ ($\mathcal{P}_{ii} \equiv 0$), and the stay (sojourn) time in Z_i is a random variable η_0 with distribution function

$$\Pr \{ \eta_0 \leq x \mid (\xi_0 = Z_i \cap \xi_1 = Z_j) \} = 1 - e^{-\rho_i x}, \quad x > 0;$$

as the process enters Z_j , the next state to be entered, say Z_k ($k \neq j$), will be selected with probability $p_{jk} \geq 0$ ($p_{jj} \equiv 0$) and the stay (sojourn) time η_1 in Z_j will be distributed according to

$$\Pr\{\eta_1 \leq x \mid (\xi_n = Z_j \cap \xi_2 = Z_k)\} = 1 - e^{-\rho_j x}, \quad x > 0,$$

etc.

The sequence $\xi_n, n = 0, 1, \dots$ of the states successively occupied by the process is that of the Markov chain embedded in $\xi(t)$, the so called *embedded Markov chain*. The random variable η_n is the stay (sojourn) time of the process in the state defined by ξ_n . From the above description it becomes clear that every state $Z_i, i = 0, \dots, m$, is a *regeneration state*.

In practical applications, the following procedure can be used to find the quantities $Q_{ij}(x), p_{ij}$ & $F_{ij}(x)$ in Eq.(A7.95) for time-homogeneous Markov processes and in Eqs.(A7.158) & (A7.161) for semi-Markov processes [A7.2 (1985)]:

If the process enters the state Z_i at an arbitrary time, say at $t=0$, then a set of independent random times $\tau_{ij} > 0, j \neq i$, begin (τ_{ij} is the stay (sojourn) time in Z_i with the next jump to Z_j); the process will then jump to Z_j at the time x if $\tau_{ij}=x$ and $\tau_{ik} > \tau_{ij}$ for (all) $k \neq i, j$ ($i, j, k \in \{0, \dots, m\}$).

In this interpretation, the quantities $Q_{ij}(x), p_{ij}$, and $F_{ij}(x)$ are given by

$$Q_{ij}(x) = \Pr\{\tau_{ij} \leq x \cap \tau_{ik} > \tau_{ij}, k \neq i, j\}, \quad j \neq i, x > 0, Q_{ij}(x) = 0 \text{ for } x \leq 0, \quad (\text{A7.99})$$

$$p_{ij} = \Pr\{\tau_{ik} > \tau_{ij}, k \neq i, j\} = Q_{ij}(\infty), \quad p_{ii} \equiv 0, \quad (\text{A7.100})$$

$$F_{ij}(x) = \Pr\{\tau_{ij} \leq x \mid \tau_{ik} > \tau_{ij}, k \neq i, j\}, \quad j \neq i, x > 0, F_{ij}(x) = 0 \text{ for } x \leq 0. \quad (\text{A7.101})$$

Assuming for the time-homogeneous Markov process (memoryless property)

$$\Pr\{\tau_{ij} \leq x\} = 1 - e^{-\rho_{ij} x}, \quad j \neq i, x > 0,$$

it follows that (as for Eq. (A7.95)),

$$Q_{ij}(x) = \int_0^x \rho_{ij} e^{-\rho_{ij} y} \prod_{\substack{k=0 \\ k \neq i, j}}^m e^{-\rho_{ik} y} dy = \frac{\rho_{ij}}{\rho_i} (1 - e^{-\rho_i x}), \quad j \neq i, x > 0, \\ Q_{ij}(x) = 0 \text{ for } x \leq 0, \quad (\text{A7.102})$$

$$p_{ij} = \frac{\rho_{ij}}{\rho_i} = Q_{ij}(\infty), \quad j \neq i, \quad p_{ii} \equiv 0, \quad \rho_i = \sum_{\substack{j=0 \\ j \neq i}}^m \rho_{ij}, \quad \sum_{\substack{j=0 \\ j \neq i}}^m p_{ij} = 1, \quad (\text{A7.103})$$

$$F_{ij}(x) = 1 - e^{-\rho_i x}, \quad j \neq i, x > 0, F_{ij}(x) = 0 \text{ for } x \leq 0. \quad (\text{A7.104})$$

It should be emphasized that due to the *memoryless property* of the time-homogeneous Markov process, there is no difference whether at $t=0$ the process enters Z_i or it is already there. However, this is *not true* for semi-Markov processes (Eq. A7.158)).

Quite generally,

a repairable system can be described by a time-homogeneous Markov process if and only if all random variables occurring (failure-free, repair, wait, travel times, etc.) are independent and exponentially distributed.

If some times are Erlang distributed (Appendix A6.10.3), the time evolution can be described by a time-homog. Markov process with supplementary states (Fig. 6.6).

A powerful tool when investigating time-homogeneous Markov processes is the *diagram of transition probabilities* in $(t, t + \delta t]$, where $\delta t \downarrow 0$ and t is an *arbitrary time point* (e.g. $t=0$). This diagram is a directed graph with nodes labeled by states $Z_i, i = 0, \dots, m$, and arcs labeled by transition probabilities $P_{ij}(\delta t)$, where terms of order $o(\delta t)$ are omitted. It is related to the *state transition diagram* of the system involved, take care of particular assumptions (such as repair priority, change of failure or repair rates at a state change, etc.), and has often more than 2^n states, if n elements in the reliability block diagram are involved (Fig. A7.6, Section 6.7.1). Taking into account Eq. (A7.99), it follows that for $\delta t \rightarrow 0$

$$\begin{aligned} \Pr\{(\xi(\delta t) = Z_j \cap \text{only one jump occurs in } (0, \delta t]) \mid \xi(0) = Z_i\} \\ = (1 - e^{-\rho_{ij}\delta t}) \prod_{k=0, k \neq i, j}^m e^{-\rho_{ik}\delta t} = \rho_{ij}\delta t + o(\delta t), \end{aligned} \quad (A7.105)$$

and

$$\Pr\{(\xi(\delta t) = Z_j \cap \text{more than 1 jump in } (0, \delta t]) \mid \xi(0) = Z_i\} = o(\delta t). \quad (A7.106)$$

From this,

$$P_{ij}(\delta t) = \rho_{ij}\delta t + o(\delta t), \quad j \neq i \quad \text{and} \quad P_{ii}(\delta t) = 1 - \rho_i\delta t + o(\delta t),$$

as with Eq. (A7.88). Although for $\delta t \rightarrow 0$ it holds that $P_{ij}(\delta t) = Q_{ij}(\delta t) = \rho_{ij}\delta t$, $P_{ij}(\delta t)$ per Eq. (A7.79) and $Q_{ij}(\delta t)$ per Eq. (A7.95) are *basically different*. With

$Q_{ij}(x), Z_j$ is the *next state visited* after Z_i , this is *not the case* for $P_{ij}(x)$.⁺⁾

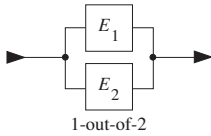
Examples A7.3 to A7.5 give the diagram of transition probabilities in $(t, t + \delta t]$ for some typical structures for reliability applications. The states in which the system is *down* are *gray*. In state Z_0 all elements are up (operating or in reserve).⁺⁺⁾

Example A7.3

Figure A7.4 shows several possibilities for a *1-out-of-2 redundancy*. The difference with respect to the number of repair crews appears when leaving states Z_2 for case a) and Z_3 for cases b) and c); cases b) and c) are identical when two repair crews are available.

⁺⁾ Note also that $\rho_{ii} = 0$ refers to the embedded Markov chain only, and does not imply $\rho_{ii} = 0$ ($\rho_{ii}\delta t = 1 - \rho_i\delta t$, see e.g. Figs. A7.6 & A7.8).

⁺⁺⁾ The memoryless property, characterizing the time-homogeneous Markov processes, is satisfied in all diagrams of Fig. A7.4 and in all similar diagrams given in this book. Assuming, for instance, that at a given time t the system of Fig. A7.4b left is in state Z_4 , development after t is independent of how many times before t the system has oscillate e.g. between Z_2, Z_0 or Z_2, Z_0, Z_1, Z_3 . *Necessary and sufficient* for a Markov process is that all stay times are *exponentially distributed*.



Distribution of failure-free times

- operating state: $F(t) = 1 - e^{-\lambda t}$
- reserve state: $F(t) = 1 - e^{-\lambda_r t}$

Distribution of repair time: $G(t) = 1 - e^{-\mu t}$

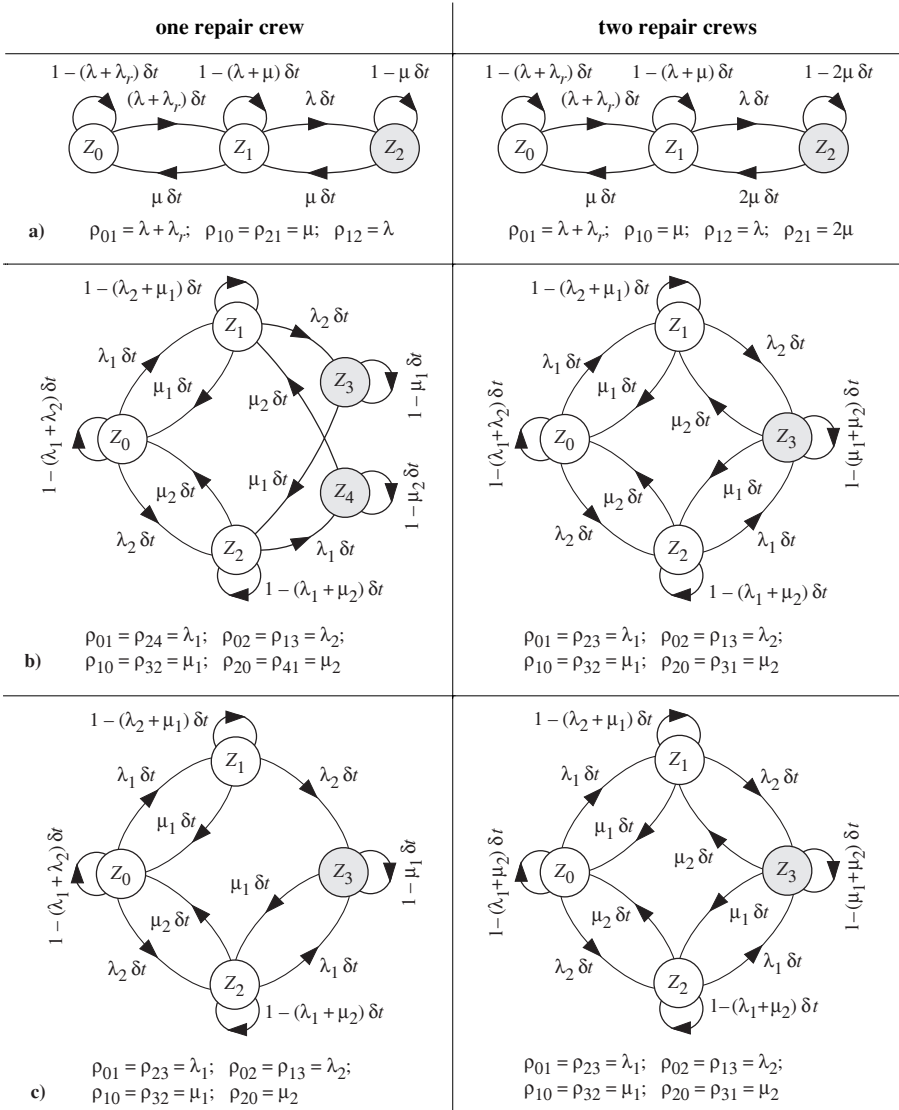


Figure A7.4 Diagram of transition probabilities in $(t, t+\delta t]$ for a *repairable 1-out-of-2 redundancy* (constant failure rates λ, λ_r and repair rate μ): **a)** Warm redundancy with $E_1 = E_2$ ($\lambda_r = \lambda \rightarrow$ active, $\lambda_r = 0 \rightarrow$ standby); **b)** Active redundancy, $E_1 \neq E_2$, left with *repair as per first-in first-out*; **c)** Active redundancy, $E_1 \neq E_2$, left with *repair priority on E_1* (ideal failure detection and switch, Z_2 for a), Z_3, Z_4 down states, t arbitrary, $\delta t \downarrow 0$, Markov proc.; see Tables 6.6, 6.9, 6.10 for results)

Example A7.4

Figure A7.5 shows two cases of a *k-out-of-n active redundancy* with two repair crews. In the first case, the system operates up to the failure of all elements (with reduced performance from state Z_{n-k+1}). In the second case no further failures can occur when the system is down.

Example A7.5

Figure A7.6 shows a *series-parallel structure* consisting of the series connection (in the reliability sense) of a 1-out-of-2 active redundancy, with elements $E_2=E_3=E$ and a switching element E_1 . The system has only one repair crew. Since one of the redundant elements E_2 or E_3 can be down without having a *system failure*, in cases a) and b) the repair of element E_1 is given *first priority*. This means that if a failure of E_1 occurs during a repair of E_2 or E_3 , the repair is stopped and E_1 will be repaired. In cases c) and d) the *repair priority* on E_1 has been dropped.

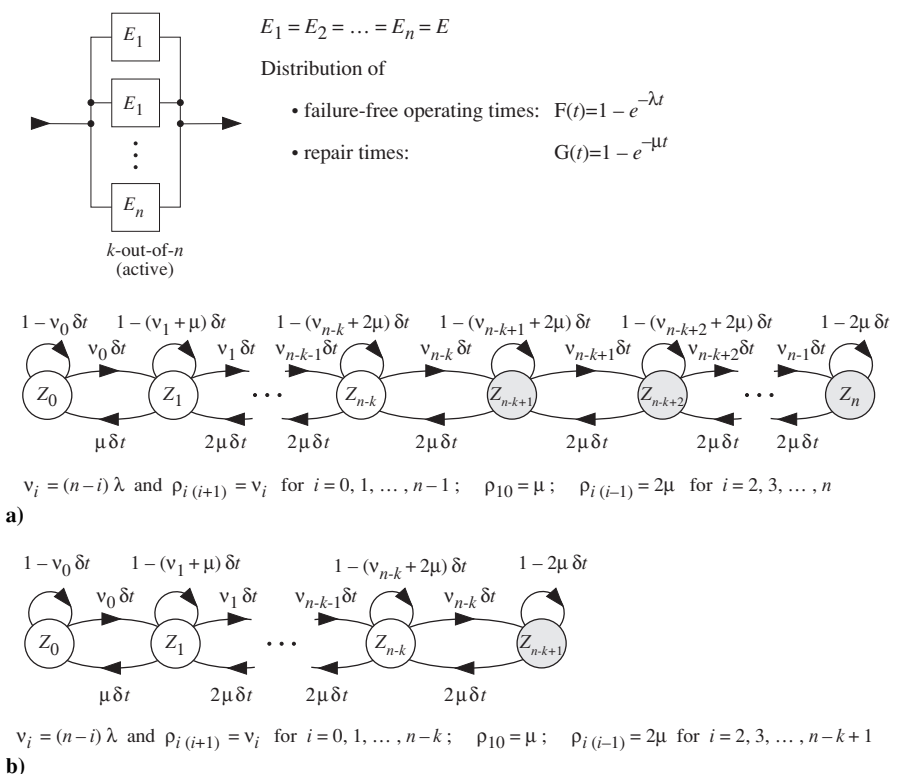
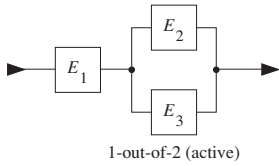


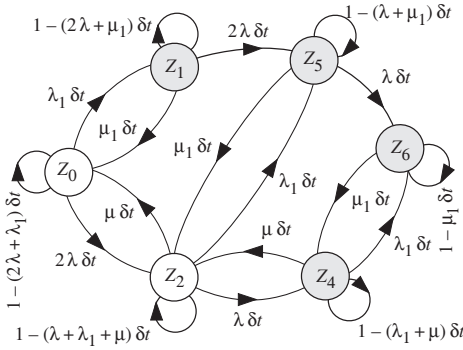
Figure A7.5 Diagram of transition probabilities in $(t, t + \delta t]$ for a *repairable k-out-of-n active redundancy* with *two repair crews* (constant failure rate λ and constant repair rate μ): **a)** The system operates up to the failure of the last element; **b)** No further failures at system down (system up if at least k elements are operating, ideal failure detection and switch, Z_{n-k+1}, \dots, Z_n down states, t arbitrary, $\delta t \downarrow 0$, Markov process; see Section 6.5 for results)



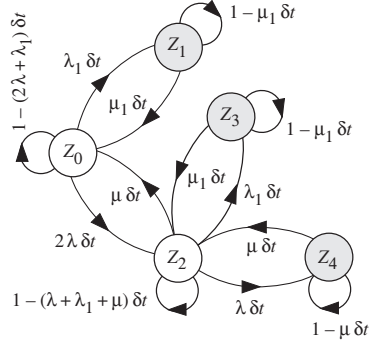
$$E_2 = E_3 = E$$

Distribution of

- failure-free times: $F(t) = 1 - e^{-\lambda t}$ for E , $F(t) = 1 - e^{-\lambda_1 t}$ for E_1
- repair times: $G(t) = 1 - e^{-\mu t}$ for E , $G(t) = 1 - e^{-\mu_1 t}$ for E_1



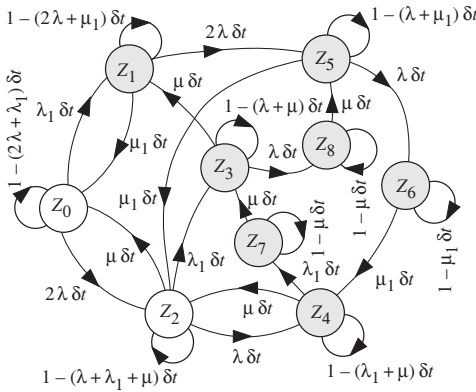
$$\begin{aligned} \rho_{01} = \rho_{25} = \rho_{46} = \lambda_1; \quad \rho_{02} = \rho_{15} = 2\lambda; \quad \rho_{24} = \lambda; \\ \rho_{10} = \rho_{52} = \rho_{64} = \mu_1; \quad \rho_{20} = \rho_{42} = \mu; \quad \rho_{56} = \lambda \end{aligned}$$



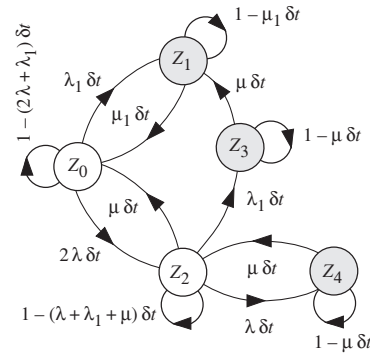
$$\begin{aligned} \rho_{01} = \rho_{23} = \lambda_1; \quad \rho_{02} = 2\lambda; \quad \rho_{24} = \lambda; \\ \rho_{10} = \rho_{32} = \mu_1; \quad \rho_{20} = \rho_{42} = \mu \end{aligned}$$

a) Repair priority on E_1

b) As a), but no further failures at system down



$$\begin{aligned} \rho_{01} = \rho_{23} = \rho_{47} = \lambda_1; \quad \rho_{02} = \rho_{15} = 2\lambda; \quad \rho_{10} = \rho_{52} = \rho_{64} = \mu_1; \\ \rho_{20} = \rho_{31} = \rho_{42} = \rho_{73} = \rho_{85} = \mu; \quad \rho_{24} = \rho_{38} = \rho_{56} = \lambda \end{aligned}$$



$$\begin{aligned} \rho_{01} = \rho_{23} = \lambda_1; \quad \rho_{02} = 2\lambda; \quad \rho_{24} = \lambda; \\ \rho_{10} = \mu_1; \quad \rho_{20} = \rho_{31} = \rho_{42} = \mu \end{aligned}$$

c) No repair priority (repair as per first-in first-out, yielding 16 states for $E_1 \neq E_2$)

d) As c), but no further failures at system down

Figure A7.6 Diagram of transition probabilities in $(t, t + \delta t]$ for a repairable series-parallel structure with $E_2 = E_3 = E$ and one repair crew: **a)** Repair priority on E_1 and system operates up to the failure of the last element; **b)** Repair priority on E_1 and at system failure no further failures can occur; **c)** & **d)** as **a)** & **b)**, but with repair as per first-in first-out (const. failure & repair rates $\lambda, \lambda_1, \mu, \mu_1$, ideal failure detection & switch, $Z_1, Z_3 - Z_8$ down states, t arbitrary, $\delta t \downarrow 0$, Markov process)

A7.5.3 State Probabilities and Stay Times (Sojourn Times) in a Given Class of States

In reliability theory, two important quantities are the *state probabilities* and the distribution function of the *stay (sojourn) times* in the set of system up states. The state probabilities allow calculation of the *point availability*. The *reliability function* can be obtained from the distribution function of the stay time in the set of system up states. Furthermore, a combination of these quantities allows, for time-homogeneous Markov processes, a simple calculation of the *interval reliability*.⁺⁾

In such analyses, it is useful to partition the system state space into two complementary sets U and \bar{U}

$$\begin{aligned}
 U &= \text{set of the } \textit{system up states} \text{ (up states at system level)} \\
 \bar{U} &= \text{set of the } \textit{system down states} \text{ (down states at system level).} \tag{A7.107}
 \end{aligned}$$

Partition of the state space in more than two classes is possible, see e. g. [A7.28].

Calculation of state probabilities and stay (sojourn) times can be carried out for Markov processes using the method of differential equations or of integral equations.

A7.5.3.1 Method of Differential Equations

The *method of differential equations* is the classical one used in investigating time-homogeneous Markov processes, and is based on the *diagram of transition probabilities in $(t, t+\delta t)$* . Consider a time-homogeneous Markov process $\xi(t)$ with arbitrary initial distribution $P_j(0) = \Pr\{\xi(0) = Z_j\}$ and transition rates ρ_{ij} and ρ_i (Eq. (A7.98)). The state probabilities defined by Eq. (A7.83)

$$P_j(t) = \Pr\{\xi(t) = Z_j\}, \quad j = 0, \dots, m, \quad t > 0,$$

satisfy the system of differential equations

$$\dot{P}_j(t) = -\rho_j P_j(t) + \sum_{\substack{i=0 \\ i \neq j}}^m P_i(t) \rho_{ij}, \quad j = 0, \dots, m, \quad t > 0, \quad \rho_j = \sum_{\substack{i=0 \\ i \neq j}}^m \rho_{ji}. \tag{A7.108}$$

Equation (A7.108) uses the *memoryless property* of the time-homogeneous Markov process & Eq. (A7.90), and follows from $P_j(t+\delta t) = P_j(t)(1-\rho_j\delta t) + \sum_{i \neq j} P_i(t)\rho_{ij}\delta t$, see also Example A7.6). The *point availability* $PA_S(t)$, for arbitrary initial conditions at $t=0$, follows then from⁺⁾

$$PA_S(t) = \Pr\{\xi(t) \in U\} = \sum_{Z_j \in U} P_j(t), \quad t > 0. \tag{A7.109}$$

⁺⁾ Reliability figures at system level will have indices S_i (e.g. $MTTF_{S_i}$), where S stands for system and i is the state entered at $t=0$ (system refers in this book, and often in practical applications, to the highest integration level of the item considered, $i=0$ refers in this book to item new).

In reliability analysis, particular *initial conditions* (Eq.(A7.82)) are often of interest. Assuming

$$P_i(0)=1 \quad \text{and} \quad P_j(0)=0 \quad \text{for} \quad j \neq i, \tag{A7.110}$$

i. e., that the system is in Z_i at $t=0$, the state probabilities $P_j(t)$, obtained as solution of Eq. (A7.108) with *initial conditions* per Eq. (A7.110), become the *transition probabilities* $P_{ij}(t)$ defined by Eqs. (A7.78) & (A7.79) ⁺⁾

$$P_{ij}(t) \equiv P_j(t), \quad i, j \in \{0, \dots, m\}. \tag{A7.111}$$

The *point availability*, designated with $PA_{S_i}(t)$ (footnote on p.491) is then given by

$$PA_{S_i}(t) = \Pr\{\xi(t) \in U \mid \xi(0) = Z_i\} = \sum_{Z_j \in U} P_{ij}(t), \quad \begin{matrix} i=0, \dots, m, t > 0, \\ PA_{S_i}(0) = 1 \text{ for } Z_i \in U. \end{matrix} \tag{A7.112}$$

$PA_{S_i}(t)$ is the probability that the system is in one of the up states at t , given it was in Z_i at $t = 0$; thus, $PA_{S_i}(0)=1$ holds only for $Z_i \in U$. Example A 7.6 illustrate calculation of the point-availability for a 1-out-of-2 active redundancy.

Example A7.6

Assume a 1-out-of-2 active redundancy, consisting of 2 identical elements $E_1 = E_2 = E$ with constant failure rate λ and repair rate μ , and only one repair crew. Give the state probabilities of the involved Markov process (E_1 and E_2 are new at $t = 0$).

Solution

Figure A7.7 shows the diagram of transition probabilities in $(t, t + \delta t]$ for the investigation of the point availability. Because of the *memoryless property* of the involved Markov Process, Fig A7.7 and Eqs. (A7.83) & (A7.90) lead to the following system of *difference equations* (by omitting the terms in $o(\delta t)$, as per Eq. (A7.89))

$$\begin{aligned} P_0(t + \delta t) &= P_0(t)(1 - 2\lambda \delta t) + P_1(t)\mu \delta t \\ P_1(t + \delta t) &= P_1(t)(1 - (\lambda + \mu)\delta t) + P_0(t)2\lambda \delta t + P_2(t)\mu \delta t \\ P_2(t + \delta t) &= P_2(t)(1 - \mu \delta t) + P_1(t)\lambda \delta t, \end{aligned}$$

and then, as $\delta t \downarrow 0$,

$$\begin{aligned} \dot{P}_0(t) &= -2\lambda P_0(t) + \mu P_1(t) \\ \dot{P}_1(t) &= -(\lambda + \mu)P_1(t) + 2\lambda P_0(t) + \mu P_2(t) \\ \dot{P}_2(t) &= -\mu P_2(t) + \lambda P_1(t). \end{aligned} \tag{A7.113}$$

The system of *differential equations* (A7.113) also follows from Eq. (A7.108) with the ρ_{ij} from Fig. A7.7. The solution for given initial conditions at $t = 0$, e. g. $P_0(0) = 1, P_1(0) = P_2(0) = 0$, leads to state probabilities $P_0(t), P_1(t)$, and $P_2(t)$, and to the point availability according to Eqs. (A7.111) & (A7.112) with $i = 0$ (see pp. 197-198 and Example A7.9 (p. 503) for a detailed solution, Eq. (6.88) for an approximation, and Table 6.6 (p. 201) for a summary of important results).

^{+) Enters Z_i will be necessary for semi-Markov processes, often $Z_i = Z_0$ denoting *all elements new*.}

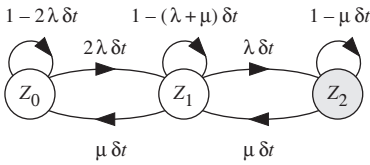


Figure A7.7 Diagram of the transition probabilities in $(t, t + \delta t]$ for availability calculation of a *repairable 1-out-of-2 active redundancy* with $E_1 = E_2 = E$, constant failure rate λ , constant repair rate μ , and *one repair crew* (ideal failure detection and switch, Z_2 down state, t arbitrary, $\delta t \downarrow 0$, Markov process with $\rho_{01} = 2\lambda, \rho_{10} = \mu, \rho_{12} = \lambda, \rho_{21} = \mu, \rho_0 = 2\lambda, \rho_1 = \lambda + \mu, \rho_2 = \mu$)

A further important quantity for reliability analyses is the *reliability function* $R_S(t)$; i.e., the probability of no system failure (no failure at system level) in $(0, t]$. $R_S(t)$ can be calculated using the method of differential equations if all states in \bar{U} are declared to be *absorbing states*. This means that the process will never leave Z_k if it jumps into a state $Z_k \in \bar{U}$. It is not difficult to see that in this case, the events

- { first system failure occurs before t }
- and
- { system is in one of the states \bar{U} at t }

are equivalent, so that the probability to be in one of the states in U is the required reliability function, i.e., the probability that up to the time t the process has never left the set of up states U . To make this analysis rigorous, consider the *modified Markov process* $\xi'(t)$ with transition probabilities $P'_{ij}(t)$ and transition rates

$$\rho'_{ij} = \rho_{ij} \text{ if } Z_i \in U, \quad \rho'_{ij} = 0 \text{ if } Z_i \in \bar{U}, \quad \rho'_i = \sum_{j=0, i \neq j}^m \rho_{ij}. \quad (\text{A7.114})$$

The state probabilities $P'_j(t)$ of $\xi'(t)$ satisfy the following system of differential equations (see Example A7.7 for an application)

$$\dot{P}'_j(t) = -\rho'_j P'_j(t) + \sum_{j=0, i \neq j}^m P'_i(t) \rho'_{ij}, \quad j=0, \dots, m, \quad t > 0, \quad \rho'_j = \sum_{j=0, i \neq j}^m \rho'_{ij}. \quad (\text{A7.115})$$

Assuming as *initial conditions* $P'_i(0) = 1$ and $P'_j(0) = 0$ for $j \neq i$, with $Z_i \in U$, the solution of Eq. (A7.115) leads to the state probabilities $P'_j(t)$ and from these to the *transition probabilities* (as for Eq. (A7.111))

$$P'_{ij}(t) \equiv P'_j(t). \quad (\text{A7.116})$$

The *reliability function* $R_{S_i}(t)$ is then given by (footnote on p. 491)

$$R_{S_i}(t) = \Pr\{\xi(x) \in U \text{ for } 0 < x \leq t \mid \xi(0) = Z_i\} = \sum_{Z_j \in U} P'_{ij}(t), \quad \begin{matrix} Z_i \in U, t > 0, \\ R_{S_i}(0) = 1. \end{matrix} \quad (\text{A7.117})$$

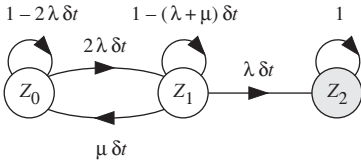


Figure A7.8 Diagram of the transition probabilities in $(t, t + \delta t]$ for the reliability function of a repairable 1-out-of-2 active redundancy with $E_1 = E_2 = E$, constant failure rate λ , constant repair rate μ , one repair crew (ideal failure detection and switch, Z_2 down state (absorbing), t arbitrary, $\delta t \downarrow 0$, Markov process (see footnote on p. 497) with $\rho_{01} = 2\lambda$, $\rho_{10} = \mu$, $\rho_{12} = \lambda$, $\rho_0 = 2\lambda$, $\rho_1 = \lambda + \mu$, $\rho_2 = 1$)

Example A7.7 illustrates the calculation of the reliability function for a 1-out-of-2 active redundancy. Finally,

the probabilities marked with ' ($P'_i(t)$) are reserved for reliability calculation, when using the method of differential equations; this to avoid confusion with the corresponding quantities for the point availability.

Equations (A7.112) and (A7.117) can be combined to determine the probability that the process is in an up state (set U) at t and does not leave the set U in the time interval $[t, t + \theta]$, given $\xi(0) = Z_i$. This quantity is the *interval reliability* $IR_{Si}(t, t + \theta)$. Due to the *memoryless property* of the involved Markov process,

$$\begin{aligned}
 IR_{Si}(t, t + \theta) &= \Pr\{\xi(x) \in U \text{ for } t \leq x \leq t + \theta \mid \xi(0) = Z_i\} \\
 &= \sum_{Z_j \in U} P_{ij}(t) \cdot R_{Sj}(\theta), \quad i = 0, \dots, m, \quad t, \theta > 0, \quad (A7.119)
 \end{aligned}$$

with $P_{ij}(t)$ as given in Eq. (A7.111) and $R_{Si}(\theta)$ per Eq. (A7.117) with $t = \theta$.

Example A7.7

Investigate the reliability function for the same case as in Example A7.6; i. e., the probability that the system has not left the states Z_0 and Z_1 up to time t .

Solution

The diagram of transition probabilities in $(t, t + \delta t]$ of Fig. A7.7 is modified as in Fig. A7.8 by making the down state Z_2 absorbing. For the state probabilities it follows that (Example A7.6)

$$\begin{aligned}
 \dot{P}'_0(t) &= -2\lambda P'_0(t) + \mu P'_1(t) \\
 \dot{P}'_1(t) &= -(\lambda + \mu)P'_1(t) + 2\lambda P'_0(t) \\
 \dot{P}'_2(t) &= \lambda P'_1(t). \quad (A7.118)
 \end{aligned}$$

The solution of Eq. (A7.118) with the given initial conditions at $t = 0$ ($P'_0(0) = 1$, $P'_1(0) = P'_2(0) = 0$) leads to the state probabilities $P'_0(t)$, $P'_1(t)$ and $P'_2(t)$, and then to the transition probabilities and to the reliability function according to Eqs. (A7.116) and (A7.117), respectively (dashed state probabilities should avoid confusion with the solution given by Eq. (A7.113); see pp. 198-199 and Example A7.9 (p. 503) for a detailed solution, Eq. (6.94) for an approximation, and Table 6.6 (p. 201) for a summary of important results).

A7.5.3.2 Method of Integral Equations

The *method of integral equations* is based on the representation of the time-homogeneous Markov process $\xi(t)$ as a pure jump process by means of ξ_n and η_n as introduced in Appendix A7.5.2 (Eq. (A7.95), Fig. A7.10). From the *memoryless property* it uses *only* the fact that jump points (in a new state) are *regeneration points* of $\xi(t)$.

The *transition probabilities* $P_{ij}(t) = \Pr\{\xi(t) = Z_j \mid \xi(0) = Z_i\}$ can be obtained by solving the following system of *integral equations*

$$P_{ij}(t) = \delta_{ij} e^{-\rho_i t} + \sum_{\substack{k=0 \\ k \neq i}}^m \int_0^t \rho_{ik} e^{-\rho_i x} P_{kj}(t-x) dx, \quad i, j \in \{0, \dots, m\}, t > 0, \quad (A7.120)$$

with $\rho_i = \sum_{j \neq i} \rho_{ij}$, $\delta_{ij} = 0$ for $j \neq i$, $\delta_{ii} = 1$, and $P_{ij}(0) = \delta_{ij}$ per Eq. (A7.85). The first term of Eq. (A7.120) only holds for $j = i$ and gives the probability that the process will *not leave* the state Z_i ($e^{-\rho_i t} = \Pr\{\tau_{ij} > t \text{ for all } j \neq i\}$). To prove the second term of Eq. (A7.120), consider that it holds

$$P_{ij}(t) = \sum_{\substack{k=0 \\ k \neq i}}^m \Pr\{\text{first jump in } Z_k \text{ at } x \text{ for } 0 < x \leq t \text{ and } \xi(x) = Z_k \\ \text{is a regeneration point} \mid \xi(0) = Z_i\}, \quad (A7.121)$$

this term gives the probability that the process will first move from Z_i to Z_k at x for $0 < x \leq t$, $k \neq i$, and take into account that occurrence of Z_k is a *regeneration point* ($\Pr\{\xi_1 = Z_k \cap \eta_0 \leq x \mid \xi_0 = Z_i\} = Q_{ik}(x) = (1 - e^{-\rho_i x}) \rho_{ik} / \rho_i$, yields $dQ_{ik}(x) / dx = \rho_{ik} e^{-\rho_i x}$ and $\Pr\{\xi(t) = Z_j \mid (\xi_0 = Z_i \cap \eta_0 = x \cap \xi_1 = Z_k)\} = P_{kj}(t-x)$). Equation (A7.121) then follow from the *theorem of total probability* (Eq. (A6.17)).

In the same way as for Eq. (A.120), it can be shown that the *reliability function* $R_{S_i}(t)$, as defined in Eq. (A7.117), satisfies the following system of *integral equations*

$$R_{S_i}(t) = e^{-\rho_i t} + \sum_{\substack{Z_j \in U \\ j \neq i}} \int_0^t \rho_{ij} e^{-\rho_i x} R_{S_j}(t-x) dx, \quad \rho_i = \sum_{\substack{j=0 \\ j \neq i}}^m \rho_{ij}, \quad Z_i \in U, t > 0, \\ R_{S_i}(0) = 1. \quad (A7.122)$$

Point availability $PA_{S_i}(t)$ and *interval reliability* $IR_{S_i}(t, t+\theta)$ are given by Eqs. (A7.112) and (A7.119), with $P_{ij}(t)$ per Eq. (A7.120); see, for instance, Eqs. (6.85) and (6.96) for a 1-out-of-2 redundancy.

Use of integral equations, as in Eq. (A7.122), for $PA_{S_i}(t)$ leads to mistakes, since $R_{S_i}(t)$ and $PA_{S_i}(t)$ describe two basically different situations (summing for $PA_{S_i}(t)$ over all states $j \neq i$ yields $PA_{S_i}(t) = 1$, as for Eq. (A7.112) with $j = 0, \dots, m$).

The systems of integral equations (A7.120) and (A7.122) can be solved using Laplace transforms. Referring to Appendix A9.7,

$$\tilde{P}_{ij}(s) = \frac{\delta_{ij}}{s + \rho_i} + \sum_{\substack{k=0 \\ k \neq i}}^m \frac{\rho_{ik}}{s + \rho_i} \tilde{P}_{kj}(s), \quad \rho_i = \sum_{\substack{j=0 \\ j \neq i}}^m \rho_{ij}, \quad i, j \in \{0, \dots, m\}, \quad (\text{A7.123})$$

and

$$\tilde{R}_{Si}(s) = \frac{1}{s + \rho_i} + \sum_{\substack{Z_j \in U \\ j \neq i}} \frac{\rho_{ij}}{s + \rho_i} \tilde{R}_{Sj}(s), \quad \rho_i = \sum_{\substack{j=0 \\ j \neq i}}^m \rho_{ij}, \quad Z_i \in U. \quad (\text{A7.124})$$

A direct advantage of the method based on integral equations appears in the calculation of $MTTF_{Si}$, i.e., of the *system mean time to failure*, provided the system is in state $Z_i \in U$ at $t = 0$. Considering Eqs. (A6.38) & (2.61), or Appendix A9.7, it follows that

$$MTTF_{Si} = \int_0^{\infty} R_{Si}(t) dt = \tilde{R}_{Si}(0). \quad (\text{A7.125})$$

Thus, according to Eq. (A7.124), $MTTF_{Si}$ satisfies the following system of algebraic equations (see Example A7.9 for an application)

$$MTTF_{Si} = \frac{1}{\rho_i} + \sum_{\substack{Z_j \in U \\ j \neq i}} \frac{\rho_{ij}}{\rho_i} MTTF_{Sj}, \quad \rho_i = \sum_{\substack{j=0 \\ j \neq i}}^m \rho_{ij}, \quad Z_i \in U. \quad (\text{A7.126})$$

A7.5.3.3 Stationary State and Asymptotic Behavior

The determination of time-dependent state probabilities or of the point availability of a system whose elements have constant failure and repair rates is still possible using differential or integral equations. However, it can become time-consuming. The situation is easier where the state probabilities are independent of time, i.e., when the process involved is *stationary* (the system of differential or integral equations reduces to a system of algebraic equations):

A time-homogeneous Markov process $\xi(t)$ with states Z_0, \dots, Z_m is stationary, if its state probabilities $P_i(t) = \Pr\{\xi(t) = Z_i\}$, $i = 0, \dots, m$ do not depend on t .

This can be seen from the following relationship

$$\Pr\{\xi(t_1) = Z_{i_1} \cap \dots \cap \xi(t_n) = Z_{i_n}\} = \Pr\{\xi(t_1) = Z_{i_1}\} P_{i_1 i_2}(t_2 - t_1) \dots P_{i_{n-1} i_n}(t_n - t_{n-1})$$

which, according to the Markov property (Eq. (A7.77)) must be valid for arbitrary $t_1 < \dots < t_n$ and $i_1, \dots, i_n \in \{0, \dots, m\}$. For any $a > 0$ this leads to

$$\Pr\{\xi(t_1) = Z_{i_1} \cap \dots \cap \xi(t_n) = Z_{i_n}\} = \Pr\{\xi(t_1 + a) = Z_{i_1} \cap \dots \cap \xi(t_n + a) = Z_{i_n}\}.$$

From $P_i(t+a) = P_i(t)$ it follows $P_i(t) = P_i(0) = P_i$, and, in particular, $\dot{P}_i(t) = 0$. Consequently, the process $\xi(t)$ is *stationary* (in *steady-state*) if and only if its initial distribution (*initial conditions* $P_i = P_i(0) = \Pr\{\xi(0) = Z_i\}$, $i = 0, \dots, m$, satisfy (Eq. (A7.108))

$$P_j \rho_j = \sum_{\substack{i=0 \\ i \neq j}}^m P_i \rho_{ij}, \quad \text{with } P_j \geq 0, \quad \sum_{j=0}^m P_j = 1, \quad \rho_j = \sum_{\substack{i=0 \\ i \neq j}}^m \rho_{ji}, \quad j = 0, \dots, m. \tag{A7.127}$$

The system of Eq. (A7.127) must be solved by replacing one (arbitrarily chosen) equation by $\sum P_j = 1$. Every solution of Eq. (A7.127) with $P_j \geq 0$, $j = 0, \dots, m$, is a *stationary initial distribution* of the Markov process. Equation (A7.127) expresses that

$$\Pr\{\text{to come out from state } Z_j\} = \Pr\{\text{to come in state } Z_j\},$$

also known as *generalized cut sets theorem* (see e. g. also Eq. (A7.152)).

A Markov process with a *finite number of states* ($m < \infty$) is *irreducible* if for every pair $i, j \in \{0, \dots, m\}$ there exists a t such that $P_{ij}(t) > 0$; i. e., if every state can be reached from every other state. It can be shown that if $P_{ij}(t_0) > 0$ for some $t_0 > 0$, then $P_{ij}(t) > 0$ for any $t > 0$. A Markov process is irreducible if and only if its *embedded Markov chain is irreducible* (Eq. (A7.75)). For an irreducible Markov process, there exist quantities $P_j > 0$, $j = 0, \dots, m$, with $P_0 + \dots + P_m = 1$, such that *independently of the initial condition* $P_i(0)$ the following holds (Markov theorem, e.g. [A6.6 (V. 1)])

$$\lim_{t \rightarrow \infty} P_j(t) = P_j > 0, \quad j = 0, \dots, m. \tag{A7.128}$$

For any $i = 0, \dots, m$ it follows then that

$$\lim_{t \rightarrow \infty} P_{ij}(t) = P_j > 0, \quad j = 0, \dots, m. \tag{A7.129}$$

The set of values P_0, \dots, P_m from Eq. (A7.128) is the *limiting distribution* of the Markov process. From Eq. (A7.129) it follows (as for Eq. (A7.76)), that for an *irreducible Markov process* the limiting distribution is the *only stationary and ergodic distribution*, i. e., the only solution of Eq. (A7.127) with $P_j > 0$, $j = 0, \dots, m < \infty$.^{*)}

Further important results follow from Eqs. (A7.174)-(A7.180). In particular,

- the initial distribution in steady-state $A_{ij}^0(x) = (1 - e^{-P_i x}) P_i \rho_{ij} / \rho_i$ (Eq. (A7.181)),
- the frequency $h_i = P_i \rho_i$, of consecutive occurrences of state Z_i (Eq. (A7.181a)),
- the relation between stationary values \mathcal{P}_i per Eqs. (A7.175) & (A7.103) for the embedded Markov chain and P_i per Eq. (A7.127) for the involved Markov process (Eq. (A7.176) with $T_i = 1/\rho_i$ per Eqs. (A7.166), (A7.165), (A7.102))

$$P_i = \frac{\mathcal{P}_i / \rho_i}{\sum_{k=0}^m \mathcal{P}_k / \rho_k}. \tag{A7.130}$$

^{*)} On the contrary, if the embedded Markov chain is *not irreducible* (Fig. A7.8), the consequence of Z_2 absorbing is that $\lim_{t \rightarrow \infty} P_2(t) = 1$ and $\lim_{t \rightarrow \infty} P_0(t) = \lim_{t \rightarrow \infty} P_1(t) = 0$ (according to Eq. (A7.127)).

From the results given by Eqs. (A7.127)-(A7.129), the *asymptotic & steady-state value* of the point availability PA_S follows as

$$\lim_{t \rightarrow \infty} PA_{S_i}(t) = PA_S = \sum_{Z_j \in U} P_j, \quad i = 0, \dots, m. \tag{A7.131}$$

For the *interval reliability*, Eq. (A7.119) holds with $P_{ij}(t)$ as per Eq. (A7.129).

If K is a subset of $\{Z_0, \dots, Z_m\}$, the Markov process is irreducible, and P_0, \dots, P_m are the limiting probabilities obtained from Eq. (A7.127) then,

$$\Pr \left\{ \lim_{t \rightarrow \infty} \frac{\text{total sojourn time in states } Z_j \in K \text{ in } (0, t]}{t} = \sum_{Z_j \in K} P_j \right\} = 1, \tag{A7.132}$$

irrespective of the initial distribution $P_0(0), \dots, P_m(0)$. From Eq. (A7.132) it follows

$$\Pr \left\{ \lim_{t \rightarrow \infty} \frac{\text{total operating time in } (0, t]}{t} = \sum_{Z_j \in U} P_j = PA_S \right\} = 1.$$

The *average availability* of the system can be expressed as (see Eq. (6.24))

$$AA_{S_i}(t) = \frac{1}{t} E[\text{total operating time in } (0, t] \mid \xi(0) = Z_i] = \frac{1}{t} \int_0^t PA_{S_i}(x) dx. \tag{A7.133}$$

The above considerations lead to (for any $Z_i \in U$)

$$\lim_{t \rightarrow \infty} AA_{S_i}(t) = AA_S = PA_S = \sum_{Z_j \in U} P_j. \tag{A7.134}$$

Expressions $\sum_k P_k$ are useful in practical applications, e.g. for *cost optimizations*.

Except for investigations on the reliability function ($R_S(t)$) (see footnote on p. 497), an *irreducible embedded Markov chain* can be assumed in reliability applications. For such cases, according to Eqs. (A7.127) and (A7.128),

asymptotic & steady-state can be used as a synonym for *stationary* (see e.g. also pp. 187-188, 472, 477, 479, 509, 514).

A7.5.4 Frequency / Duration and Reward Aspects

In some applications, it is important to consider the *frequency* with which failures at system level occur and the *mean duration* of system down time (or operating time) in *stationary state*. Also of interest is the investigation of fault tolerant systems for which a *reconfiguration* can take place after a failure, allowing continuation of operation with defined loss of performance (*reward*). Basic considerations on these aspects are given in this section. Some applications are in Section 6.8.6.

A7.5.4.1 Frequency / Duration

To introduce the concept of *frequency / duration* let us consider the one-item structure discussed in Appendix A7.3 as application of the alternating renewal process.

As in Appendix A7.3 assume an item (system) which alternates between operating state, with mean time to failure $MTTF$, and repair state, with complete renewal and mean repair time $MTTR$. In the *stationary state*, the *frequency* at which item failures f_{ud} or item repairs (restorations) f_{du} occurs is given as (Eq. (A7.60))

$$f_{ud} = f_{du} = h_{ud}(t) = h_{du}(t) = \frac{1}{MTTF + MTTR}, \quad t \geq 0. \quad (A7.135)$$

Furthermore, for the one-item structure, the *mean up time* MUT is

$$MUT = MTTF. \quad (A7.136)$$

Consequently, considering Eq. (A7.58) the basic relation

$$PA = \frac{MTTF}{MTTF + MTTR} = f_{ud} \cdot MUT, \quad \text{i. e. } MUT = PA / f_{ud}, \quad (A7.137)$$

can be established, where PA is the point availability (probability to be up) in the *stationary state*. Similarly, for the *mean failure duration* MDT one has

$$MDT = MTTR \quad (A7.138)$$

and thus

$$1 - PA = \frac{MTTR}{MTTF + MTTR} = f_{du} \cdot MDT, \quad \text{i. e. } MDT = (1 - PA) / f_{du}. \quad (A7.139)$$

Constant failure rate $\lambda = 1/MTTF$ and repair (restoration) rate $\mu = 1/MTTR$ leads to

$$PA \cdot \lambda = (1 - PA) \cdot \mu = f_{ud} = f_{du}, \quad (A7.140)$$

which expresses the *stationary property* of time-homogeneous Markov processes, as particular case of Eq. (A7.127) with $m = \{0,1\}$.

For systems of arbitrary complexity with constant failure and repair (restoration) rates, described by time-homogeneous Markov processes (Appendix A7.5.2), generalization of Eqs. (A7.135) & (A7.137) yields for the asymptotic & steady-state *system failure frequency* f_{udS} and *system mean (expected) up time* MUT_S

$$f_{udS} = \sum_{Z_j \in U, Z_i \in \bar{U}} P_j \rho_{ji} = \sum_{Z_j \in U} P_j (\sum_{Z_i \in \bar{U}} \rho_{ji}) \quad (A7.141)$$

and

$$MUT_S = (\sum_{Z_j \in U} P_j) / f_{udS} = PA_S / f_{udS}, \quad (A7.142)$$

respectively. U is the set of states considered as *up states* for f_{udS} and MUT_S calculation, \bar{U} the complement to the totality of states considered. MUT_S is the mean of the time in which the system is moving in the set of up states $Z_j \in U$ before a transition to the set of down states $Z_i \in \bar{U}$ occurs in the stationary case or for $t \rightarrow \infty$. In Eq. (A7.141), all transition rates ρ_{ji} leaving state $Z_j \in U$ toward $Z_i \in \bar{U}$ are considered (*cumulated states*). Similar results hold for semi-Markov processes.

Equations (A7.141) & (A7.142) have a great intuitive appeal: (i) Because of the memoryless property of the time-homogeneous Markov processes, the asymptotic & steady-state probability to have a failure in $(t, t+\delta t]$ is $f_{udS} \delta t$ (ii) Setting UT as up time and $v(t)$ as number of failures in $(0, t]$, $\lim_{t \rightarrow \infty} (UT/t) = PA_S$ and $\lim_{t \rightarrow \infty} (v(t)/t) = f_{udS}$, lead to $UT/v(t) \rightarrow MUT_S = PA_S / f_{udS}$ for $t \rightarrow \infty$.

Similar results hold for the *system repair* (restoration) frequency f_{duS} and *system mean* (expected) *down time* MDT_S (mean repair (restoration) time at system level)

$$f_{duS} = \sum_{Z_i \in \bar{U}, Z_j \in U} P_i \rho_{ij} = \sum_{Z_i \in \bar{U}} P_i \left(\sum_{Z_j \in U} \rho_{ij} \right) \quad (\text{A7.143})$$

and

$$MDT_S = \left(\sum_{Z_i \in \bar{U}} P_i \right) / f_{duS} = (1 - PA_S) / f_{duS}. \quad (\text{A7.144})$$

respectively.

f_{duS} is the *system failure intensity* $z_S(t) = z_S$ as per Eq. (A7.230) in steady-state or for $t \rightarrow \infty$. Considering that every failure at system level is followed by a repair (restoration) at system level, one has $f_{udS} = f_{duS}$ and thus (see also Eq. (A7.60))

$$f_{duS} = f_{udS} = z_S = \sum_{Z_i \in \bar{U}, Z_j \in U} P_i \rho_{ij} = \sum_{Z_j \in U, Z_i \in \bar{U}} P_j \rho_{ji} = 1 / (MUT_S + MDT_S). \quad (\text{A7.145})$$

Equations (A7.142), (A7.144), and (A7.145) yield to the following important relation between MDT_S and MUT_S (see also Eqs. (A7.137) & A7.139))

$$MDT_S = MUT_S (1 - PA_S) / PA_S. \quad (\text{A7.146})$$

Equation (A7.146) satisfy $PA_S = MUT_S / (MUT_S + MDT_S)$ as per Eqs. (6.48) & (6.49).

Computation of the frequency of failures (f_{duS}) and mean failure duration (MDT_S) based on *fault tree* and corresponding *minimal cut-sets* (Sections 2.3.4, 2.6) is often used in power systems [6.4, 6.22], where f_f , d_f and P_f appear for f_{duS} , MDT_S , and $1 - PA_S$. The central part of Eq. (A7.145) is known as *theorem of cuts*.

Although appealing, $\sum P_j MTTF_{Sj}$, with $MTTF_{Sj}$ from Eq. (A7.126) & P_j from Eq. (A7.127), can't be used to compute MUT_S ,

Eq. (A7.127) refers to a steady-state, not compatible with Eq. (A7.126). However, $MUT_S \approx P_0 MTTF_{S0} \approx MTTF_{S0}$ can often be used in practical applications, see Eq. (6.95), Example 6.29 on p. 279 & the numerical results in Example 6.27 on p. 270.

A7.5.4.2 Reward

Complex fault tolerant systems have been conceived to be able to reconfigure themselves at the occurrence of a failure and continue operation, if necessary with reduced performance. Such a feature is important for many systems, e.g. production, information, and power systems, which should assure continuation of operation

after a system failure. Besides *fail-safe* aspects, investigation of such systems is based on the superposition of *performance behavior* (often assumed deterministic) and stochastic *dependability behavior* (including reliability, maintainability, availability, and logistic support). Considering that P_i is the asymptotic & steady-state probability to be in state Z_i (Eqs. (A7.83), (A7.128), (A7.127)), giving also the *expected percentage of time* the system stays at the performance level specified by Z_i (Eq. (A7.132)), a straightforward possibility is to assign to every state Z_i of the dependability model a *reward rate* $0 \leq r_i \leq 1$ which take care of the performance reduction in the state considered. From this, the *mean (expected) reward rate* $MIR_S(t)$ can be calculated in stationary state as

$$MIR_S = \sum_{i=0}^m r_i P_i. \tag{A7.147}$$

Thereby, $r_i=0$ for down states and $r_i=1$ for up states with 100% performance. The *mean (expected) accumulated reward* $MAR_S(t)$ follows for the stationary state as

$$MAR_S(t) = \int_0^t MIR_S(x) dx = MIR_S \cdot t. \tag{A7.148}$$

$MAR_S(t)$ gives the reward over $(0, t]$ on the basis of the stay (sojourn) times in each state. Other metrics are possible, e.g. *reward impulses* at state transition, expected ratio of *busy channels* etc. (see e.g. [6.19(1995), 6.26, 6.34]). Of less importance for practical applications is the use of reward aspects for $R_{S_i}(t)$ or $MTTF_{S_i}$. For the purpose of this book, application in Section 6.8.6.4 will be limited to Eq. (A7.147).

A7.5.5 Birth and Death Process

A birth and death process is a Markov process characterized by the property that transitions from a state Z_i can only occur to state Z_{i+1} (birth) or Z_{i-1} (death). In the time-homogeneous case, it is used to investigate *k-out-of-n redundancies* with identical elements and *constant failure & repair rates* during the stay (sojourn) time in any given state (not necessarily at state transitions, e.g. load sharing). The diagram of transition probabilities in $(t, t + \delta t]$ is given in Fig. A7.9. v_i and θ_i are the transition rates from state Z_i to Z_{i+1} and Z_i to Z_{i-1} , respectively (transitions outside

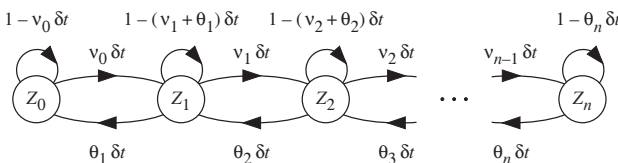


Figure A7.9 Diagram of transition probabilities in $(t, t + \delta t]$ for a *birth and death process* with $(n + 1) < \infty$ states (t arbitrary, $\delta t \downarrow 0$, Markov process)

neighboring states can occur in $(t, t + \delta t]$ only with probability $o(\delta t)$. The system of differential equations describing the *birth and death process* given in Fig. A7.9 is

$$\begin{aligned} \dot{P}_j(t) &= -(v_j + \theta_j)P_j(t) + v_{j-1}P_{j-1}(t) + \theta_{j+1}P_{j+1}(t) \\ &\text{with } \theta_0 = v_{-1} = v_n = \theta_{n+1} = 0, \quad j = 0, \dots, n < \infty. \end{aligned} \quad (\text{A7.149})$$

The conditions $v_j > 0$ ($j = 0, \dots, n-1$) and $\theta_j > 0$ ($j = 1, \dots, n < \infty$) are sufficient for the existence of the *limiting probabilities* (see e.g. [6.3 (1983), A6.6 (Vol. I)])

$$\lim_{t \rightarrow \infty} P_j(t) = P_j, \quad \text{with } P_j > 0 \text{ and } \sum_{j=0}^n P_j = 1. \quad (\text{A7.150})$$

It can be shown (Example A7.8), that the probabilities P_j are given by

$$P_j = \pi_j P_0 = \pi_j / \sum_{i=0}^n \pi_i, \quad \text{with } \pi_0 = 1 \text{ \& } \pi_i = \frac{v_0 \cdots v_{i-1}}{\theta_1 \cdots \theta_i}, \quad j = 0, \dots, n. \quad (\text{A7.151})$$

From Eq. (A7.151) one recognizes that

$$P_k v_k = P_{k+1} \theta_{k+1}, \quad k = 0, \dots, n-1,$$

yielding (Fig. A7.9)

$$P_k \cdot (v_k + \theta_k) = P_{k-1} v_{k-1} + P_{k+1} \theta_{k+1}, \quad k = 0, \dots, n, \quad \theta_0 = v_{-1} = v_n = \theta_{n+1} = 0. \quad (\text{A6.152})$$

The values of P_j given by Eq. (A7.151) can be used in Eq. (A7.134) to calculate the stationary (asymptotic & steady-state) value of the *point availability*. The system *mean time to failure* follows from Eq. (A7.126). Examples A7.9 and A7.10 are applications of the birth and death process.

Example A7.8

Assuming Eq. (A7.150) prove Eq. (A7.151).

Solution

Considering Eqs. (A7.149) & (A7.150), P_j are the solution of following system of algebraic eqs.

$$\begin{aligned} 0 &= -v_0 P_0 + \theta_1 P_1 \\ &\vdots \\ 0 &= -(v_j + \theta_j)P_j + v_{j-1}P_{j-1} + \theta_{j+1}P_{j+1}, \quad j = 1, \dots, n-1, \\ &\vdots \\ 0 &= -\theta_n P_n + v_{n-1}P_{n-1}. \end{aligned}$$

From the first equation it follows $P_1 = P_0 v_0 / \theta_1$. With this P_1 , the second equation leads to

$$P_2 = \frac{v_1 + \theta_1}{\theta_2} P_1 - \frac{v_0}{\theta_2} P_0 = \left(\frac{v_1 + \theta_1}{\theta_2} \cdot \frac{v_0}{\theta_1} - \frac{v_0}{\theta_2} \right) P_0 = \frac{v_0 v_1}{\theta_1 \theta_2} P_0.$$

Recursively one obtains

$$P_j = \frac{v_0 \cdots v_{j-1}}{\theta_1 \cdots \theta_j} P_0 = \pi_j P_0, \quad j = 1, \dots, n, \quad \pi_0 = 1.$$

P_0 follows then from $P_0 + \dots + P_n = 1$.

Example A7.9

For the 1-out-of-2 active redundancy with one repair crew of Examples A7.6 and A7.7, i.e. for $v_0 = 2\lambda$, $v_1 = \lambda$, $\theta_1 = \theta_2 = \mu$, $U = \{Z_0, Z_1\}$ and $\bar{U} = \{Z_2\}$, give the asymptotic & steady-state value PA_S of the point availability and the mean time to failure $MTTF_{S0}$ and $MTTF_{S1}$.

Solution

The asymptotic & steady-state value of point availability is given by Eqs. (A7.131) and (A7.151)

$$PA_S = P_0 + P_1 = (\pi_0 + \pi_1) P_0 = \frac{1 + 2\lambda / \mu}{1 + 2\lambda / \mu + 2\lambda^2 / \mu^2} = \frac{\mu^2 + 2\lambda\mu}{2\lambda(\lambda + \mu) + \mu^2}, \tag{A7.153}$$

as per Eq. (6.87). The system's mean time to failure follows from Eq. (A7.126), with $\rho_{01} = \rho_{10} = 2\lambda$, $\rho_{12} = \lambda$, $\rho_{21} = \mu$, and $\rho_1 = \lambda + \mu$, as solution of

$$MTTF_{S0} = 1 / 2\lambda + MTTF_{S1}$$

$$MTTF_{S1} = \frac{1}{\lambda + \mu} + \frac{\mu}{\lambda + \mu} MTTF_{S0},$$

yielding

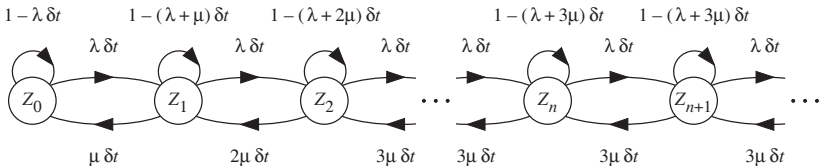
$$MTTF_{S0} = \frac{3\lambda + \mu}{2\lambda^2} \quad \text{and} \quad MTTF_{S1} = \frac{2\lambda + \mu}{2\lambda^2}. \tag{A7.154}$$

Example A7.10

A computer system consists of 3 identical CPUs. Jobs arrive independently and the arrival times form a *Poisson process* with intensity λ . The duration of each individual job is distributed exponentially with parameter μ . All jobs have the same memory requirements D . Give for $\lambda = 2\mu$ the minimum size n of the memory required in units of D , so that in the stationary case (asymptotic & steady-state) a new job can immediately find storage space with a probability γ of at least 95%. When overflow occurs, jobs are queued.

Solution

The problem can be solved using the following birth and death process



In state Z_i , exactly i memory units are occupied. n is the smallest integer such that in the steady-state, $P_0 + \dots + P_{n-1} = \gamma \geq 0.95$ (if the assumption were made that jobs are lost if overflow occurs, then the process would stop at state Z_n). For steady-state, Eq. (A7.127) yields

$$0 = -\lambda P_0 + \mu P_1$$

$$0 = \lambda P_0 - (\lambda + \mu) P_1 + 2\mu P_2$$

$$0 = \lambda P_1 - (\lambda + 2\mu) P_2 + 3\mu P_3$$

$$0 = \lambda P_2 - (\lambda + 3\mu) P_3 + 3\mu P_4$$

$$\vdots$$

$$0 = \lambda P_i - (\lambda + 3\mu) P_{i+1} + 3\mu P_{i+2}, \quad i > 2.$$

The solution leads to

$$P_1 = \frac{\lambda}{\mu} P_0 \quad \text{and} \quad P_i = \frac{\lambda^i P_0}{2 \cdot 3^{i-2} \mu^i} = \frac{9}{2} \left(\frac{\lambda/\mu}{3}\right)^i P_0 \quad \text{for } i \geq 2.$$

Considering $\lim_{n \rightarrow \infty} \sum_{i=0}^n P_i = 1$ (Eq. (A7.150)), $\frac{\lambda}{3\mu} = \frac{2}{3} = a < 1$ & $\lim_{n \rightarrow \infty} \sum_{i=2}^n a^i = \frac{a^2}{1-a}$ it follows that

$$P_0 \left[1 + \frac{\lambda}{\mu} + \sum_{i=2}^{\infty} \frac{9}{2} \left(\frac{\lambda/\mu}{3}\right)^i \right] = P_0 \left[1 + \frac{\lambda}{\mu} + \frac{3(\lambda/\mu)^2}{2(3-\lambda/\mu)} \right] = 1,$$

and thus,

$$P_0 = \frac{2(3-\lambda/\mu)}{6+4\lambda/\mu+(\lambda/\mu)^2}.$$

The size of the memory n can now be determined from

$$\frac{2(3-\lambda/\mu)}{6+4\lambda/\mu+(\lambda/\mu)^2} \left[1 + \frac{\lambda}{\mu} + \sum_{i=2}^{n-1} \frac{9}{2} \left(\frac{\lambda/\mu}{3}\right)^i \right] \geq \gamma.$$

For $\lambda/\mu = 2$ and $\gamma = 0.95$, the smallest n satisfying the above equation is $n = 9$ ($P_0 = 1/9$, $P_1 = 2/9$, $P_i = 2^{i-1}/3^i$ for $i \geq 2$, yielding $P_0 + P_1 + \dots + P_8 \approx 0.961$).

As shown by Examples A7.9 and A7.10, reliability applications of birth and death processes identify v_i as failure rates and θ_i as repair rates. In this case,

$$v_j \ll \theta_{j+1}, \quad j = 0, \dots, n-1,$$

with v_j and θ_{j+1} as in Fig. A7.9. Assuming

$$\max \{v_j / \theta_{j+1}\} = r, \quad 0 < r < 1, \quad j = 0, \dots, n-1, \quad (\text{A7.155})$$

the following relationships for the steady-state probability P_j can be obtained (Example A7.11)

$$P_j \geq \frac{1-r}{r(1-r^{n-j})} \sum_{i=j+1}^n P_i, \quad 0 < r < 1, \quad j = 0, \dots, n-1. \quad (\text{A7.156})$$

Thus, for $r \leq 1/2$, i.e. for $2v_j \leq \theta_{j+1}$ ($j = 0, \dots, n-1$), it follows that

$$P_j > \sum_{i=j+1}^n P_i, \quad 2v_j \leq \theta_{j+1}, \quad j = 0, \dots, n-1. \quad (\text{A7.157})$$

Equation (A7.157) states that for $2v_0 \leq \theta_1, \dots, 2v_{n-1} \leq \theta_n$ the *steady-state probability* in a state Z_j of a birth and death process described by Fig. A7.9 is greater than the sum of steady-state probabilities in all states following Z_j , $j = 0, \dots, n-1$ [2.50 (1992)]; property useful in developing *approximate expressions* for system availability (however, the condition $\max \{v_j / \theta_{j+1}\} \leq 1/2$, sufficient for reliability applications, can be weakened for arbitrary birth and death processes).

Example A7.11

Assuming Eq.(A7.155), prove Eqs. (A7.156) and (A7.157).

Solution

Using Eq. (A7.151),

$$\frac{\sum_{i=j+1}^n P_i}{P_j} = \frac{\sum_{i=j+1}^n \pi_i}{\pi_j} = \sum_{i=j+1}^n \frac{\pi_i}{\pi_j} = \frac{v_j}{\theta_{j+1}} + \frac{v_j v_{j+1}}{\theta_{j+1} \theta_{j+2}} + \dots + \frac{v_j \dots v_{n-1}}{\theta_{j+1} \dots \theta_n} .$$

Setting $\max\{v_i / \theta_{i+1}\} = r$ for $0 < r < 1$ and $i = j, j + 1, \dots, n - 1$, it follows that

$$\sum_{i=j+1}^n P_i / P_j \leq r + r^2 + \dots + r^{n-j} = r (1 - r^{n-j}) / (1 - r),$$

and thus Eq. (A7.156). Furthermore, considering $0 < r < 1$ and $(n - j) \in \{0, 1, \dots, n\}$ it follows that $(1 - r^{n-j}) < 1$ and, for $r \leq 1/2$, $r / (1 - r) \leq 1$; thus, $r \leq 1/2$ yields $r (1 - r^{n-j}) / (1 - r) < 1$ and hence Eq. (A7.157).

A7.6 Semi-Markov Processes with a Finite Number of States

The description of Markov processes given in Appendix A7.5.2 allows a straightforward generalization to *semi-Markov processes*. In a semi-Markov process, the sequence of *consecutively* occurring states forms an *embedded* time-homogeneous *Markov chain*, just as with Markov processes. The *stay (sojourn) time* in a given state Z_i is a random variable $\tau_{ij} > 0$ whose distribution depends on Z_i and on the following state Z_j , but in contrast to time-homogeneous Markov processes it is *arbitrarily and not exponentially distributed*. Related to semi-Markov processes are *Markov renewal processes* $\{N_i(t) = \text{number of transitions to state } Z_i \text{ in } (0, t]\}$ [A7.23].

To define semi-Markov processes, let ξ_0, ξ_1, \dots be the sequence of *consecutively* occurring states, i.e., a sequence of random variables taking values in $\{Z_0, \dots, Z_m\}$, and η_0, η_1, \dots the *stay times between consecutive states*, i.e., a sequence of random variables > 0 . A stochastic process $\xi(t)$ with state space $\{Z_0, \dots, Z_m\}, 0 < m < \infty$, is a *semi-Markov process* in continuous time ($t \geq 0$) with a *finite number of states*, if for $n = 0, 1, 2, \dots$, arbitrary $i, j, i_0, \dots, i_{n-1} \in \{0, \dots, m\}$, and arbitrary $x, x_0, \dots, x_{n-1} > 0$

$$\begin{aligned} \Pr \{(\xi_{n+1} = Z_j \cap \eta_n \leq x) \mid (\xi_n = Z_i \cap \eta_{n-1} = x_{n-1} \cap \dots \cap \xi_1 = Z_{i_1} \cap \eta_0 = x_0 \cap \xi_0 = Z_{i_0})\} \\ = \Pr \{(\xi_{n+1} = Z_j \cap \eta_n \leq x) \mid \xi_n = Z_i\} = Q_{ij}(x)^+ \end{aligned} \quad (\text{A7.158})$$

holds. $\xi(t) = \xi_0$ for $0 \leq t < \eta_0$ and $\xi(t) = \xi_n$ for $\eta_0 + \dots + \eta_{n-1} \leq t < \eta_0 + \dots + \eta_n$ & $n \geq 1$ is a *jump process*, as visualized in Fig. A7.10.

^{+) A semi-Markov process (SMP) with states Z_0, Z_1 and $\mathcal{P}_{00} = \mathcal{P}_{11} = 0$ ($\mathcal{P}_{01} = \mathcal{P}_{10} = 1$) is an *alternating renewal process* (Appendix A7.3 and Fig. A7.3); the case of only one state is not considered as a SMP but as a *renewal process* (Appendix A7.2 and Fig. A7.1a).}

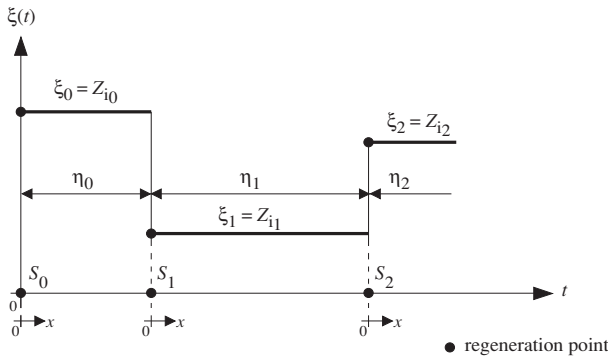


Figure A7.10 Possible realization for a semi-Markov process (x starts by 0 at every state change)

The functions $Q_{ij}(x)$ in Eq. (A7.158), defined for $j \neq i$, are the semi-Markov transition probabilities, often known as one-step transition probabilities (see remarks with Eqs. (A7.95) - (A7.101)). Setting

$$Q_{ij}(\infty) = P_{ij}, \quad j \neq i, \quad P_{ii} \equiv 0, \quad (A7.159)$$

and, for $P_{ij} > 0$,

$$F_{ij}(x) = Q_{ij}(x) / P_{ij}, \quad j \neq i, \quad x > 0, \quad F_{ij}(x) = 0 \text{ for } x \leq 0, \quad (A7.160)$$

leads to

$$Q_{ij}(x) = P_{ij} F_{ij}(x), \quad j \neq i, \quad x > 0, \quad Q_{ij}(x) = 0 \text{ for } x \leq 0, \quad (A7.161)$$

with (Example A7.2)

$$P_{ij} = \Pr\{\xi_{n+1} = Z_j \mid \xi_n = Z_i\} = Q_{ij}(\infty), \quad P_{ii} \equiv 0, \quad n = 0, 1, 2, \dots, \quad \sum_{\substack{j=0 \\ j \neq i}}^m P_{ij} = 1, \quad (A7.162)$$

and

$$F_{ij}(x) = \Pr\{\eta_n \leq x \mid (\xi_n = Z_i \cap \xi_{n+1} = Z_j)\}, \quad \begin{matrix} j \neq i, \quad n = 0, 1, 2, \dots \\ F_{ij}(x) = 0 \text{ for } x \leq 0. \end{matrix} \quad (A7.163)$$

The interpretation of the quantities $Q_{ij}(x)$ given by Eqs. (A7.99) - (A7.101) are useful for practical applications (see for instance Eqs. (A7.182) - (A7.187)).

$P_{ii} \equiv 0$ is mandatory for time-homogeneous Markov processes (with a finite number of states), as well as for the semi-Markov processes used in reliability analysis. However, as pointed out in the footnote on p. 510, $P_{ii} > 0$ must be accepted for a semi-Markov process embedded in a semi-regenerative process.

From Eq. (7.158), the consecutive jump points at which the process enters Z_i are regeneration points. This holds for any $i \in \{0, \dots, m\}$ and thus,

all states of a semi-Markov process are regeneration states.

The renewal density of the embedded renewal process of consecutive jumps in Z_i (i -renewals) will be denoted as $h_i(t)$, see Eq. (A7.177) for the stationary case.

The *initial distribution*, i.e. of the vector $(\xi_0 \equiv \xi(0), \xi_1, \eta_0^\circ)$, is given by

$$A_{ij}^\circ(x) = \Pr\{\xi(0)=Z_i \cap \xi_1=Z_j \cap \text{residual sojourn time } \eta_0^\circ \text{ in } Z_i \leq x\} = P_i(0) \mathcal{P}_{ij} F_{ij}^\circ(x) \tag{A7.164}$$

with $P_i(0) = \Pr\{\xi(0) = Z_i\}$, p_{ij} as per Eq. (A7.162), and $F_{ij}^\circ(x) = \Pr\{\text{residual sojourn time } \eta_0^\circ \text{ in } Z_i \leq x \mid (\xi(0)=Z_i \cap \xi_1=Z_j)\}$. $\xi(0)$ is used here for clarity instead of ξ_0 . The semi-Markov process is *memoryless only at the transition points from one state to the other*. To have the time $t=0$ as a *regeneration point*, the initial condition $\xi(0)=Z_i$, sufficient for time-homogeneous Markov processes, *must be reinforced* by

Z_i is entered at $t = 0$.

The sequence $\xi_0 \equiv \xi(0), \xi_1, \dots$ forms a Markov chain, *embedded* in the semi-Markov process, with *transition probabilities* \mathcal{P}_{ij} as per Eq. (A7.162) and *initial probabilities* $P_i(0)$, $i = 0, \dots, m$. $F_{ij}(x)$ is the *conditional distribution function of the stay (sojourn) time* in Z_i with consequent jump in Z_j (next state to be visited). $F_{ij}(x) = 1 - e^{-\mathcal{P}_{ij}x}$ ($i, j \in \{0, \dots, m\}$), yields to a time-homogeneous *Markov process*.

An example of a two state semi-Markov process is the *alternating renewal process* given in Appendix A7.3 ($Z_0 = up, Z_1 = down, \mathcal{P}_{01} = \mathcal{P}_{10} = 1, F_{01}(x) = F(x), F_{10}(x) = G(x), F_0^\circ(x) = F_A(x), F_1^\circ(x) = G_A(x), P_0(0) = p, P_1(0) = 1 - p$).

In many applications, the quantities $Q_{ij}(x)$, or \mathcal{P}_{ij} and $F_{ij}(x)$, can be evaluated using Eqs. (A7.99) - (A7.101), as shown in Appendix A7.7 and Sections 6.3 – 6.6.

For the *unconditional stay (sojourn) time* in Z_i , the distribution function is

$$Q_i(x) = \Pr\{\eta_n \leq x \mid \xi_n = Z_i\} = \sum_{\substack{j=0 \\ j \neq i}}^m \mathcal{P}_{ij} F_{ij}(x) = \sum_{\substack{j=0 \\ j \neq i}}^m Q_{ij}(x), \tag{A7.165}$$

with $Q_{ij}(x)$ as per Eq. (A7.161) & $Q_i(\infty) = 1$, and the *mean*

$$T_i = \int_0^\infty (1 - Q_i(x)) dx < \infty. \tag{A7.166}$$

In the following it will be assumed that

$$q_{ij}(x) = dQ_{ij}(x) / dx \tag{A7.167}$$

exists for all $i, j \in \{0, \dots, m\}$.

Consider first the case in which *the process enters the state Z_i at $t = 0$* , i.e. that

$$P_i(0) = 1 \quad \text{and} \quad F_{ij}^\circ(x) = F_{ij}(x).$$

The *transition probabilities*

$$P_{ij}(t) = \Pr\{\xi(t) = Z_j \mid Z_i \text{ is entered at } t = 0\} \tag{A7.168}$$

can be obtained by generalizing Eq. (A7.120),

$$P_{ij}(t) = \delta_{ij}(1 - Q_i(t)) + \sum_{\substack{k=0 \\ k \neq i}}^m \int_0^t q_{ik}(x) P_{kj}(t-x) dx, \quad t > 0, P_{ij}(0) = \delta_{ij}, \tag{A7.169}$$

with δ_{ij} & $Q_i(t)$ per Eqs.(A7.85)&(A7.165). Note that in $Q_{ij}(x)$, Z_j is the next state visited after Z_i , but this is not the case for $P_{ij}(t)$. The state probabilities follow as

$$P_j(t) = \Pr\{\xi(t) = Z_j\} = \sum_{i=0}^m \Pr\{Z_i \text{ is entered at } t=0\} P_{ij}(t), \quad t > 0, \quad (\text{A7.170})$$

with $P_j(t) \geq 0$, $i, j \in \{0, \dots, m\}$, and $P_0(t) + \dots + P_m(t) = 1$. If the state space is divided into the complementary sets U for the up states and \bar{U} for the down states, as in Eq. (A7.107), the point availability follows from Eq. (A7.112)

$$PA_{S_i}(t) = \Pr\{\xi(t) \in U \mid \xi(0) = Z_i\} = \sum_{Z_j \in U} P_{ij}(t), \quad \begin{matrix} i=0, \dots, m, \\ PA_{S_i}(0) = 1 \text{ for } Z_i \in U, \end{matrix} \quad t > 0, \quad (\text{A7.171})$$

with $P_{ij}(t)$ per Eq. (A7.169), see also the remark at the bottom of p. 495. The probability that the first transition from a state in U to a state in \bar{U} occurs after the time t , i.e. the reliability function, follows from Eq. (A7.122) as

$$\begin{aligned} R_{S_i}(t) &= \Pr\{\xi(x) \in U \text{ for } 0 < x \leq t \mid Z_i \text{ is entered at } t=0\} \\ &= 1 - Q_i(t) + \sum_{\substack{Z_j \in U \\ j \neq i}} \int_0^t q_{ij}(x) R_{S_j}(t-x) dx, \quad Z_i \in U, t > 0, R_{S_i}(0) = 1, \end{aligned} \quad (\text{A7.172})$$

with $Q_i(t)$ & $q_{ij}(x)$ as per Eqs.(A7.165)&(A7.167). The mean of the stay (sojourn) time in U , i.e. the system mean time to failure, follows from Eq. (A7.172) as solution of the following system of algebraic equations (with T_i as per Eq. (A7.166))

$$MTTF_{S_i} = T_i + \sum_{\substack{Z_j \in U \\ j \neq i}} P_{ij} MTTF_{S_j}, \quad Z_i \in U. \quad (\text{A7.173})$$

Consider now the case of a stationary semi-Markov process. Under the assumption that the embedded Markov chain is irreducible (every state can be reached from every other state with probability > 0), the semi-Markov process is stationary if and only if the initial distribution (Eq. (A7.164)) is given by [6.3, A7.22, A7.23, A7.28]

$$A_{ij}^\circ(x) = \frac{P_i P_{ij}}{\sum_{k=0}^m P_k T_k} \int_0^x (1 - F_{ij}(y)) dy = \frac{P_i P_{ij}}{T_i} \int_0^x (1 - F_{ij}(y)) dy. \quad (\text{A7.174})$$

In Eq. (A7.174), P_{ij} are the transition probabilities (Eq.(A7.162)) and P_i the stationary distribution of the embedded Markov chain; P_i are the unique solutions of

$$P_j = \sum_{i=0}^m P_i P_{ij}, \quad \text{with } P_{ii} = 0, P_{ij} = Q_{ij}(\infty), P_j > 0, \sum_{j=0}^m P_j = 1, j = 0, \dots, m. \quad (\text{A7.175})$$

The system given by Eq. (A7.175) must be solved by replacing one (arbitrarily chosen) equation by $\sum P_j = 1$. It differs from that of Eq. (A7.74) because of $P_{ii} = 0$. For the stationary semi-Markov process (with irreducible embedded Markov chain),

the state probabilities are independent of time and given by [6.3, A7.22, A7.23, A7.28]

$$P_i(t) = P_i = \frac{T_i}{T_{ii}} = \frac{\mathcal{P}_i T_i}{\sum_{k=0}^m \mathcal{P}_k T_k}, \quad t \geq 0, \quad i=0, \dots, m, \tag{A7.176}$$

with $T_i < \infty$ per Eq. (A7.166) and \mathcal{P}_i from Eq. (A7.175). P_i per Eq. (A7.176) and $A_{ij}^\circ(x)$ per Eq. (A7.174) are thus the *initial conditions* at $t=0$. T_{ii} is the mean of the time interval between *two consecutive occurrences of the state Z_i* (in steady-state). These time points form a *stationary renewal process* with renewal density

$$h_i(t) = h_i = \frac{1}{T_{ii}} = \frac{\mathcal{P}_i}{\sum_{k=0}^m \mathcal{P}_k T_k}, \quad t \geq 0, \quad i=0, \dots, m. \tag{A7.177}$$

h_i is the *frequency* of successive occurrences of state Z_i . In Eq. (A7.176), P_i can be heuristically interpreted as $P_i = \lim_{t \rightarrow \infty} [(t / T_{ii}) T_i] / t = T_i / T_{ii}$ or as ratio of the mean time in which the embedded Markov chain is in state Z_i to the mean time in all states $P_i = \mathcal{P}_i T_i / \sum \mathcal{P}_k T_k$. Similar is for $A_{ij}^\circ(x)$ in Eqs. (A7.174), considering also Eq. (A7.35). The stationary (asymptotic and steady-state) value of the *point availability* PA_S and *average availability* AA_S follows from Eq. (A7.176)

$$PA_S = AA_S = \sum_{Z_i \in U} P_i = \sum_{Z_i \in U} \frac{\mathcal{P}_i T_i}{\sum_{k=0}^m \mathcal{P}_k T_k}. \tag{A7.178}$$

Similarly as for Markov processes, the *system mean up time, mean down time, and failure & repair frequencies* are given by (Eq.(A7.141)-(A7.146), (A7.103))

$$MUT_S = \frac{PA_S}{f_{udS}}, \quad MDT_S = \frac{(1 - PA_S)}{PA_S} MUT_S, \quad f_{udS} = f_{dus} = \sum_{Z_j \in U, Z_i \in \bar{U}} P_j \mathcal{P}_{ji} / T_j. \tag{A7.179}$$

Under the assumptions made above (continuous sojourn times with finite means, *irreducible embedded Markov chain*), following holds for $i, j \in \{0, \dots, m\}$ regardless of the initial distribution at $t=0$ [6.3, A7.22, A7.23, A7.28]

$$\begin{aligned} \lim_{t \rightarrow \infty} \Pr \{ \xi(t) = Z_i \cap \text{next transition in } Z_j \cap \text{residual sojourn time in } Z_i \leq x \} \\ = \frac{P_i \mathcal{P}_{ij}}{T_i} \int_0^x (1 - F_{ij}(y)) dy = \frac{\mathcal{P}_i \mathcal{P}_{ij}}{\sum_{k=0}^m \mathcal{P}_k T_k} \int_0^x (1 - F_{ij}(y)) dy = A_{ij}^\circ(x), \\ \lim_{t \rightarrow \infty} \Pr \{ \xi(t) = Z_i \} = \lim_{t \rightarrow \infty} P_{ji}(t) = P_i = \frac{T_i}{T_{ii}}, \quad \lim_{t \rightarrow \infty} PA_{Si}(t) = PA_S = \sum_{Z_i \in U} P_i. \end{aligned} \tag{A7.180}$$

Except for investigations on the reliability function ($R_S(t)$) (see footnote on p. 497), an *irreducible embedded Markov chain* can be assumed in reliability applications. For such cases, according to Eqs. (A7.176) and (A7.180),

asymptotic & steady-state can be used as a synonym for *stationary* (see e. g. also pp. 187-188, 472, 477, 479, 498, 514).

For the *alternating renewal process* (Fig. A7.3, $Z_0 = up, Z_1 = down$) it holds that $\mathcal{P}_{00} = \mathcal{P}_{11} = 0, \mathcal{P}_{10} = \mathcal{P}_{01} = 1 \Rightarrow \mathcal{P}_0 = \mathcal{P}_1 = 1/2$ (embed. Markov chain), $T_0 = MTTF, T_1 = MTTR, T_{00} = T_{11} = T_0 + T_1$; Eqs. (A7.176) leads to $P_0 = MTTF / (MTTF + MTTR) \approx 1 - MTTR / MTTF$. This example shows the *basic difference* between \mathcal{P}_j as stationary distribution of the embedded Markov chain and the limiting state probability P_i in state Z_i of the original process (P_i is related to the stay time in Z_i, \mathcal{P}_j to the state changes).

For a stationary *time-homogeneous Markov processes* (Appendix A7.5.3.3), Eqs. (A7.166), (A7.165) & (A7.102) yield $T_i = 1/\rho_i$. From Eqs. (A7.174), (A7.176), (A7.103) & (A7.104) it follows then

$$A_{ij}^\circ(x) = (1 - e^{-\rho_i x}) P_i \rho_{ij} / \rho_i, \tag{A7.181}$$

and (Eq. (A7.177))

$$h_i(t) = h_i = P_i \rho_i = P_i / T_i = 1 / T_{ii}, \quad i = 0, \dots, m. \tag{A7.181a}$$

A7.7 Semi-regenerative Processes with a Finite Number of States

As pointed out in Appendix A7.5.2, the time behavior of a repairable system can be described by a time-homogeneous Markov process *if and only if failure-free and repair times of all elements are exponentially distributed* (constant failure and repair rates during the stay time in each state, with possible stepwise change at state transitions, e.g. because of load sharing). Except for *Erlang distributions* (Section 6.3.3), non exponentially distributed repair and/or failure-free times lead in some cases to semi-Markov processes (Sections 6.2, 6.3.2, 6.8.4 (Fig. 6.27), 6.10) and in general to processes *with only few regeneration states* or to *nonregenerative processes*.

To make sure that the time behavior of a system can be described by a semi-Markov process, there must be no “running” time (failure-free or repair) at any state change which is not exponentially distributed.⁺⁾

Figure A7.11 shows the case of a process with states Z_0, Z_1, Z_2 in which only states Z_0 and Z_1 are regeneration states. Z_0 & Z_1 form a semi-Markov process *embedded* in the original process, on which investigations can be based. Processes with an embedded semi-Markov process *with irreducible Markov chain* are called (in this book) *semi-regenerative processes*. Their investigation can become time-consuming and has to be performed on a *case-by-case basis*, often using a time schedule.⁺⁺⁾

⁺⁾ For a time-homogeneous Markov process, this rule holds at any arbitrary time $t > 0$.

⁺⁺⁾As discussed in Example A7.12, $\mathcal{P}_{i,i} > 0$ must be accepted for an *embedded semi-Markov process* (during a transition $Z_1 \rightarrow Z_2 \rightarrow Z_1$ the embedded Markov chain remains in Z_1 , making a transition $Z_1 \rightarrow Z_1$ at the transition points $Z_2 \rightarrow Z_1$ of the original process); Figures A7.11 - A7.13, 6.10, 6.14, 6.16, and the corresponding investigations, give some examples as how to operate.

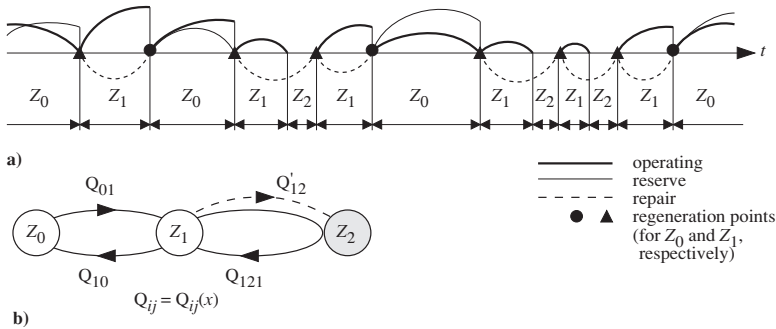


Figure A7.11 a) Possible time schedule for a 1-out-of-2 warm redundancy with constant failure rates (λ, λ_r), arbitrary repair rate (density $g(x), G(0)=0$), one repair crew (repair times greatly exaggerated), ideal failure detection & switch; b) State transition diagram for the embedded semi-Markov process with states Z_0, Z_1 (regeneration states), Q'_{12} is not a semi-Markov transition probability and during a transition $Z_1 \rightarrow Z_2 \rightarrow Z_1$ the embedded Markov chain (on Z_0, Z_1) remains in Z_1 , Z_2 down state (absorbing for rel. calculation); holds also for a k-out-of-n warm redundancy with $n-k=1$

Example A7.12 investigates a basic situation.

Example A7.12

Consider a 1-out-of-2 warm redundancy as in Fig. A7.4a with constant failure rates λ in operating & λ_r in reserve state and one repair crew with arbitrarily distributed repair time (density $g(x), G(0)=0$). Give the transition probabilities for the embedded semi-Markov process.

Solution

As Fig. A7.11a shows, only states Z_0 and Z_1 are regeneration states. Z_2 is not a regeneration state because at the transition points into Z_2 a repair with arbitrary repair rate is running. Thus, the process involved is not a semi-Markov process. However, states Z_0 and Z_1 form an embedded semi-Markov process on which investigations can be based. The transition probabilities of the embedded semi-Markov process (on Z_0, Z_1) are (Fig. A7.11, Eqs. (A7.99)-(A7.101))

$$\begin{aligned}
 Q_{01}(x) &= Q_{00}(x) = 1 - e^{-(\lambda + \lambda_r)x}, & Q_{121}(x) &= \int_0^x g(y) (1 - e^{-\lambda y}) dy, \\
 Q_{10}(x) &= \int_0^x g(y) e^{-\lambda y} dy = G(x) e^{-\lambda x} + \int_0^x \lambda e^{-\lambda y} G(y) dy.
 \end{aligned}
 \tag{A7.182}$$

$Q_{121}(x)$ is used to calculate the point availability (Eqs. (6.106), (6.109)). It accounts for the transitions throughout the not regeneration down state Z_2 . During a transition $Z_1 \rightarrow Z_2 \rightarrow Z_1$, the embedded Markov chain remains in Z_1 (Fig. A7.11a, footnote on p.510), and for the embedded Markov chain it holds that $P_{00}=0, P_{01}=1, P_{10}=\tilde{g}(\lambda), P_{11}=1-\tilde{g}(\lambda)$ with $\tilde{g}(\lambda) = \int_0^\infty g(x) e^{-\lambda x} dx = \Pr\{\tau_{\text{failure-free}} > \tau_{\text{repair}}\}$. This is important for the calculation of $Q_1(x)$, see below. $Q'_{12}(x)$ as given in Fig. A7.11b is not a semi-Markov transition probability; however, $Q'_{12}(x)$ expressed as (see Fig. A7.11a)

$$Q'_{12}(x) = \int_0^x \lambda e^{-\lambda y} (1 - G(y)) dy = 1 - e^{-\lambda x} - \int_0^x \lambda e^{-\lambda y} G(y) dy,$$

yields

$$Q_1(x) = Q_{10}(x) + Q'_{12}(x) = 1 - (1 - G(x)) e^{-\lambda x}.
 \tag{A7.183}$$

Supplementary results: Section 6.4.2 investigates reliability & availability. $k\lambda$ instead of λ in Eqs. (A7.182) & (A7.183) yields results for a k-out-of-n warm redundancy with $n-k=1$, one repair crew, and no further failure at system down.

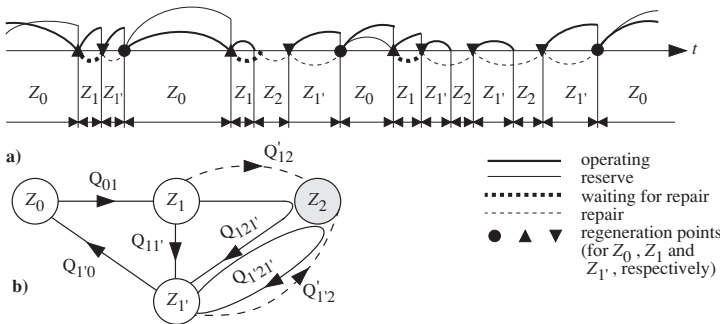


Figure A7.12 a) Possible time schedule for a 1-out-of-2 warm redundancy with constant failure rates (λ, λ_r) , arbitrary repair times (density $g(x), G(0)=0$), arbitrary travel times (density $w(x), W(0)=0$) for failures in state Z_0 , one repair crew (repair times greatly exaggerated), ideal failure detection and switch; b) State transition diagram for the embedded semi-Markov process with states Z_0, Z_1, Z_1' (regeneration states), Z_2 down state (absorbing for reliability calculation)

As a second example, let us assume that for the 1-out-of-2 warm redundancy of Fig. A7.11, a travel time with density $w(x)$ must be considered before a repair for a failure in state Z_0 can be made. Figure A7.12 gives a possible time schedule and the state transition diagram of the involved semi-regenerative process. States Z_0, Z_1, Z_1' are regeneration states, and constitute an embedded 3 states semi-Markov process. Z_2 is not a regeneration state. The transition probabilities of the embedded semi-Markov process (on Z_0, Z_1, Z_1') are (Fig. A7.12, Eqs. (A7.99)-(A7.101))

$$\begin{aligned}
 Q_{01}(x) &= Q_{00}(x) = 1 - e^{-(\lambda + \lambda_r)x}, & Q_{11'}(x) &= \int_0^x w(y) e^{-\lambda y} dy, \\
 Q_{121'}(x) &= \int_0^x \int_0^y w(z) (1 - e^{-\lambda z}) g(y - z) dz dy, \\
 Q_{1'0}(x) &= \int_0^x g(y) e^{-\lambda y} dy, & Q_{1'21'}(x) &= \int_0^x g(y) (1 - e^{-\lambda y}) dy.
 \end{aligned} \tag{A7.184}$$

$Q_{121'}(x)$ & $Q_{1'21'}(x)$ (with Laplace transform $\tilde{Q}_{121'}(s) = (\tilde{w}(s) - \tilde{w}(s + \lambda)) \tilde{g}(s) / s$ & $\tilde{Q}_{1'21'}(s) = (\tilde{g}(s) - \tilde{g}(s + \lambda)) / s$) are used to calculate the point availability. They account for the transitions throughout the not regeneration down state Z_2 . The quantities

$$Q'_{12}(x) = \int_0^x \lambda e^{-\lambda y} (1 - W(y)) dy \quad \text{and} \quad Q'_{1'2}(x) = \int_0^x \lambda e^{-\lambda y} (1 - G(y)) dy \tag{A7.185}$$

are not semi-Markov transition probabilities; however, they are necessary to calculate $Q_1(x) = Q_{11'}(x) + Q'_{12}(x)$ & $Q_{1'}(x) = Q_{1'0}(x) + Q'_{1'2}(x)$. Investigation is similar to that of Fig. A7.11, yielding 9 integral equations to compute $P_{00}(t), P_{01}(t), P_{01'}(t)$ and then $PA_{S0}(t) = P_{00}(t) + P_{01}(t) + P_{01'}(t)$ (a good approximation for $PA_S = AA_S$ follows often using the first 2 terms of the series expansion of $\tilde{g}(s)$ & $\tilde{w}(s)$). Example 6.7 investigates $MTTF_{S0}$ and $PA_S = AA_S$ for exponentially distributed travel & repair times.

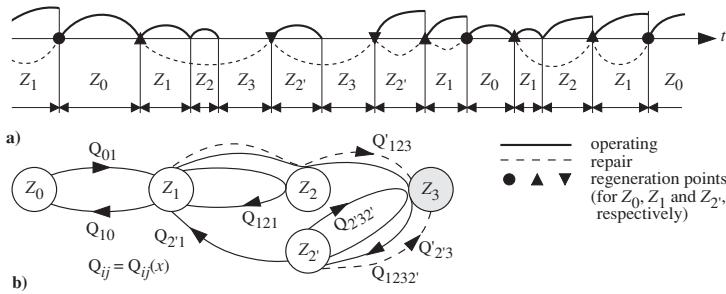


Figure A7.13 a) Possible time schedule for a k -out-of- n warm redundancy with $n-k=2$, constant failure rates (λ, λ_r) , arbitrary repair rate (density $g(x), G(0)=0$), one repair crew (repair times greatly exaggerated), no further failure at system down, ideal failure detection & switch, operating and reserve elements not separately shown; b) State transition diagram for the embedded semi-Markov proc. with states Z_0, Z_1, Z_2' (regeneration states), Z_3 down state (absorbing for reliability calculation)

As a further example, Fig. A7.13 gives a possible time schedule for a k -out-of- n warm redundancy with $n-k=2$, const. failure rates (λ, λ_r) , arbitrary repair rate (density $g(x), G(0)=0$), only one repair crew, no further failure at system down. Given is also the state transition diagram of the involved semi-regenerative process. States Z_0, Z_1, Z_2' are regeneration states, Z_2 & Z_3 are not regeneration states. The transition probabilities of the embedded semi-Markov process are (Eqs.(A7.99)-(A7.101))

$$\begin{aligned}
 Q_{01}(x) = Q_0(x) &= 1 - e^{-(k\lambda + 2\lambda_r)x}, & Q_{10}(x) &= \int_0^x g(y) e^{-(k\lambda + \lambda_r)y} dy, \\
 Q_{2'1}(x) &= \int_0^x g(y) e^{-k\lambda y} dy, & Q_{121}(x) &= \int_0^x g(y) \left[\int_0^y (k\lambda + \lambda_r) e^{-(k\lambda + \lambda_r)z} e^{-k\lambda(y-z)} dz \right] dy, \\
 Q_{1232'}(x) &= \int_0^x g(y) \left[\int_0^y (k\lambda + \lambda_r) e^{-(k\lambda + \lambda_r)z} (1 - e^{-k\lambda(y-z)}) dz \right] dy, \\
 Q_{2'32'}(x) &= \int_0^x g(y) (1 - e^{-k\lambda y}) dy.
 \end{aligned}
 \tag{A7.186}$$

$Q_{1232'}(x), Q_{2'32'}(x)$ are used to calculate the point availability. They account for the transitions throughout the not regeneration down states Z_2 and/or Z_3 . $Q_{121}(x)$ is used for the point availability and reliability calculation. The quantities

$$\begin{aligned}
 Q'_{123}(x) &= \int_0^x (1 - G(y)) \left[\int_0^y (k\lambda + \lambda_r) e^{-(k\lambda + \lambda_r)z} k\lambda e^{-k\lambda(y-z)} dz \right] dy, \\
 Q'_{2'13}(x) &= \int_0^x k\lambda e^{-k\lambda y} (1 - G(y)) dy
 \end{aligned}
 \tag{A7.187}$$

are not semi-Markov transition probabilities; however, necessary to compute $Q_1(x) = Q_{10}(x) + Q_{121}(x) + Q'_{123}(x)$ and $Q_2(x) = Q_{2'1}(x) + Q'_{2'3}(x)$ (note that Z_2 is an up state). For instance, $MTTF_{S_0} = \bar{R}_{S_0}(0)$ (Eq.(A7.125)) follows as solution of (Eq.(A7.172)) $\bar{R}_{S_0}(s) = (1 - \bar{q}_0(s))/s + \bar{q}_{01}(s)\bar{R}_{S_1}(s)$ and $\bar{R}_{S_1}(s) = (1 - \bar{q}_1(s))/s + \bar{q}_{10}(s)\bar{R}_{S_0}(s) + \bar{q}_{121}(s)\bar{R}_{S_1}(s)$, as given in Table 6.8 (p. 217) for $g(x) = \mu e^{-\lambda x}$, $n-k=2$.

Following, considerations on *semi-regenerative processes* refine those given in Appendix A7.4 for *regenerative processes*. A pure jump process $\xi(t)$, $t \geq 0$, with state space Z_0, \dots, Z_m is semi-regenerative, with regeneration states Z_0, \dots, Z_k , $0 < k < m$, if the following holds: Let ζ_0, ζ_1, \dots be the sequence of *successively* occurring regeneration states and $\varphi_0, \varphi_1, \dots$ the random time intervals between consecutive occurrence of regeneration states, assumed continuous, > 0 & with finite mean. Then, Eq. (A7.158) with ζ_n, φ_n instead of ξ_n, η_n must be fulfilled; in other words,

$\zeta(t)$ as given by $\zeta(t) = \zeta_0$ for $0 \leq t < \varphi_0$ and $\zeta(t) = \zeta_n$ for $\varphi_0 + \dots + \varphi_{n-1} \leq t < \varphi_0 + \dots + \varphi_n$, $n \geq 1$, is a semi Markov process with state space Z_0, \dots, Z_k embedded in the original process $\xi(t)$ with state space Z_0, \dots, Z_m .

The piece $\xi(t)$, $\varphi_0 + \dots + \varphi_{n-1} \leq t < \varphi_0 + \dots + \varphi_n$, $n \geq 1$, of the original process is a *cycle* (p. 478). Its distribution depends on the regeneration state involved. The epochs at which a given state Z_i , $0 \leq i \leq k$, occurs are *regeneration points* and constitute a *renewal process*, belonging to Z_i , embedded in $\xi(t)$ (see Fig. A7.3 for a simple case).

In reliability applications, the set of regeneration states is in general a subset of the system up states. The procedure used to develop Eqs. (A7.182) - (A7.187) can help to find the transition probabilities involved (see also the footnote on p. 510).

An *irreducible embedded Markov chain* (p. 481) on Z_0, \dots, Z_k , continuous $F_{ij}(x)$, $x > 0$, $i, j \in \{0, \dots, k\}$ & *finite mean cycle lengths* for the embedded semi-Markov proc., are *sufficient* for the existence of the limiting state probabilities P_e [A7.9, A7.24, 6.3]

$$P_e = \lim_{t \rightarrow \infty} \Pr\{\xi(t) = Z_e\}, \quad e = 0, \dots, m. \tag{A7.188}$$

Denoting by $T_i < \infty$ the mean stay time in the state Z_i , $i = 0, \dots, k$, and by $T_{ii} < \infty$ the mean of the time interval between *two consecutive occurrences* of Z_i , it holds that

$$\lim_{t \rightarrow \infty} \Pr\{\xi(t) = Z_i\} = P_i = T_i / T_{ii}, \quad i = 0, \dots, k, \tag{A7.188a}$$

(see also Eq. (A7.176) and Eq. (A7.67) with $T_c = E[\tau_{c_i}] = T_{ii}$). Consecutive cycles of same type are possible, yielding transitions to a same state for the embedded Markov chain if the cycle contains not regeneration states ($Z_1 \rightarrow Z_2 \rightarrow Z_1$ in Fig. A7.11a, footnote on p. 510). However, as for Markov & semi-Markov processes,

an irreducible embedded Markov chain can not be assumed for investigations on the reliability function ($R_S(t)$) (see footnote on p. 497).

For the *1-out-of-2 warm redundancy* of Fig. A7.11 it holds for the embedded Markov chain $P_{00} = 0$, $P_{01} = 1$, $P_{10} = Q_{10}(\infty) = \tilde{g}(\lambda)$, $P_{11} = 1 - P_{10} = 1 - \tilde{g}(\lambda)$, and thus $P_1 = 1/(1 + \tilde{g}(\lambda)) \geq 1/2$ & $P_0 = 1 - P_1 = \tilde{g}(\lambda)/(1 + \tilde{g}(\lambda)) \leq 1/2$; furthermore, $T_0 = 1/(\lambda + \lambda_r)$, $T_1 = (1 - \tilde{g}(\lambda))/\lambda$, $T_{00} = 1/(\lambda + \lambda_r) + MTTR / \tilde{g}(\lambda)$ and $T_{11} = MTTR + \tilde{g}(\lambda)/(\lambda + \lambda_r)$ yields $P_0 = T_0 / T_{00}$, $P_1 = T_1 / T_{11}$, and $PA_S = P_0 + P_1$ as per Eq. (6.110) (T_0 & T_1 follow from Eq. (A7.166) with $Q_0(x)$, $Q_1(x)$ as per Eqs. (A7.182), A7.183); T_{00} & T_{11} are obtained from Fig. A7.11a considering $T_{11} = \tilde{g}(\lambda)(MTTR + 1/(\lambda + \lambda_r)) + (1 - \tilde{g}(\lambda))MTTR$, $T_{00} = \tilde{g}(\lambda)(MTTR + 1/(\lambda + \lambda_r)) + (1 - \tilde{g}(\lambda))\tilde{g}(\lambda)(2MTTR + 1/(\lambda + \lambda_r)) + (1 - \tilde{g}(\lambda))^2\tilde{g}(\lambda)(3MTTR + 1/(\lambda + \lambda_r)) + \dots$, $\tilde{g}(\lambda) = \int_0^\infty g(x)e^{-\lambda x} dx = \Pr\{\text{failure-free time} > \tau_{\text{repair}}\}$, $1 + 2x + 3x^2 + \dots = 1/(1-x)^2$).

A7.8 Nonregenerative Stochastic Processes with a Countable Number of States

The assumption of arbitrarily (not exponentially) distributed failure-free and repair (restoration) times for the elements of a system, already leads to *nonregenerative stochastic processes* for simple series or parallel structures. After some general considerations, nonregenerative processes used in reliability analysis are introduced.

A7.8.1 General Considerations

Solutions for nonregenerative stochastic processes are often problem-oriented. However, as a possible general method, transformation of the given stochastic process into a Markov or a semi-Markov process by a suitable *state space extension* can be used in some cases by one of the following ways:

1. *Approximation of distribution functions*: Approximating the involved distribution functions (for repair and/or failure-free times) by an *Erlang distribution* (Eq. (A6.102)) allows a transformation of the original process into a time-homogeneous Markov process through introduction of *additional states*.
2. *Introduction of supplementary variables*: Introducing for every element of a system as supplementary variables the failure-free time since the last repair and the repair time since the last failure, the original process can be transformed into a Markov process with state space consisting of discrete and continuous parameters. Investigations usually lead to partial differential equations which have to be solved with corresponding boundary conditions.

The first method is best used when repair and/or failure rates are *monotonically increasing* from zero to a final value, its application is easy to understand (Fig. 6.6). The second method is general [A7.4 (1955)], but often time-consuming.

A further method is based on the general concept of *point process*. Considering the sequence of jump times τ_n^* and states ξ_n entered at these points, an equivalent description of the process $\xi(t)$ is obtained by a marked point process (τ_n^*, ξ_n) , $n=0, 1, \dots$. Analysis of the system's *steady-state* behavior follows using *Korolyuk's* theorem $\Pr\{\text{jump into } Z_i \text{ during } (t, t+\delta t)\} = \lambda_i^\Delta \delta t + o(\delta t)$, with $\lambda_i^\Delta = E[\text{number of jumps in } Z_i \text{ during the unit time interval}]$, see e. g. [A7.11, A7.12]. As an example, consider a repairable *coherent system with n totally independent elements* (p.61). Let $\zeta_1(t), \dots, \zeta_n(t)$ and $\zeta(t)$ be the binary processes with states 0 (*down*) & 1 (*up*) describing elements and system, respectively. If the *steady-state point availability* of every element

$$\lim_{t \rightarrow \infty} PA_i(t) = \lim_{t \rightarrow \infty} \Pr\{\zeta_i(t)=1\} = PA_i = \frac{MTF_i}{MTF_i + MTTR_i}, \quad i = 1, \dots, n,$$

exists, then the steady-state point availability of the system is given by Eq. (2.48) and can be expressed as (see e. g. [6.3, A7.10])

$$PA_S = MTF_S / (MTF_S + MTTR_S). \quad (\text{A7.189})$$

However, investigation of the time behavior of systems with arbitrary failure and/or repair rates can become time-consuming. In these cases, *approximate expressions* (Sections 6.7, 6.9.7) or Monte Carlo simulations (Sec. 6.9.6.2) can help to get results.

A7.8.2 Nonhomogeneous Poisson Processes (NHPP)

A *nonhomogeneous Poisson process* (NHPP) is a *point process with independent Poisson distributed increments*, i.e., a sequence of points (events) on the time axis, whose count function $v(t)$ has independent increments (in nonoverlapping intervals) and satisfy

$$\Pr\{v(t)=k\} = \frac{(M(t))^k}{k!} e^{-M(t)}, \quad t > 0, k=0,1, \dots, v(t)=0 \text{ for } t \leq 0, M(t)=E[v(t)]. \quad (\text{A7.190})$$

$v(t)$ gives the number of events in $(0, t]$. In the following, $v(t)$ is assumed right continuous with unit jumps. $M(t)$ is the *mean* of $v(t)$, called *mean value function*,

$$M(t)=E[v(t)], \quad t > 0, M(t)=0 \text{ for } t \leq 0, \quad (\text{A7.191})$$

and it holds that (Eqs. (A6.127) & (A6.128), Example A6.21)

$$\text{Var}[v(t)] = E[v(t)] = M(t), \quad t > 0, M(t)=0 \text{ for } t \leq 0. \quad (\text{A7.192})$$

$M(t)$ is a nondecreasing, continuous function with $M(t)=0$ for $t \leq 0$, often assumed increasing, unbounded, and absolutely continuous. If

$$m(t) = dM(t)/dt \geq 0, \quad t > 0, m(t)=0 \text{ for } t \leq 0, \quad (\text{A7.193})$$

exists, $m(t)$ is the *intensity* of the NHPP. Eqs. (A7.193) and (A7.191) yield

$$\Pr\{v(t+\delta t) - v(t) = 1\} = m(t)\delta t + o(\delta t), \quad t > 0, \delta t \downarrow 0, \quad (\text{A7.194})$$

and no distinction is made between *arrival rate* and *intensity*. Equation (A7.194) gives the *unconditional* probability for *one* event (e.g. failure) in $(t, t+\delta t]$. $m(t)$ corresponds to the *renewal density* $h(t)$ (Eq. (A7.24)) but *differs basically* from the *failure rate* $\lambda(t)$, see remark on p. 378. Equation (A7.194) also shows that an NHPP is locally *without aftereffect*. This holds globally (Eq.(A7.195)) and characterizes the NHPP. However, *memoryless*, i.e. with *independent and stationary increments*, is only the *homogeneous* Poisson process (HPP), for which $M(t) = \lambda t$ holds.

Nonhomogeneous Poisson processes have been greatly investigated in the literature, see e.g. [6.3, A7.3, A7.12, A7.21, A7.25, A7.30, A8.1]. This appendix gives some important results useful for reliability analysis. These results hold for HPPs ($M(t) = \lambda t$) as well, and *most of them are a direct consequence of the independent increments property*. In particular, the number of events in a time interval $(a, b]$

$$\Pr\{k \text{ events in } (a, b] \mid H_a\} = \Pr\{k \text{ events in } (a, b]\} = \frac{(M(b)-M(a))^k}{k!} e^{-(M(b)-M(a))},$$

$$k=0,1,\dots, 0 < a < b, \quad (\text{A7.195})$$

and the rest waiting time $\tau_R(t)$ from an arbitrary $t > 0$ to the next event

$$\Pr\{\tau_R(t) > x \mid H_t\} = \Pr\{\text{no event in } (t, t+x] \mid H_t\}$$

$$= \Pr\{\text{no event in } (t, t+x]\} = e^{-(M(t+x)-M(t))}, \quad t, x > 0, \quad (\text{A7.196})$$

are independent of the process development up to time t (history H_a or H_t); i.e. the Poisson process is a process *without aftereffect* (memoryless if homogeneous). The mean $E[\tau_R(t)]$ is thus also independent of the process development up to time t

$$E[\tau_R(t)] = \int_0^\infty e^{-(M(t+x)-M(t))} dx. \quad (\text{A7.197})$$

Let now $0 < \tau_1^* < \tau_2^* < \dots$ be the *occurrence times* (arrival times) of the event considered (e.g. failures of a repairable system), measured from the origin $t = \tau_0^* = 0$ and taking values $0 < t_1^* < t_2^* < \dots$ ^{+) Furthermore, let $\eta_n = \tau_n^* - \tau_{n-1}^*$ be the n th *interarrival time* ($n \geq 1$). Considering $M(0)=0, t > 0, \tau_0^* = t_0^* = 0$, and assuming $M(t)$ *derivable, strictly increasing* ($m(t) > 0$), and *unbounded* ($M(\infty) = \infty$), the following holds:}

1. The *occurrence times* (arrival times) $\tau_1^*, \tau_2^*, \dots$ have joint density

$$f(t_1^*, t_2^*, \dots, t_n^*) = \prod_{i=1}^n m(t_i^*) e^{-(M(t_i^*)-M(t_{i-1}^*))} = e^{-M(t_n^*)} \prod_{i=1}^n m(t_i^*), \quad t_0^* = 0 < t_1^* < \dots < t_n^*,$$

$$(\text{A7.198})$$

(follows from Eqs. (A7.194) & (A7.195)) and marginal distribution function

$$F_i(t_i^*) = \Pr\{\tau_i^* \leq t_i^*\} = 1 - \sum_{k=0}^{i-1} \frac{M(t_i^*)^k}{k!} e^{-M(t_i^*)} = \int_0^{M(t_i^*)} \frac{x^{i-1}}{(i-1)!} e^{-x} dx, \quad i=1, 2, \dots, \quad (\text{A7.199})$$

with density $f_i(t_i^*) = m(t_i^*) M(t_i^*)^{i-1} e^{-M(t_i^*)} / (i-1)!$ & mean $E[\tau_i^*] = \int_0^\infty x f_i(x) dx$ (events $\{\tau_i^* \leq t_i^*\}$ and $\{\text{at least } i \text{ events have occurred in } (0, t_i^*]\}$ are equivalent).

2. The quantities

$$\psi_1^* = M(\tau_1^*) < \psi_2^* = M(\tau_2^*) < \dots \quad (\text{A7.200})$$

are the occurrence times in an HPP with *intensity one* ($M(t) = t$) (follows from $v_{\psi^*}(M(t)) = v_{\tau^*}(t) \rightarrow v_{\psi^*}(t) = v_{\tau^*}(M^{-1}(t)) \Rightarrow E[v_{\psi^*}(t)] = E[v_{\tau^*}(M^{-1}(t))] = M(M^{-1}(t)) = t$).

3. The conditional distribution functions of η_{n+1} & τ_{n+1}^* given $\eta_1 = x_1, \dots, \eta_n = x_n$ are

$$\Pr\{\eta_{n+1} \leq x \mid \eta_1 = x_1, \dots, \eta_n = x_n\} = \Pr\{\eta_{n+1} \leq x \mid x_1 + \dots + x_n = t_n^*\}$$

$$= 1 - e^{-(M(t_n^*+x)-M(t_n^*))} = 1 - e^{-\int_{t_n^*}^{t_n^*+x} m(y) dy} = 1 - \Pr\{\text{no event in } (t_n^*, t_n^*+x]\}, \quad (\text{A7.201})$$

^{+) *} is used to explicitly show that t_1^*, t_2^*, \dots (as realizations of $\tau_1^*, \tau_2^*, \dots$) are points on the time axis and not independent observations of a random variable τ (e.g. as in Figs. 1.1, 7.12 & 7.14).

and

$$\Pr\{\tau_{n+1}^* \leq t \mid x_1 + x_2 + \dots + x_n = t_n^*\} = 1 - e^{-(M(t) - M(t_n^*))}, \quad n \geq 1, t > t_n^*, \quad (\text{A7.202})$$

(both follow directly from Eq. (A7.196)).

4. For given (fixed) $t = T$ and $v(T) = n$ (time censoring), the joint density of the occurrence times $0 < \tau_1^* < \dots < \tau_n^* < T$ under the condition $v(T) = n$ is given by

$$f(t_1^*, t_2^*, \dots, t_n^* \mid n) = n! \prod_{i=1}^n (m(t_i^*) / M(T)), \quad 0 < t_1^* < \dots < t_n^* < T, \quad n = 1, 2, \dots, \quad (\text{A7.203})$$

(see Eq. (A7.210)) and that of $0 < \tau_1^* < \dots < \tau_n^* < T \cap v(T) = n$ is

$$f(t_1^*, t_2^*, \dots, t_n^*, n) = f(t_1^*, t_2^*, \dots, t_n^* \mid n) \cdot \frac{M(T)^n e^{-M(T)}}{n!} = e^{-M(T)} \prod_{i=1}^n m(t_i^*), \quad 0 < t_1^* < \dots < t_n^* < T, \quad n = 1, 2, \dots, \quad (\text{A7.204})$$

(follows from Eqs. (A7.203) and (A7.190)). From Eq. (A7.203) one recognizes that for given (fixed) $t = T$ and $v(T) = n$, the occurrence times $0 < \tau_1^* < \dots < \tau_n^* < T$ have the same distribution as if they were the *order statistic* of n independent identically distributed random variables with density

$$m(t) / M(T), \quad 0 < t < T, \quad (\text{A7.205})$$

& distribution function $M(t) / M(T)$ on $(0, T)$ (compare Eqs. (A7.210), (A7.211)).

5. Furthermore, for given (fixed) $t = T$ and $v(T) = n$, the quantities

$$0 < M(\tau_1^*) / M(T) < \dots < M(\tau_n^*) / M(T) < 1 \quad (\text{A7.206})$$

have the same distribution as if they were the *order statistic* of n independent identically distributed random variables uniformly distributed on $(0, 1)$ (follows from Point 2 above (Eqs. (A7.200) & (A7.213)). For *failure censoring* (test stopped at t_n^*), Eqs. (A7.203) - (A7.206) and (A7.210) - (A7.213) hold, taking $T = t_n^* - 0$ and multiplying over $n-1$ instead of n , yielding e. g. $f(t_1^*, \dots, t_{n-1}^* \mid n-1) = (n-1)! \prod_{i=1}^{n-1} (m(t_i^*) / M(t_n^*))$ for Eq. (A7.210).

6. The quantity

$$(v(t) - M(t)) / \sqrt{M(t)} \quad (\text{A7.207})$$

has for $t \rightarrow \infty$ a standard normal distribution (follows from the central limit theorem for renewal processes (Eq. (A7.34)) and Eqs. (A7.191) & (A7.192)).

7. The sum of n independent NHPPs with mean value function $M_i(t)$ and intensity $m_i(t)$ is an NHPP with mean value function and intensity

$$M(t) = \sum_{i=1}^n M_i(t) \quad \text{and} \quad m(t) = \sum_{i=1}^n m_i(t), \quad M_i(t) = m_i(t) = 0 \text{ for } t \leq 0, \quad (\text{A7.208})$$

respectively (follows from the *independent increments* property of NHPPs and Eq. (A7.190), see Eq. (7.27) for HPPs).

From the above properties, the following conclusions can be drawn:

1. For $i = 1$, Eq. (A7.199) yields

$$\Pr\{\tau_1^* \leq t\} = 1 - e^{-M(t)} = 1 - e^{-\int_0^t m(x) dx}; \tag{A7.209}$$

thus, comparing Eqs. (A7.209) & (A6.26) it follows that the *intensity* of an NHPP is equal to the *failure rate of the first occurrence time* $\eta_1 = \tau_1^*$ (see also Point 2).

2. Taking $\partial/\partial x$ in Eq. (A7.201), Eq. (A6.25) show that the *failure rate referred to the interarrival time* $\eta_{n+1} = \tau_{n+1}^* - \tau_n^*$ given $\tau_n^* = t_n^*$ is independent of the process development up to the time t_n^* and is equal to the *failure rate at time $t_n^* + x$ referred to the first interarrival time η_1 or arrival time τ_1^* ($\eta_1 = \tau_1^*$)*; i.e., for $n \geq 1$, $\lambda_{\eta_{n+1}}(x | t_n^*) = m(t_n^* + x) = \lambda_{\eta_1}(t_n^* + x)$, as per Eq. (A6.28). This leads to the concept of *as-bad-as-old*, used in some considerations on repairable systems subjected to minimal repair (only failed parts are restored to as-good-as-new, Section 4.6.2). However, if a repaired part has a time dependent failure rate, the system failure rate can not, after repair, be the same as just before failure (\approx in (i) on p. 427).

Example A7.13

Show that for *given* (fixed) T and $v(T) = n$, the occurrence times $0 < \tau_1^* < \dots < \tau_n^* < T$ in a non homogeneous Poisson Process with *intensity* $m(t)$ have the same joint density as the *order statistic* of n independent identically distributed random variables with density $m(t)/M(T)$ on $(0, T)$.

Solution

For an NHPP with *intensity* $m(t)$, the occurrence times $0 < \tau_1^* < \dots < \tau_n^* < T$ given T (fixed) and $v(T) = n$ have joint density (Eqs. (A7.194) & (A7.195) and considering $0 < t_1^* < \dots < t_n^* < T$)

$$f(t_1^*, t_2^*, \dots, t_n^* | n) = f(t_1^*, t_2^*, \dots, t_n^*, n) / (M(T)^n e^{-M(T)} / n!) = m(t_1^*) e^{-(M(t_1^*))} m(t_2^*) e^{-(M(t_2^*) - M(t_1^*))} \dots m(t_n^*) e^{-(M(t_n^*) - M(t_{n-1}^*))} e^{-(M(T) - M(t_n^*))} / (M(T)^n e^{-M(T)} / n!) = n! \prod_{i=1}^n (m(t_i^*) / M(T)). \tag{A7.210}$$

Furthermore, considering that for a set of n realizations of a given random variable there are $n!$ permutations giving the same order statistic (p.526), the joint density of the *order statistic* of n independent identically distributed random variables with density $m(t)/M(T)$ on $(0, T)$ is given by

$$f(t_1^*, t_2^*, \dots, t_n^* | n) = n! \prod_{i=1}^n (m(t_i^*) / M(T)) \quad \text{on } (0, T), \quad 0 < t_1^* < t_2^* < \dots < t_n^* < T. \tag{A7.211}$$

Supplementary results: For a *homogeneous Poisson Process* (HPP), Eq. (A7.205) yields

$$m(t)/M(T) = 1/T \quad \& \quad f(t_1^*, \dots, t_n^* | n) = n! / T^n \quad \text{on } (0, T). \tag{A7.212}$$

Furthermore, when considering τ_i^*/T , Eq. (A7.205) and point VII in Example A6.18 with $C = 1/T$ (p. 448) yield

$$T \cdot m(t \cdot T) / M(T) = T \cdot \lambda / \lambda T = 1 \quad \& \quad f(t_1^*, \dots, t_n^* | n) = n! \quad \text{on } (0, 1). \tag{A7.213}$$

Thus, for given (fixed) T and $v(T) = n$, arrival times $0 < \tau_1^* < \dots < \tau_n^* < T$ of an HPP have the same distribution as if they were the *order statistic* of n independent identically uniformly distributed random variables on $(0, T)$, on $(0, 1)$ for $0 < \tau_1^*/T < \dots < \tau_n^*/T < 1$.

3. From Eq. (A7.202), the distribution of the occurrence time τ_{n+1}^* depends only on τ_n^* ; thus, $\tau_1^*, \tau_2^*, \dots$ is a *Markov sequence*.
4. From Eq. (A7.204) one can obtain Eq.(A7.198) when considering that $\Pr\{\text{no event in } (t_n^*, T]\} = e^{-(M(T)-M(t_n^*))}$, and vice versa.
5. Equations (A7.198) and (A7.199) show that for an NHPP, occurrence (arrival) times are *not independent*; the same is for interarrival times, which are *neither independent nor identically distributed*.

Thus, the NHPP is *not a regenerative process*. On the other hand, the *homogeneous Poisson processes (HPP)* is a renewal process, with independent interarrival times distributed according to the *same exponential distribution* (Eq. (A7.38)) and independent Erlang (Gamma) distributed occurrence times (Eqs. (A7.39)). & (A6.102) However, because of *independent increments*, the NHPP is *without aftereffect (memoryless* if HPP) and the sum of Poisson processes is a Poisson process, both in homogeneous and non-homogeneous case (Eq. (7.27)). Convergence of a point process to an NHPP or to an HPP is discussed in Appendices A7.8.3 and A7.8.5.

Although appealing, the assumption of independent increments, mandatory for Poisson processes (HPP and NHPP), can limit the validity of models used in practical applications with arbitrary failure and / or repair rates.

However, the properties in Points 1-7 above (in particular Eqs. (A7.200) & (A7.206)) are useful for statistical tests on NHPPs, as well as for *Monte Carlo simulations*. Results for exponential distributions or for HPPs can be used and the *Kolmogorov-Smirnov test* holds with $F_0(t) = M_0(t)/M_0(T)$ & $\hat{F}_n(t) = v(t)/v(T)$ (Section 7.6). Equation (A7.205) is useful to *generate realizations* of an NHPP (generate k for given T and $M(T)$ (Eq. (A7.190)), then k random variables with density $m(t)/M(T)$; the ordered values are the k occurrence times of the NHPP on $(0, T)$, see also p. 291; same for a homogeneous Poisson process, using $M(T) = \lambda T$.

A7.8.3 Superimposed Renewal Processes

Consider a repairable *series system* with n totally independent elements (p. 52) and assume that repair times are *negligible* and that after each repair (renewal) the repaired *element* is as-good-as-new. Let $MTTF_i$ be the mean time to failure of element E_i and $MTTF_S$ that of the system. The *flow of system failures* is given by the *superposition of n independent renewal processes*, each of them related to an element of the system. If $v_S(t)$ is the count function at system level giving the number of system failures in $(0, t]$ and $v_i(t)$ that of element E_i , it holds that

$$v_S(t) = \sum_{i=1}^n v_i(t), \quad t > 0, v_i(t) = 0 \text{ for } t \leq 0, i = 1, 2, \dots, n. \tag{A7.214}$$

$v_i(t)$ is a random variable, distributed as per Eq. (A7.12). Thus, for the *mean value*

function at system level $Z_S(t)$ it follows that (Eqs. (A6.68) and (A7.15))

$$Z_S(t) = E[v_S(t)] = \sum_{i=1}^n E[v_i(t)] = \sum_{i=1}^n H_i(t), \quad t > 0, Z_S(t) = 0 \text{ for } t \leq 0, \quad (\text{A7.215})$$

yielding for the failure intensity at system level $z_S(t)$ (Eq. (A7.18))

$$z_S(t) = dZ_S(t)/dt = \sum_{i=1}^n dH_i(t)/dt = \sum_{i=1}^n h_i(t), \quad t > 0, z_S(t) = 0 \text{ for } t \leq 0. \quad (\text{A7.216})$$

In Eqs. (A7.215) and (A7.216), $H_i(t)$ and $h_i(t)$ are the renewal function and renewal density of the renewal process related to element E_i . However, the point process yielding $v_S(t)$ is *not a renewal process*. Simple results hold for homogeneous Poisson processes (HPP) only, whose sum is an HPP (Eq. (7.27)) and thus a renewal process. The same holds for nonhomogeneous Poisson processes (NHPP), but an NHPP is not a renewal process.

For independent renewal processes, it can be shown that:

1. The sum of n independent stationary renewal processes is a stationary renewal process with renewal density (follows from Eqs. (A7.36) & (A7.215))

$$h_S(t) = h_S = \frac{H_S(t)}{t} = \frac{E[v_S(t)]}{t} = \frac{1}{MTF_S} = \sum_{i=1}^n \frac{1}{MTF_i}, \quad t > 0, h_S(t) = 0 \text{ for } t \leq 0. \quad (\text{A7.217})$$

2. For $t \rightarrow \infty$, $v_S(t)$ is normally distributed (Eqs. (A7.214) & (A7.34), Example A6.17).
3. For $n \rightarrow \infty$, the sum of n independent renewal processes with very low occurrence (one occurrence of any type and ≥ 2 occurrences of all types are unlikely) and for which $\lim_{n \rightarrow \infty} \sum_{i=1}^n \Pr\{v_i(t) - v_i(a) = 1\} = M(t) - M(a)$ holds for any fixed t and $a < t$, converge to an NHPP with $E[v(t)] = M(t)$ for all $t > 0$ (Grigelionis [A7.14], see also [A7.12, A7.30]); furthermore, if all renewal densities $h_i(t)$ are bounded (at $t \rightarrow 0$), the sum converge for $n \rightarrow \infty$ to an HPP [A7.14].
4. For $t \rightarrow \infty$ and $n \rightarrow \infty$, the sum of n independent renewal processes with low occurrence (one occurrence of any type is unlikely) converge to an HPP with renewal density as per Eq. (A7.217) [A7.17], see also [A7.8, A7.12, A7.30].

A7.8.4 Cumulative Processes

Cumulative processes [A7.24(1955), A7.4(1962)], also known as *compound processes* [A7.3, A7.9 (Vol. 2), A7.21], are obtained when at the occurrence of each event in a point process, a random variable is generated and the stochastic process given by the sum of these random variables is considered. The involved point process is often limited to a renewal process (including the homogeneous Poisson process (HPP), yielding a cumulative or *compound Poisson process*) or a nonhomogeneous Poisson process (NHPP). The generated random variable are independent, if not otherwise stated, and can have arbitrary distribution. Cumulative processes can be used to

model some practical situations; for instance, the *total maintenance cost* for a repairable system over a given period of time or the *cumulative damage* caused by random shocks on a mechanical structure (assuming linear damage superposition). If a subsidiary series of events is generated instead of a random variable and the two types of events are indistinguishable, the process is a *branching process* [A7.3, A7.21, A7.30], discussed e. g. in [6.1, A7.4(1968)] as a model to describe failure occurrence when secondary failures are triggered by primary failures.

Let $v(t)$ be the count function giving the number of events (on the time axis) of the involved point process (Fig. A7.1), ξ_i the generated random variable at the occurrence of the i th event, and ξ_t the sum of ξ_i over $(0, t]$

$$\xi_t = \sum_{i=1}^{v(t)} \xi_i, \quad v(t)=1, 2, \dots, t > 0, v(t)=0 \text{ for } t \leq 0, \xi_t=0 \text{ for } v(t)=0. \quad (\text{A7.218})$$

The stochastic process of value ξ_t ($t \geq 0$) is a *cumulative process*.

Assuming that the random variables ξ_i are > 0 , (totally) independent, independent from $v(t)$ and distributed according to $G(x)$, it is not difficult to recognize that ξ_t is distributed as the total repair time (*total down time*) for failures occurred in a total operating time (*total up time*) t of a repairable item, and is thus given by the *work-mission availability* (Eq. (6.32)).

In the following, results are given for the case in which the involved point process is an HPP with parameter λ and the generated random variables are (totally) independent, independent from $v(t)$, and have same exponential distribution with parameter μ . Equation (6.33) with $T_0 = t$ yields

$$\begin{aligned} \Pr\{\xi_t \leq x\} &= \text{WMA}_{S_0}(t, x) = e^{-\lambda t} + \sum_{n=1}^{\infty} \left[\frac{(\lambda t)^n}{n!} e^{-\lambda t} \left(1 - \sum_{k=0}^{n-1} \frac{(\mu x)^k}{k!} e^{-\mu x} \right) \right] \\ &= 1 - e^{-(\lambda + \mu x)} \sum_{n=1}^{\infty} \left[\frac{(\lambda t)^n}{n!} \sum_{k=0}^{n-1} \frac{(\mu x)^k}{k!} \right], \quad t > 0 \text{ given, } x > 0, \Pr\{\xi_t = 0\} = e^{-\lambda t}. \end{aligned} \quad (\text{A7.219})$$

Mean and variance of ξ_t follow as (Eqs. (A7.219), (A6.38), (A6.45), (A6.41))

$$E[\xi_t] = \lambda t / \mu \quad \text{and} \quad \text{Var}[\xi_t] = 2\lambda t / \mu^2. \quad (\text{A7.220})$$

Furthermore, for $t \rightarrow \infty$ the distribution of ξ_t approaches a normal distribution with mean and variance as per Eq. (A7.220) (see the discussion to Eq. (6.33)). Moments of ξ_t can also be obtained using the moment generating function (Table A9.7a) or directly by considering Eq. (A7.218), yielding (Example A7.14)

$$E[\xi_t] = E[v(t)]E[\xi_i] \quad \text{and} \quad \text{Var}[\xi_t] = E[v(t)]\text{Var}[\xi_i] + \text{Var}[v(t)]E^2[\xi_i]. \quad (\text{A7.221})$$

Of interest in practical applications (e. g. cost optimizations) can also be the distribution of the time τ_C at which the process ξ_t ($t > 0$) crosses a give (fixed) barrier C . For the case given by Eq. (A7.219), in particular for $\xi_i > 0$, the events

$$\{\tau_C > t\} \quad \text{and} \quad \{\xi_t \leq C\} \quad (\text{A7.222})$$

are equivalent. Form Eq. (A7.219) it follows then (C has dimension of μ^{-1})

$$\Pr\{\tau_C > t\} = 1 - e^{-(\lambda t + \mu C)} \sum_{n=1}^{\infty} \left[\frac{(\lambda t)^n}{n!} \sum_{k=0}^{n-1} \frac{(\mu C)^k}{k!} \right], \quad C > 0 \text{ given, } t > 0. \quad (\text{A7.223})$$

A7.8.5 General Point Processes

A point process is an ordered sequence of points on the time axis, giving for example the failure occurrence of a repairable system. Poisson and renewal processes are simple examples of point processes. Assuming that simultaneous events can not occur (with probability one) and assigning to the point process a count function $v(t)$ giving the number of events occurred in $(0, t]$, investigation of point processes can be performed on the basis of the involved count function $v(t)$. However, arbitrary point processes can lead to analytical difficulties, and results are known only for particular situations (low occurrence rate, stationary, regular, etc.). In reliability applications, general point processes can appear for example when investigating failure occurrence of repairable systems by neglecting repair times. In the following, only some basic properties of general point processes will be discussed, see e. g. [A7.10, A7.11, A7.12, A7.30] for greater details.

Let $v(t)$ be a count function giving the number of events occurred in $(0, t]$, assume $v(0) = 0$ and that simultaneous occurrences are not possible. The underlying point process is *stationary* if $v(t)$ has stationary increments (Eq. (A7.5)), and *without aftereffect* if $v(t)$ has independent increments (Eq. (A7.2)). The sum of

Example A7.14

Prove Eq. (A7.221).

Solution

Considering $\xi_i > 0$, (mutually) independent, independent of $v(t)$ and with finite mean & variance, Eq. (A7.218) yields, for given (fixed) $v(t) = n$ (Appendix A6.8)

$$E[\xi_t | v(t) = n] = n E[\xi_i] \quad \text{and} \quad \text{Var}[\xi_t | v(t) = n] = n \text{Var}[\xi_i]. \quad (\text{A7.224})$$

From Eq. (A7.224) it follows then (considering $v(t) = 1, 2, \dots$)

$$\begin{aligned} E[\xi_t] &= \sum_{n=1}^{\infty} \Pr\{v(t) = n\} E[\xi_t | v(t) = n] = \sum_{n=1}^{\infty} \Pr\{v(t) = n\} n E[\xi_i] \\ &= E[\xi_i] \sum_{n=1}^{\infty} n \Pr\{v(t) = n\} = E[\xi_i] E[v(t)]. \end{aligned} \quad (\text{A7.225})$$

For $\text{Var}[\xi_t]$, it holds that (Eq. (A6.45)) $\text{Var}[\xi_t] = E[\xi_t^2] - E^2[\xi_t]$; from which, considering $\xi_t^2 = (\xi_1 + \dots + \xi_{v(t)})^2$ and Eqs. (A7.225), (A6.69), and (A6.45),

$$\begin{aligned} \text{Var}[\xi_t] &= E[v(t) \cdot \xi_i^2 + v(t)(v(t) - 1) \cdot \xi_i \xi_j] - (E[v(t)] E[\xi_i])^2 \\ &= E[v(t)] E[\xi_i^2] + E[v^2(t)] E^2[\xi_i] - E[v(t)] E^2[\xi_i] - (E[v(t)] E[\xi_i])^2 \\ &= E[v(t)] \text{Var}[\xi_i] + \text{Var}[v(t)] E^2[\xi_i]. \end{aligned} \quad (\text{A7.226})$$

independent stationary point processes is a stationary point process. The same holds for processes without aftereffect. However, only the *homogeneous Poisson process* (HPP) is stationary and without aftereffect (*memoryless*).

For a general point process, a *mean value function*

$$Z(t) = E[v(t)], \quad t > 0, Z(t) = 0 \text{ for } t \leq 0, \quad (\text{A7.227})$$

giving the mean (expectation) of the number of points (events) in $(0, t]$ can be defined. $Z(t)$ is a nondecreasing, continuous function with $Z(0) = 0$, often assumed increasing, unbounded and absolutely continuous. If

$$z(t) = \frac{dZ(t)}{dt} = \frac{dE[v(t)]}{dt} \geq 0, \quad t > 0, z(t) = 0 \text{ for } t \leq 0, \quad (\text{A7.228})$$

exists, $z(t)$ is the *intensity of the point process*. Equations (A7.228) & (A7.227) yield

$$\Pr\{v(t+\delta t) - v(t) = 1\} = z(t)\delta t + o(\delta t), \quad t > 0, \delta t \downarrow 0, \quad (\text{A7.229})$$

and no distinction is made between *arrival rate* and *intensity*. $z(t)\delta t$ gives the *unconditional* probability for *one* event (failure) in $(t, t+\delta t]$. $z(t)$ corresponds thus to $m(t)$ (Eq. (A7.193)) and $h(t)$ (Eq. (A7.24)), but *differs basically* from the *failure rate* $\lambda(t)$ (Eq. (A6.25)) which gives (as $\lambda(t)\delta t$) the *conditional* probability for a failure in $(t, t+\delta t]$ given that the item was new at $t=0$ and *no failure has occurred* in $(0, t]$. This distinction is important also for the case of a *homogeneous Poisson process* (Appendix A7.2.5), for which $\lambda(x) = \lambda$ holds for *all interarrival times* (with x starting by 0 at every renewal point) and $h(t) = \lambda$ holds for the whole process. Misuses are known, in particular when dealing with reliability data analysis (see e.g. [6.1, A7.30] and comments on pp. 378 & 380, Appendix A7.8.2, and Sections 1.2.3, 7.6, 7.7). Thus, as a first rule to avoid confusion,

for repairable items, it is mandatory to use for interarrival times the variable x starting by 0 at every repair (renewal), instead of t .

Some limits theorems on point processes are known, in particular on the convergence to an HPP, see e.g. [A7.10, A7.11, A7.12].

In reliability applications, $z(t)$ is called *failure intensity* [A1.4], *ROCOF* (rate of occurrence of failures) in [6.1]. $z(t)$ applies in particular to repairable systems when repair (restoration) times are neglected. In this case, $v_S(t)$ is the count function giving the number of system failures occurred in $(0, t]$, with $v(0) = 0$, and

$$z_S(t) = \frac{dZ_S(t)}{dt} = \frac{dE[v_S(t)]}{dt} \geq 0, \quad t > 0, z_S(t) = 0 \text{ for } t \leq 0, \quad (\text{A7.230})$$

is the *system failure intensity*.

A8 Basic Mathematical Statistics

Mathematical statistics deals basically with situations which can be described as follows: Given a population of *statistically identical and independent elements* with unknown statistical properties, measurements regarding these properties are made on a (random) sample of this population and on the basis of the collected data, conclusions are made for the *remaining elements* of the population. Examples are the estimation of an unknown probability (e. g. a defective probability p), the parameter estimation for the distribution function of an item's failure-free time τ , or a decision whether the mean of τ is greater than a given value. Mathematical statistics thus goes from *observations* (realizations) of a given (random) event in a series of *independent trials* to search for a suitable *probabilistic model* for the event considered (inductive approach). Methods used are based on probability theory and *results obtained can only be formulated in a probabilistic language*. Risk minimization for a false conclusion is an important objective in mathematical statistics. This Appendix introduces the basic concepts of mathematical statistics necessary for the quality and reliability tests given in Chapter 7. It is a compendium of mathematical statistics, consistent from a mathematical point of view but still with reliability engineering applications in mind (demonstration of established theorems is referred, and for all other propositions or equations, sufficient details for complete demonstration are given). Emphasis is on *empirical methods, parameter estimation, and testing of hypotheses*. To simplify the notation, *sample* is used for *random sample*, *mean* for *expected value*, and *independent* for *totally* (mutually, statistically, stochastically) *independent* (p. 419). Estimated (or empirical) values are marked with $\hat{\cdot}$. Selected examples illustrate the practical aspects.

A8.1 Empirical Methods

Empirical methods allow a quick and easy evaluation/estimation of the distribution function and of the mean, variance, and other moments characterizing a random variable. These *estimates* are based on the empirical distribution function and have a great intuitive appeal. An advantage of the empirical distribution function, when plotted on an appropriate probability charts (probability plot papers, p.531), is to give a simple visual rough check as to whether the assumed model seems correct.

A8.1.1 Empirical Distribution Function

A *sample* of size n of a random variable τ with the distribution function $F(t)$ is a random vector $\vec{\tau} = (\tau_1, \dots, \tau_n)$ whose components τ_i are assumed (totally) *independent* and *identically distributed* random variables with $F(t) = \Pr\{\tau_i \leq t\}$, $i = 1, \dots, n$. For instance, τ_1, \dots, τ_n are the *failure-free times* (*failure-free operating time*) of n items randomly selected from a lot of statistically identical items with a distribution function $F(t)$ for the failure-free time τ . The *observed* failure-free times, i.e. the *realization* of the random vector $\vec{\tau} = (\tau_1, \dots, \tau_n)$, is a set t_1, \dots, t_n of independent real values (> 0 in the case of failure-free times). Distinction between random variables τ_1, \dots, τ_n and their observations t_1, \dots, t_n is important from a mathematical point of view.⁴⁾

When the sample elements (*observations*) are ordered by increasing magnitude, an *order statistic* (order sample) $t_{(1)}, \dots, t_{(n)}$ is obtained. In life tests, observations t_1, \dots, t_n constitute often themselves an order statistic. An advantage of an order statistic of n observations on independent, identically distributed random variables with density $f(t)$ is the simple form of the joint density $f(t_{(1)}, \dots, t_{(n)}) = n! \Pi_i f(t_{(i)})$ (Example (A7.13, on p. 519).

With the purpose of saving test duration and cost, life tests can be terminated (stopped) at the occurrence of the k th ordered observation (k th failure) or at a given (fixed) time T_{test} . If the test is stopped at the k th failure, a *type II censoring* occurs (from the left if the time origin of all observations is not known). A *type I censoring* occurs if the test is stopped at T_{test} . A third possibility is to stop the test at a given (fixed) number k of observations (failures) or at T_{test} whenever the first occurs. The corresponding test plans are termed (n, \bar{r}, k) , (n, \bar{r}, T_{test}) , and $(n, \bar{r}, (k, T_{test}))$, respectively, where \bar{r} stands for "without replacement". In many applications, failed items can be replaced (for instance in the case of a repairable item or system); in these cases, \bar{r} is changed with r in the test plans.

For a set of ordered observations $t_{(1)}, \dots, t_{(n)}$, the right continuous function

$$\hat{F}_n(t) = \begin{cases} 0 & \text{for } t < t_{(1)} \\ \frac{i}{n} & \text{for } t_{(i)} \leq t < t_{(i+1)}, \\ 1 & \text{for } t \geq t_{(n)} \end{cases} \quad i = 1, 2, \dots, n-1, \quad (\text{A8.1})$$

is the *empirical distribution function* (EDF) of the random variable τ , see Fig. A8.1 for a graphical representation. $\hat{F}_n(t)$ expresses the relative frequency of the event $\{\tau \leq t\}$ in n independent trial repetitions, and provides a well defined estimate of

⁴⁾ The investigation of statistical methods and the discussion of their properties can only be based on the (random) *sample* τ_1, \dots, τ_n . However, in applying the methods for a numerical evaluation (statistical decision), the *observations* t_1, \dots, t_n have to be used. For this reason, the same equation (or procedure) can be applied to τ_i or t_i according to the situation.

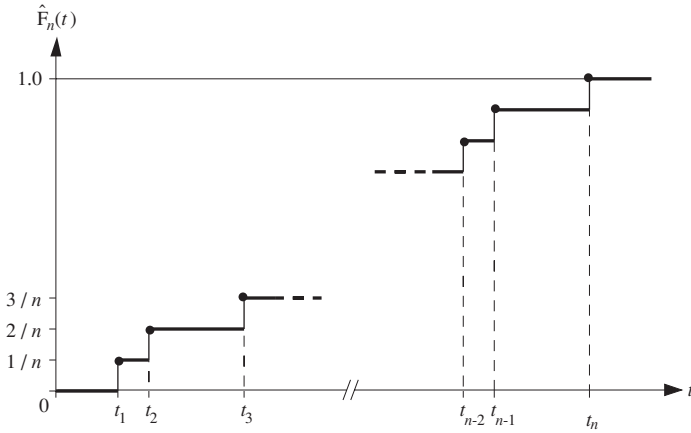


Figure A8.1 Example of an empirical distribution function ($t_1, \dots, t_n \equiv t_{(1)}, \dots, t_{(n)}$ is assumed here)

the distribution function $F(t) = \Pr\{\tau \leq t\}$. The symbol $\hat{}$ is hereafter used to denote an estimate of an unknown quantity. As stated in the footnote on p. 526, when investigating the properties of the empirical distribution function $\hat{F}_n(t)$ it is necessary in Eq. (A8.1) to replace the observations $t_{(1)}, \dots, t_{(n)}$ by the sample elements $\tau_{(1)}, \dots, \tau_{(n)}$.

For given $F(t)$ and any fixed value of t , the number of observations $\leq t$, i.e. $n\hat{F}_n(t)$, is binomially-distributed (Eq. (A6.120)) with parameter $p = F(t)$, mean

$$E[n\hat{F}_n(t)] = nF(t), \tag{A8.2}$$

and variance

$$\text{Var}[n\hat{F}_n(t)] = nF(t)(1 - F(t)), \tag{A8.3}$$

(Eqs. (A6.122) & (A6.123)). Moreover, application of the *strong law of large numbers* (Eq. (A6.146)) shows that for any given (fixed) value of t , $\hat{F}_n(t)$ converges to $F(t)$ with *probability one* for $n \rightarrow \infty$. This convergence is *uniform* in t and holds for the whole distribution function $F(t)$. Proof of this important result is given in the *Glivenko-Cantelli theorem* [A8.4, A8.14, A8.16], which states that the largest absolute deviation between $\hat{F}_n(t)$ and $F(t)$ over all t , i.e.

$$D_n = \sup_{-\infty < t < \infty} \left| \hat{F}_n(t) - F(t) \right|, \tag{A8.4}$$

converges with *probability one* toward 0

$$\Pr\{\lim_{n \rightarrow \infty} D_n = 0\} = 1. \tag{A8.5}$$

In life tests, observations t_1, \dots, t_n constitute often themselves an *order statistic*. This is useful for statistical evaluation of data. However, if the test is stopped at the occurrence of the k th failure or at T_{test} and k or T_{test} are small, the homogeneity of the sample can be questionable and the shape of $F(t)$ could change for $t > t_k$ or $t > T_{test}$ (e.g. because of wear-out, see the remark on p. 342).

A8.1.2 Empirical Moments and Quantiles

The moments of a random variable τ are completely determined by the distribution function $F(t) = \Pr\{\tau \leq t\}$. The empirical distribution $\hat{F}_n(t)$ introduced in Appendix A8.1.1 can be used to estimate the unknown moments of τ .

The observed values $t_{(1)}, \dots, t_{(n)}$ having been fixed, $\hat{F}_n(t)$ can be regarded as the distribution function of a discrete random variable with probability $p_k = 1/n$ at the points $t_{(k)}$, $k = 1, \dots, n$. Using Eq. (A6.35), the corresponding mean is the *empirical mean* (empirical expectation) of τ and is given by

$$\hat{E}[\tau] = \frac{1}{n} \sum_{i=1}^n t_i. \quad (\text{A8.6})$$

Taking into account the footnote on p. 526, $\hat{E}[\tau]$ is a random variable with mean

$$E[\hat{E}[\tau]] = E\left[\frac{1}{n} \sum_{i=1}^n \tau_i\right] = \frac{1}{n} n E[\tau] = E[\tau], \quad (\text{A8.7})$$

and variance

$$\text{Var}[\hat{E}[\tau]] = \text{Var}\left[\frac{1}{n} \sum_{i=1}^n \tau_i\right] = \frac{1}{n^2} n \text{Var}[\tau] = \frac{\text{Var}[\tau]}{n}. \quad (\text{A8.8})$$

Equation (A8.7) shows that $\hat{E}[\tau]$ is an *unbiased estimate* of $E[\tau]$, see Eq. (A8.18). Furthermore, from the *strong law of large numbers* (Eq. (A6.147)) it follows that for $n \rightarrow \infty$, $\hat{E}[\tau]$ converges with probability one toward $E[\tau]$

$$\Pr\left\{\lim_{n \rightarrow \infty} \left(\frac{1}{n} \sum_{i=1}^n \tau_i\right) = E[\tau]\right\} = 1. \quad (\text{A8.9})$$

The exact distribution function of $\hat{E}[\tau]$ is known in a closed simple form only for some particular cases (normal, exponential, Gamma distributions). However, the *central limit theorem* (Eq. (A6.148)) shows that for large values of n the distribution of $\hat{E}[\tau]$ can always be approximated by a *normal distribution* with mean $E[\tau]$ and variance $\text{Var}[\tau]/n$.

Based on $\hat{F}_n(t)$, Eqs.(A6.43) & (A8.6) provide an estimate of the variance of τ as

$$\frac{1}{n} \sum_{i=1}^n (t_i - \frac{1}{n} \sum_{i=1}^n t_i)^2 = \frac{1}{n} \sum_{i=1}^n (t_i - \hat{E}[\tau])^2.$$

This estimate is biased ($E[\frac{1}{n} \sum_{i=1}^n (t_i - \frac{1}{n} \sum_{i=1}^n t_i)^2] = \text{Var}[\tau] (n-1)/n$); as *empirical variance* of τ one defines often

$$\text{V}\hat{\text{ar}}[\tau] = \frac{1}{n-1} \sum_{i=1}^n (t_i - \hat{E}[\tau])^2 = \frac{1}{n-1} [\sum_{i=1}^n t_i^2 - \frac{1}{n} (\sum_{i=1}^n t_i)^2], \tag{A8.10}$$

which is unbiased, i. e.

$$E[\text{V}\hat{\text{ar}}[\tau]] = \text{Var}[\tau]. \tag{A8.11}$$

The empirical *higher-order moments* (Eqs. (A6.41) and (A6.50)) can be estimated with

$$\frac{1}{n} \sum_{i=1}^n t_i^k \quad \text{and} \quad \frac{1}{n-1} \sum_{i=1}^n (t_i - \hat{E}[\tau])^k. \tag{A8.12}$$

The *empirical quantile* \hat{t}_q is defined as the q *quantile* (Appendix A6.6.3) of the empirical distribution function $\hat{F}_n(t)$

$$\hat{t}_q = \inf \{ t: \hat{F}_n(t) \geq q \}. \tag{A8.13}$$

A8.1.3 Further Applications of the Empirical Distribution Function

Comparison of the empirical distribution function $\hat{F}_n(t)$ with a given distribution function $F(t)$ is the basis for several *non-parametric* statistical methods. These include goodness-of-fit tests, confidence bands for distribution functions, and graphical methods using probability charts (probability plot papers).

A quantity often used in this context is the largest absolute deviation D_n between $\hat{F}_n(t)$ and $F(t)$, defined by Eq. (A8.4). If the distribution function $F(t)$ of the random variable τ is continuous, then the random variable $F(\tau)$ is uniformly distributed on $(0, 1)$. It follows that D_n has a distribution independent of $F(t)$. A.N. Kolmogorov showed [A8.20] that for $F(t)$ continuous and $x > 0$,

$$\lim_{n \rightarrow \infty} \Pr\{\sqrt{n} D_n \leq x \mid F(t)\} = 1 + 2 \sum_{k=1}^{\infty} (-1)^k e^{-2k^2 x^2}.$$

The series converges rapidly for $x > 1$, or $y = x/\sqrt{n} > 1/\sqrt{n}$, so that $k = 1$ yields

$$\lim_{n \rightarrow \infty} \Pr\{D_n \leq y \mid F(t)\} \approx 1 - 2e^{-2ny^2}. \tag{A8.14}$$

Table A8.1 Values of $y_{1-\alpha}$, for which $\Pr\{D_n \leq y_{1-\alpha} \mid F(t)\} = 1 - \alpha$

n	$a = 0.2$	$a = 0.1$	$a = 0.05$
2	0.684	0.776	0.842
5	0.447	0.509	0.563
10	0.323	0.369	0.409
20	0.232	0.265	0.294
30	0.190	0.218	0.242
40	0.165	0.189	0.210
50	0.148	0.170	0.188
for $n > 50$	$\lesssim 1.07/\sqrt{n}$	$\lesssim 1.22/\sqrt{n}$	$\lesssim 1.36/\sqrt{n}$

The distribution function of D_n has been tabulated for small values of n [A8.2, A8.27], see Table A9.5 and Table A8.1. From the above it follows that:

For a given continuous distribution function $F(t)$, the band $F(t) \pm y_{1-\alpha}$ overlaps the empirical distribution function $\hat{F}_n(t)$ with probability $1 - \alpha_n$ where $\alpha_n \rightarrow \alpha$ as $n \rightarrow \infty$, with $y_{1-\alpha}$ defined by

$$\Pr\{D_n \leq y_{1-\alpha} \mid F(t)\} = 1 - \alpha \quad (\text{A8.15})$$

and given in Table A9.5 or Table A8.1.

From Table A8.1 one recognizes that the convergence $\alpha_n \rightarrow \alpha$ is good (for practical purposes) for $n > 50$. If $F(t)$ is not continuous, it can be shown that with $y_{1-\alpha}$ from Eq. (A8.15), the band $F(t) \pm y_{1-\alpha}$ overlaps $\hat{F}_n(t)$ with a probability $1 - \alpha'_n$, where $\alpha'_n \rightarrow \alpha' \leq \alpha$ as $n \rightarrow \infty$.

The role of $F(t)$ and $\hat{F}_n(t)$ can be *reversed* (see also pp. 459, 542, 543), yielding:

The random band $\hat{F}_n(t) \pm y_{1-\alpha}$ overlaps the true (unknown) distribution function $F(t)$ with probability $1 - \alpha_n$, where $\alpha_n \rightarrow \alpha$ as $n \rightarrow \infty$.

This last consideration is an aspect of *mathematical statistics*, while the former one (in relation to Eq. (A8.15)) was a problem of *probability theory*. One has thus the possibility to *estimate* an unknown continuous distribution function $F(t)$ on the basis of the empirical distribution function $\hat{F}_n(t)$, see e. g. Figs. 7.12 and 7.14.

Example A8.1

How large is the confidence band around $\hat{F}_n(t)$ for $n = 30$ and for $n = 100$ if $\alpha = 0.2$?

Solution

From Table A8.1, $y_{0.8} = 0.19$ for $n = 30$ and $y_{0.8} = 0.107$ for $n = 100$. This leads to the band $\hat{F}_n(t) \pm 0.19$ for $n = 30$ and $\hat{F}_n(t) \pm 0.107$ for $n = 100$.

To simplify investigations, it is often useful to draw $\hat{F}_n(t)$ on a *probability chart* (probability plot paper). The method is as follows:

The empirical distribution function $\hat{F}_n(t)$ is drawn in a system of coordinates in which a postulated type of continuous distribution function is represented by a straight line; if the underlying distribution $F(t)$ belongs to this type of distribution function, then for a sufficiently large value of n the points $(t_{(i)}, \hat{F}_n(t_{(i)}))$ will approximate to a straight line (a systematic deviation from a straight line, particularly in the domain $0.1 < \hat{F}_n(t) < 0.9$, leads to rejection of the type of distribution function assumed).

This can also be used as a simple rough visual check as to whether an assumed model ($F(t)$) seems correct. In many cases, estimates for unknown parameters of the underlying distribution function $F(t)$ can be obtained from the estimated straight line for $\hat{F}_n(t)$. Probability charts for the Weibull (including exponential), lognormal and normal distribution functions are given in Appendix A9.8, some applications are in Section 7.5.

The following is a derivation of the *Weibull probability chart*. The function

$$F(t) = 1 - e^{-(\lambda t)^\beta}$$

can be transformed to $\log_{10}(1/(1-F(t))) = (\lambda t)^\beta \log_{10}(e)$ and finally to

$$\log_{10} \log_{10} \left(\frac{1}{1-F(t)} \right) = \beta \log_{10}(t) + \beta \log_{10}(\lambda) + \log_{10} \log_{10}(e). \quad (\text{A8.16})$$

In the system of coordinates $\log_{10}(t)$ and $\log_{10} \log_{10}(1/(1-F(t)))$, the *Weibull distribution* function given by $F(t) = 1 - e^{-(\lambda t)^\beta}$ appears as a straight line. Fig. A8.2 shows this for $\beta = 1.5$ and $\lambda = 1/800\text{h}$. As illustrated by Fig. A8.2, the parameters β and λ can be obtained graphically

- β is the slope of the straight line, it appears on the scale $\log_{10} \log_{10}(1/(1-F(t)))$ if t is changed by one decade (e. g. from 10^2 to 10^3 h in Fig. A8.2),
- for $\log_{10} \log_{10}(1/(1-F(t))) = \log_{10} \log_{10}(e)$, i.e. on the dashed line in Fig. A8.2, one has $\log_{10}(\lambda t) = 0$ and thus $\lambda = 1/t$.

The Weibull probability chart also applies to the *exponential distribution* ($\beta = 1$).

For a *three parameter Weibull distribution* ($F(t) = 1 - e^{-(\lambda(t-\psi))^\beta}$, $t > \psi$) one can operate with the time axis $t' = t - \psi$, giving a straight line as before, or consider the concave curve obtained when using t (see Fig. A8.2 for an example). Conversely, from a concave curve describing a Weibull distribution (for instance, in the case of an *empirical data analysis*) it is possible to find ψ using the relationship $\psi = (t_1 t_2 - t_m^2) / (t_1 + t_2 - 2t_m)$ existing between two arbitrary points t_1, t_2 and t_m obtained from the mean of $F(t_1)$ and $F(t_2)$ on the scale $\log_{10} \log_{10}(1/(1-F(t)))$, see Example A6.14 for a derivation and Fig. A8.2 for an application with $t_1 = 400\text{h}$ and $t_2 = 1000\text{h}$, yielding $t_m = 600\text{h}$ and $\psi = 200\text{h}$.

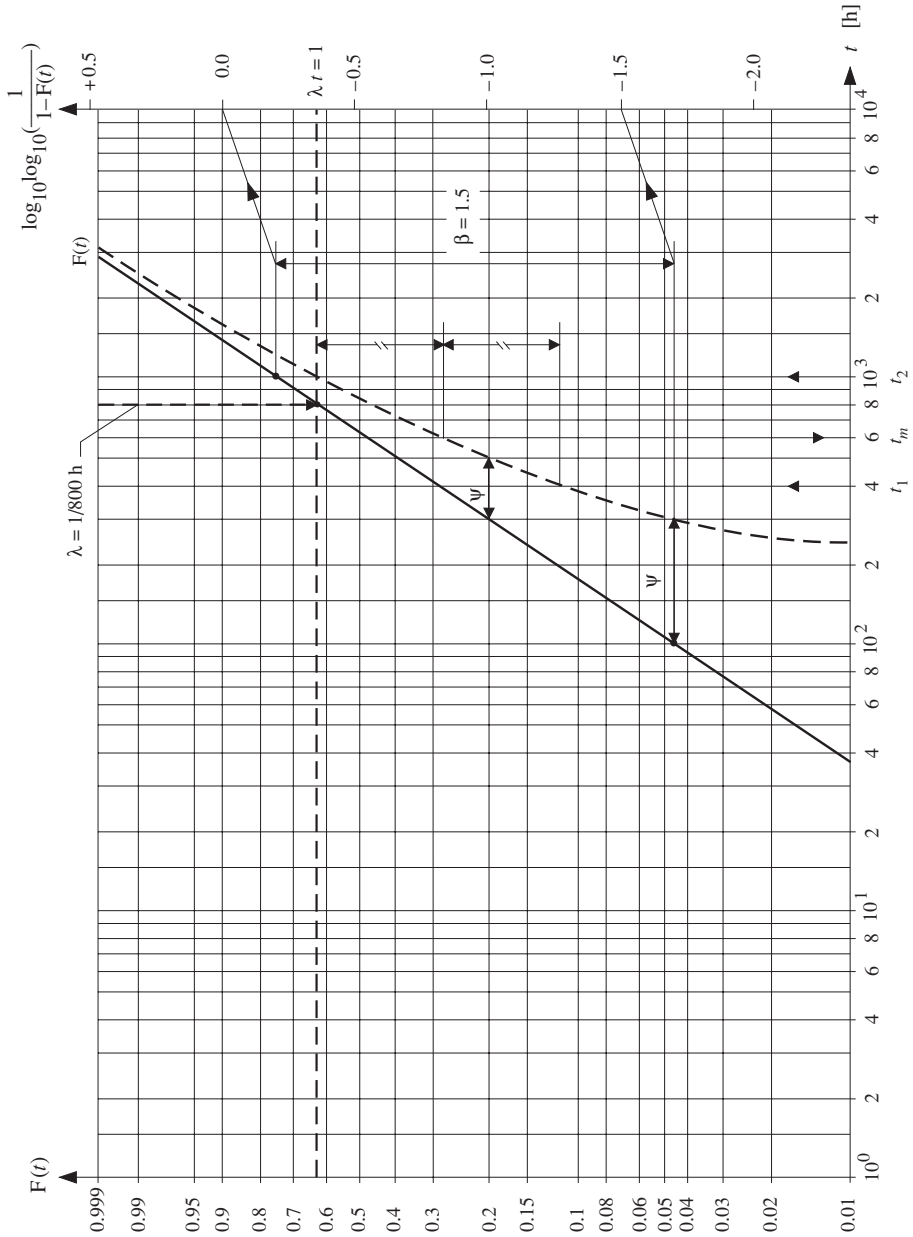


Figure A8.2 Weibull probability chart: The distribution function $F(t) = 1 - e^{-(\lambda t)^\beta}$ appears as a straight line (in the example $\lambda = 1/800$ h and $\beta = 1.5$); for a three parameter distribution $F(t) = 1 - e^{-(\lambda(t-\psi))^\beta}$, $t > \psi$, one can use $t' = t - \psi$ or operate with a concave curve and determine (as necessary) ψ , λ , and β graphically (dashed curve for $\lambda = 1/800$ h, $\beta = 1.5$, and $\psi = 200$ h as an example)

A8.2 Parameter Estimation

In many applications it can be assumed that the *type* of distribution function $F(t)$ of the underlying random variable τ is known. This means that $F(t) = F(t, \theta_1, \dots, \theta_r)$ is known in its functional form, the real-valued parameters $\theta_1, \dots, \theta_r$ having to be estimated. The unknown parameters of $F(t)$ must be estimated on the basis of the (totally) independent observations t_1, \dots, t_n of the random variable τ . A distinction is made between *point* and *interval estimation*.

A8.2.1 Point Estimation

Consider first the case where the given distribution function $F(t)$ only depends on a parameter θ , assumed hereafter as an *unknown constant*⁺⁾ . A *point estimate* for θ is a function

$$\hat{\theta}_n = u(t_1, \dots, t_n) \quad (\text{A8.17})$$

of the observations t_1, \dots, t_n of the random variable τ (not of the unknown parameter θ itself). The estimate $\hat{\theta}_n$ is

- *unbiased*, if

$$E[\hat{\theta}_n] = \theta, \quad (\text{A8.18})$$

- *consistent*, if $\hat{\theta}_n$ converges to θ in probability, i.e., if for any $\varepsilon > 0$

$$\lim_{n \rightarrow \infty} \Pr\{|\hat{\theta}_n - \theta| > \varepsilon\} = 0, \quad (\text{A8.19})$$

- *strongly consistent*, if $\hat{\theta}_n$ converges to θ with probability one

$$\Pr\{\lim_{n \rightarrow \infty} \hat{\theta}_n = \theta\} = 1, \quad (\text{A8.20})$$

- *efficient*, if

$$E[(\hat{\theta}_n - \theta)^2] \quad (\text{A8.21})$$

is minimum over all possible point estimates for θ ,

- *sufficient* (*sufficient statistic for* θ), if $\hat{\theta}_n$ delivers the complete information about θ (available in the observations t_1, \dots, t_n), i.e., if the conditional distribution of τ for given $\hat{\theta}_n$ does not depend on θ .

⁺⁾ Bayesian estimation theory (based on the Bayes theorem (Eq. (A6.18) & note to Eq. (A6.58)), which considers θ as a random variable and assigns to it an *a priori* distribution function, will not be considered in this book (as a function of the random sample, $\hat{\theta}_n$ is a random variable, while θ is an unknown constant). However, a Bayesian statistics can be useful if knowledge on the a priori distribution function is well founded, for these cases one may refer e. g. to [A8.24, A8.25].

For an unbiased estimate, Eq. (A8.21) becomes

$$E[(\hat{\theta}_n - \theta)^2] = E[(\hat{\theta}_n - E[\hat{\theta}_n])^2] = \text{Var}[\hat{\theta}_n]. \quad (\text{A8.22})$$

An unbiased estimate is thus efficient if $\text{Var}[\hat{\theta}_n]$ is minimum over all possible point estimates for θ , and consistent if $\text{Var}[\hat{\theta}_n] \rightarrow 0$ for $n \rightarrow \infty$. This last statement is a consequence of Chebyshev's inequality (Eq. (A6.49)). Efficiency can be checked using the Cramér - Rao inequality and sufficiency using the factorization criterion of the *likelihood function*, other useful properties of estimates are asymptotic unbiasedness and asymptotic efficiency, see e.g. [A8.1, A8.23].

Several methods are known for estimating θ . To these belong the methods of moments, quantiles, least squares, and maximum likelihood. The *maximum likelihood method* is commonly used in engineering applications. It provides point estimates which under general conditions are consistent, asymptotically unbiased, asymptotically efficient, and asymptotically normally distributed. Furthermore, if an efficient estimate exists, then the *likelihood equation* (Eqs.(A8.23) & A8.24)) has this estimate as a unique solution, and an estimate $\hat{\theta}_n$ is *sufficient* if and only if the *likelihood function* can be written in two factors, one depending on t_1, \dots, t_n only, the other on θ and $\hat{\theta}_n = u(t_1, \dots, t_n)$ (Examples A8.2 - A8.4), see e.g. [A8.1, A8.8, A8.15, A8.23].

The *maximum likelihood method* was developed 1921 by R.A. Fisher [A8.15] and is based on the following idea:

Maximize, with respect to the unknown parameter θ , the probability (Pr) that in a sample of size n , exactly the values t_1, \dots, t_n will be observed (i.e., maximize the probability of observing that record); this by maximizing the likelihood function ($L \sim \text{Pr}$), defined as

$$L(t_1, \dots, t_n, \theta) = \prod_{i=1}^n p_i(\theta), \quad \text{with } p_i(\theta) = \text{Pr}\{\tau = t_i\}, \quad (\text{A8.23})$$

in the discrete case, and as

$$L(t_1, \dots, t_n, \theta) = \prod_{i=1}^n f(t_i, \theta), \quad \text{with } f(t_i, \theta) \text{ as density function,} \quad (\text{A8.24})$$

in the continuous case.

Since the logarithmic function is monotonically increasing, the use of $\ln(L)$ instead of L leads to the same result. If $L(t_1, \dots, t_n, \theta)$ is derivable and the *maximum likelihood estimate* $\hat{\theta}_n$ exists, then it will satisfy the equation

$$\left. \frac{\partial L(t_1, \dots, t_n, \theta)}{\partial \theta} \right|_{\theta = \hat{\theta}_n} = 0, \quad (\text{A8.25})$$

or

$$\frac{\partial \ln(L(t_1, \dots, t_n, \theta))}{\partial \theta} \Bigg|_{\theta = \hat{\theta}_n} = 0. \tag{A8.26}$$

The maximum likelihood method can be generalized to the case of a distribution function with a finite number of unknown parameters $\theta_1, \dots, \theta_r$. Instead of Eq. (A8.26), the following system of r algebraic equations must be solved

$$\frac{\partial \ln(L(t_1, \dots, t_n, \theta_1, \dots, \theta_r))}{\partial \theta_i} \Bigg|_{\theta_i = \hat{\theta}_{in}} = 0, \quad i = 1, \dots, r. \tag{A8.27}$$

The existence and uniqueness of a maximum likelihood estimate is satisfied in most practical applications (Eq. (A8.26) or (A8.27) is necessary and sufficient for the existence of a maximum).

To simplify the notation, in the following the index n will be *omitted* for the estimated parameters.

Example A8.2

Let t_1, \dots, t_n be independent observations of an exponentially distributed failure-free time τ . Give the maximum likelihood estimate for the unknown parameter λ of the *exponential distribution*.

Solution

With $f(t, \lambda) = \lambda e^{-\lambda t}$, Eq. (A8.24) yields $L(t_1, \dots, t_n, \lambda) = \lambda^n e^{-\lambda(t_1 + \dots + t_n)}$, from which

$$\hat{\lambda} = \frac{n}{t_1 + \dots + t_n}. \tag{A8.28}$$

This case corresponds to a sampling plan with n elements without replacement, terminated at the occurrence of the n th failure. λ depends only on the sum $t_1 + \dots + t_n$, not on the individual values of t_i ; $t_1 + \dots + t_n$ is a *sufficient statistic* and $\hat{\lambda}$ is a *sufficient estimate* ($L = 1 \cdot \lambda^n e^{-n\lambda/\hat{\lambda}}$). However, $\hat{\lambda} = n / (t_1 + \dots + t_n)$ is a biased estimate, unbiased is $\hat{\lambda} = (n - 1) / (t_1 + \dots + t_n)$, as well as $\hat{E}[\tau] = (t_1 + \dots + t_n) / n$ given by Eq. (A8.6).

Example A8.3

Assuming that an event A has occurred exactly k times in n Bernoulli trials, give the maximum likelihood estimate for the *unknown probability* p for event A to occur.

Solution

Using the binomial distribution (Eq. (A6.120)), the likelihood function (Eq. (A8.23)) becomes

$$L = p_k = \binom{n}{k} p^k (1 - p)^{n-k} \quad \text{or} \quad \ln L = \ln \binom{n}{k} + k \ln p + (n - k) \ln(1 - p).$$

This leads to

$$\hat{p} = k / n. \tag{A8.29}$$

\hat{p} is the observed *relative frequency*, it is unbiased and depends only on k , i. e. on the number of the event occurrences in n independent trials; k is a *sufficient statistic* and \hat{p} is a *sufficient estimate* ($L = \binom{n}{k} \cdot [p^{\hat{p}}(1-p)^{(1-\hat{p})}]^n$).

Example A8.4

Let k_1, \dots, k_n be independent observations of a random variable ζ distributed according to the Poisson distribution defined by Eq. (A6.125). Give the maximum likelihood estimate for the unknown parameter m of the *Poisson distribution*.

Solution

Using Eq. (A6.120), the likelihood function becomes

$$L = \frac{m^{k_1 + \dots + k_n}}{k_1! \dots k_n!} e^{-nm} \quad \text{or} \quad \ln L = (k_1 + \dots + k_n) \ln m - nm - \ln(k_1! \dots k_n!),$$

and thus

$$\hat{m} = \frac{k_1 + \dots + k_n}{n}. \tag{A8.30}$$

\hat{m} is unbiased. It depends only on the sum $k_1 + \dots + k_n$, not on the individual k_i ; $k_1 + \dots + k_n$ is a *sufficient statistic* and \hat{m} is a *sufficient estimate* ($L = (1/k_1! \dots k_n!) \cdot (m^n e^{-nm})$).

Example A8.5

Let t_1, \dots, t_n be independent observations of a Weibull distributed failure-free time τ . Give the max. likelihood estimate for the unknown parameters λ and β .

Solution

With $f(t, \lambda, \beta) = \beta \lambda (\lambda t) \beta - 1 e^{-(\lambda t)^\beta}$ (Eq. (A6.90)), it follows from Eq. (A8.24) that

$$L(t_1, \dots, t_n, \lambda, \beta) = (\beta \lambda^\beta)^n e^{-\lambda^\beta (t_1^\beta + \dots + t_n^\beta)} \prod_{i=1}^n t_i^{\beta-1},$$

yielding (Eq. (A8.27) and considering $a^x = e^{x \ln a}$)

$$\hat{\beta} = \left[\frac{\sum_{i=1}^n t_i^{\hat{\beta}} \ln t_i}{\sum_{i=1}^n t_i^{\hat{\beta}}} - \frac{1}{n} \sum_{i=1}^n \ln t_i \right]^{-1} \quad \text{and} \quad \hat{\lambda} = \left[\frac{n}{\sum_{i=1}^n t_i^{\hat{\beta}}} \right]^{1/\hat{\beta}}. \tag{A8.31}$$

The solution for $\hat{\beta}$ is unique and can be found, using Newton's approximation method (the value obtained from the empirical distribution function can give a good initial value, see Fig. 7.12).

Due to cost and time limitations, the situation often arises in reliability applications in which the items under test are run in parallel and the test is stopped before all items have failed. If there are n items, and at the end of the test k have failed (at the individual failure times (times to failure) $t_1 < t_2 < \dots < t_k$) and $n - k$ are still working, then the operating times T_1, \dots, T_{n-k} of the items still working at the end of the test should also be accounted for in the evaluation. Considering a *Weibull distribution* as in Example A8.5, and assuming that the operating times T_1, \dots, T_{n-k} have been observed in addition to the failure-free times t_1, \dots, t_k , then

$$L(t_1, \dots, t_k, \lambda, \beta) \sim (\beta \lambda^\beta)^k e^{-\lambda^\beta (t_1^\beta + \dots + t_k^\beta)} \prod_{i=1}^k t_i^{\beta-1} \prod_{j=1}^{n-k} e^{-(\lambda T_j)^\beta},$$

leads to (Eq. (A8.27) and considering $a^x = e^{x \ln a}$)

$$\hat{\beta} = \left[\frac{\sum_{i=1}^k t_i^{\hat{\beta}} \ln t_i + \sum_{j=1}^{n-k} T_j^{\hat{\beta}} \ln T_j}{\sum_{i=1}^k t_i^{\hat{\beta}} + \sum_{j=1}^{n-k} T_j^{\hat{\beta}}} - \frac{1}{k} \sum_{i=1}^k \ln t_i \right]^{-1}, \quad \hat{\lambda} = \left[\frac{k}{\sum_{i=1}^k t_i^{\hat{\beta}} + \sum_{j=1}^{n-k} T_j^{\hat{\beta}}} \right]^{1/\hat{\beta}}. \quad (A8.32)$$

The calculation method for Eq.(A8.32) applies for any distribution function, yielding

$$L = \prod_i f(t_i, \theta) \cdot \prod_j (1 - F(T_j, \theta)), \quad (A8.33)$$

where i sums over all observed times to failure, j sums over all failure-free times, and θ can be a vector. However, following two cases must be distinguished:

- (i) $T_1 = \dots = T_{n-k} = t_k$, i. e., the test is stopped at the (random) occurrence of the k th failure (*Type II censoring*),
- (ii) $T_1 = \dots = T_{n-k} = T_{test}$ is the given (fixed) test duration (*Type I censoring*).

The two situations are *basically different* and this has to be considered in data analysis, see e. g. the discussion below with Eqs. (A8.34) and (A8.35).

For the *exponential distribution* ($\beta = 1$), Eq. (A8.31) reduces to Eq. (A8.28) and Eq. (A8.32) to

$$\hat{\lambda} = \frac{k}{\sum_{i=1}^k t_i + \sum_{j=1}^{n-k} T_j}. \quad (A8.34)$$

If the test is stopped at the occurrence of the k th failure, as per (i) above, $T_1 = \dots = T_{n-k} = t_k$ holds in general, and the quantity $T_r = t_1 + \dots + t_k + (n-k)t_k$ is the *random cumulative operating time* over all items during the test. This situation corresponds to a sampling plan with n elements *without replacement* (renewal), censored at the occurrence of the k th failure. Because of the *memoryless property* of the Poisson process (Eqs. (7.26) and (7.27)), T_r can be calculated as $T_r = n t_1 + (n-1)(t_2 - t_1) + \dots + (n-k+1)(t_k - t_{k-1}) = t_1 + \dots + t_k + (n-k)t_k$ (Eq. (7.23)). It can be shown that $\hat{\lambda} = k / T_r$ is biased, unbiased is

$$\hat{\lambda} = \frac{k-1}{t_1 + \dots + t_k + (n-k)t_k}. \quad (A8.35)$$

If the test is stopped at the fixed time T_{test} , $T_r = t_1 + \dots + t_k + (n-k)T_{test}$, as per (i) above, (Eq.(7.25)). In this case, T_{test} is given (fixed) but k as well as t_1, \dots, t_k are *random*. This situation corresponds to a sampling plan with n elements *without replacement*, censored at a fixed test time T_{test} . Also for this case, k / T_r is biased. However,

important for practical applications, also because results are not biased (for $k > 1$), is the case with replacement (Appendix A8.2.2.2, Section 7.2.3).

A8.2.2 Interval Estimation

As shown in Appendix A8.2.1, a point estimation has the advantage of providing an estimate quickly. However, it does not give any indication as to the deviation of the estimate from the true parameter. More information can be obtained from an interval estimation. With an *interval estimation*, a *random interval* $[\hat{\theta}_l, \hat{\theta}_u]$ is sought such that it *overlaps* (covers) the true value of the unknown parameter θ with a given probability γ . $[\hat{\theta}_l, \hat{\theta}_u]$ is the *confidence interval*, $\hat{\theta}_l$ and $\hat{\theta}_u$ are the *lower* and *upper confidence limits*, and γ is the *confidence level*. γ has the following interpretation:

In an increasing number of (totally) independent samples of size n (used to obtain confidence intervals), the relative frequency of the cases in which the confidence intervals $[\hat{\theta}_l, \hat{\theta}_u]$ overlap (cover) the unknown parameter θ converges to the confidence level $\gamma = 1 - \beta_1 - \beta_2$ ($0 < \beta_1 < 1 - \beta_2 < 1$).

β_1 and β_2 are the error probabilities related to the interval estimation. If γ can not be reached exactly, the true overlap probability should be near to, but not less than, γ .

The confidence interval can also be *one-sided*, i. e. $[0, \hat{\theta}_u]$ or $[\hat{\theta}_l, \infty)$ for $\theta \geq 0$. Figure A8.3 shows some examples of confidence intervals.

The concept of confidence intervals was introduced independently by J. Neyman and R. A. Fisher around 1930. In the following, some important cases for quality control and reliability tests are considered.

A8.2.2.1 Estimation of an Unknown Probability p

Consider a sequence of *Bernoulli trials* (Appendix A6.10.7) where a given event A can occur with constant probability p at each trial. The *binomial distribution*

$$p_k = \binom{n}{k} p^k (1 - p)^{n-k}$$

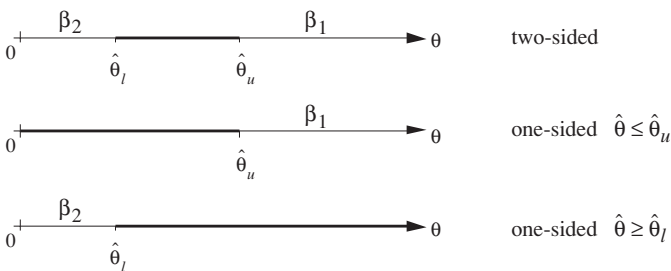


Figure A8.3 Examples of *confidence intervals* for $\theta \geq 0$

gives the probability that the event A will occur exactly k times in n independent trials. From the expression for p_k , it follows that

$$\Pr\{k_1 \leq \text{observations of } A \text{ in } n \text{ trials} \leq k_2 \mid p\} = \sum_{i=k_1}^{k_2} \binom{n}{i} p^i (1-p)^{n-i}. \quad (\text{A8.36})$$

However, in mathematical statistics, the parameter p is unknown. A *confidence interval* for p is sought, based on the observed number of occurrences of the event A in n Bernoulli trials. A solution to this problem has been presented 1934 by Clopper and Pearson [A8.6]. For given $\gamma = 1 - \beta_1 - \beta_2$ ($0 < \beta_1 < 1 - \beta_2 < 1$) the following holds:

If in n Bernoulli trials the event A has occurred k times, there is a probability nearly equal to (but not smaller than) $\gamma = 1 - \beta_1 - \beta_2$ that the confidence interval $[\hat{p}_l, \hat{p}_u]$ overlaps the true (unknown) probability p , with \hat{p}_l & \hat{p}_u given by

$$\sum_{i=k}^n \binom{n}{i} \hat{p}_l^i (1 - \hat{p}_l)^{n-i} = \beta_2, \quad \text{for } 0 < k < n, \quad (\text{A8.37})$$

and

$$\sum_{i=0}^k \binom{n}{i} \hat{p}_u^i (1 - \hat{p}_u)^{n-i} = \beta_1, \quad \text{for } 0 < k < n; \quad (\text{A8.38})$$

for $k = 0$ take

$$\hat{p}_l = 0 \quad \text{and} \quad \hat{p}_u = 1 - \sqrt[n]{\beta_2}, \quad \text{with} \quad \gamma = 1 - \beta_1, \quad (\text{A8.39})$$

and for $k = n$ take

$$\hat{p}_l = \sqrt[n]{\beta_2} \quad \text{and} \quad \hat{p}_u = 1, \quad \text{with} \quad \gamma = 1 - \beta_2. \quad (\text{A8.40})$$

Considering that k is a random variable, \hat{p}_l and \hat{p}_u are *random variables*. According to the footnote on p. 526, it would be more correct (from a mathematical point of view) to compute from Eqs. (A8.37) and (A8.38) the quantities p_{kl} and p_{ku} , and then to set $\hat{p}_l = p_{kl}$ and $\hat{p}_u = p_{ku}$. For simplicity, this has been omitted here. Assuming p as a random variable, β_1 and β_2 would be the probabilities for p to be greater than \hat{p}_u and smaller than \hat{p}_l , respectively (Fig. A8.3).

The proof of Eqs. (A8.38) is based on the monotonic property of the function

$$B_n(k, p) = \sum_{i=0}^k \binom{n}{i} p^i (1-p)^{n-i}.$$

For given (fixed) n , $B_n(k, p)$ decreases in p for fixed k and increases in k for fixed p (Fig. A8.4). Thus, for any $p > \hat{p}_u$ it follows that

$$B_n(k, p) < B_n(k, \hat{p}_u) = \beta_1.$$

For $p > \hat{p}_u$, the probability that the (random) number of observations in n trials will

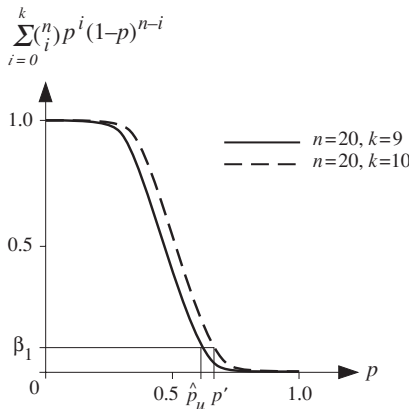


Figure A8.4 Binomial distribution as a function of p for n fixed and two values of k

take one of the values $0, 1, \dots, k$ is thus $< \beta_1$ (for $p > p'$ in Fig. A8.4, the statement would also be true for a $K > k$). This holds in particular for a number of observations equal to k and proves Eq. (A8.38). Proof of Eq. (A8.37) is similar.

To determine \hat{p}_l & \hat{p}_u per Eqs. (A8.37) & (A8.38), a Table of the *Fisher distribution* (yielding e.g. $\hat{p}_u = (k + 1) F_{2(k+1), 2(n-k), 1-\beta_1} / [n - k + (k + 1) F_{2(k+1), 2(n-k), 1-\beta_1}]$, Appendix A9.4) or of the *Beta function* can be used. However, for n sufficiently large and $\beta_1 = \beta_2 = (1 - \gamma) / 2$, one of the following *approximate solutions* can be used in practical applications:

1. For large values on n ($\min(np, n(1-p)) \geq 5$), a good estimate for \hat{p}_l and \hat{p}_u can be found using the *integral Laplace theorem*. Taking $\varepsilon = b \sqrt{np(1-p)} / n$ and considering $\sum_{i=1}^k \delta_i = k$ (or rearranging Eq. (A6.149)), Eq. (A6.150) yields

$$\lim_{n \rightarrow \infty} \Pr \left\{ \left(\frac{k}{n} - p \right)^2 \leq \frac{b^2 p(1-p)}{n} \right\} = \frac{2}{\sqrt{2\pi}} \int_0^b e^{-x^2/2} dx. \tag{A8.41}$$

The right-hand side of Eq. (A8.41) is equal to the confidence level γ , i.e.

$$\frac{2}{\sqrt{2\pi}} \int_0^b e^{-x^2/2} dx = \gamma.$$

Thus, for a given γ , the value of b can be obtained from a table of the normal distribution (Table A9.1). b is the $1/2 + \gamma/2 = (1 + \gamma)/2$ quantile of the standard normal distribution $\Phi(t)$, i.e., $b = t_{(1+\gamma)/2}$ giving e.g. $b = 1.64$ for $\gamma = 0.9$. On the left-hand side of Eq. (A8.41), the expression

$$\left(\frac{k}{n} - p \right)^2 = \frac{b^2 p(1-p)}{n} \tag{A8.42}$$

is the equation of the *confidence ellipse*. For given values of k , n , and b , confidence limits \hat{p}_l and \hat{p}_u can be determined as roots of Eq. (A8.42)

$$\hat{p}_{l,u} = \frac{k + 0.5b^2 \pm b\sqrt{k(1-k/n) + b^2/4}}{n + b^2}, \quad \beta_1 = \beta_2 = (1 - \gamma)/2, \quad (A8.43)$$

see Figs. A8.5 and 7.1 for some Examples.

- For small values of n , confidence limits can be determined graphically from the envelopes of Eqs. (A8.37) and (A8.38) for $\beta_1 = \beta_2 = (1 - \gamma)/2$, see Fig. 7.1 for $\gamma = 0.8$ and $\gamma = 0.9$. For $n > 50$, the curves of Fig. 7.1 practically agree with the confidence ellipses given by Eq. (A8.43).

One-sided confidence intervals can also be obtained from the above values for \hat{p}_l and \hat{p}_u . Figure A8.3 shows that

$$0 \leq p \leq \hat{p}_u, \quad \text{with } \gamma = 1 - \beta_1 \quad \text{and} \quad \hat{p}_l \leq p \leq 1, \quad \text{with } \gamma = 1 - \beta_2. \quad (A8.44)$$

Example A8.6

Using confidence ellipses, give the confidence interval $[\hat{p}_l, \hat{p}_u]$ for an unknown probability p for the case $n = 50$, $k = 5$, and $\gamma = 0.9$.

Solution

Setting $n = 50$, $k = 5$, and $b = 1.64$ in Eq. (A8.43) yields the confidence interval $[0.05, 0.19]$, see also Fig. 8.5 or Fig. 7.1 for a graphical solution.

Supplementary results: Corresponding one-sided confidence intervals would be $p \leq 0.19$ or $p \geq 0.05$ with $\gamma = 0.95$.

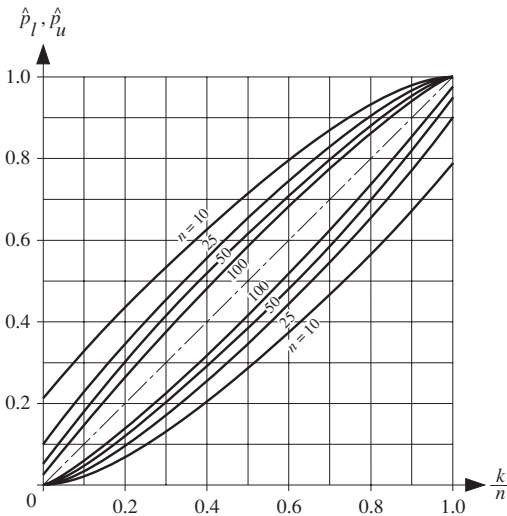


Figure A8.5 Confidence limits (ellipses) for an unknown probability p with a confidence level $\gamma = 1 - \beta_1 - \beta_2 = 0.9$, here with $\beta_1 = \beta_2$, and for $n = 10, 25, 50, 100$ (according to Eq. (A8.43))

The role of k/n and p can be *reversed*, and Eq. (A8.42) can be used (as consequence of Eq. (A8.41)) to solve a problem of *probability theory*, i. e., to compute for a *given* probability $\gamma = 1 - \beta_1 - \beta_2$ with $\beta_1 = \beta_2$, the limits k_1 and k_2 of the number of observations k in n *independent trials* for *given* (fixed) values of p and n (e. g. the number k of defective items in a sample of size n); see also the remarks on pp. 459, 530, 543)

$$k_{1,2} = np \pm b \sqrt{np(1-p)}. \quad (\text{A8.45})$$

As in Eq. (A8.43), the quantity b in Eq. (A8.45) is the $(1 + \gamma)/2$ quantile of the normal distribution (e. g. $b = 1.64$ for $\gamma = 0.9$ from Table A9.1). For a graphical solution, Fig. A8.5 can be used, taking the ordinate p as known and by reading k_1/n and k_2/n from the abscissa. An exact solution follows from Eq. (A8.36).

A8.2.2.2 Estimation of the Parameter λ for an Exponential Distribution: Fixed Test Duration (Time Censoring), Instantaneous Replacement

Consider an item having a *constant failure rate* λ and assume that at each failure it will be *immediately replaced* by a new, statistically equivalent item, in a negligible replacement time (Appendix A7.2). Because of the *memoryless property* (constant failure rate), the number of failures in $(0, T]$ is Poisson distributed and given by $\Pr\{k \text{ failures in } (0, T] \mid \lambda\} = (\lambda T)^k e^{-\lambda T} / k!$ (Eq. (A7.41)). The maximum likelihood point estimate for λ follows from Eq. (A8.30), with $n = 1$ and $m = \lambda T$, as

$$\hat{\lambda} = \frac{k}{T}. \quad (\text{A8.46})$$

Similarly, estimation of the confidence interval for the failure rate λ can be reduced to the *estimation of the confidence interval for the parameter $m = \lambda T$ of a Poisson distribution*. Considering Eqs. (A8.37) and (A8.38) and the similarity between the binomial and the Poisson distribution, the confidence limits $\hat{\lambda}_l$ and $\hat{\lambda}_u$ can be determined for given $\beta_1, \beta_2, \gamma = 1 - \beta_1 - \beta_2$ ($0 < \beta_1 < 1 - \beta_2 < 1$) from

$$\sum_{i=k}^{\infty} \frac{(\hat{\lambda}_l T)^i}{i!} e^{-\hat{\lambda}_l T} = \beta_2, \quad \text{for } k > 0, \quad (\text{A8.47})$$

and

$$\sum_{i=0}^k \frac{(\hat{\lambda}_u T)^i}{i!} e^{-\hat{\lambda}_u T} = \beta_1, \quad \text{for } k > 0; \quad (\text{A8.48})$$

for $k = 0$ takes

$$\hat{\lambda}_l = 0 \quad \text{and} \quad \hat{\lambda}_u = \frac{\ln(1/\beta_1)}{T}, \quad \text{with } \gamma = 1 - \beta_1. \quad (\text{A8.49})$$

On the basis of the known relationship to the chi-square (χ^2) distribution (Eqs. (A6.102), (A6.103), Appendix A9.2), the values $\hat{\lambda}_l$ and $\hat{\lambda}_u$ from Eqs. (A8.47) and (A8.48) follow from the quantiles of the chi-square distribution, as

$$\hat{\lambda}_l = \frac{\chi_{2k, \beta_2}^2}{2T}, \quad \text{for } k > 0, \tag{A8.50}$$

and

$$\hat{\lambda}_u = \frac{\chi_{2(k+1), 1-\beta_1}^2}{2T}, \quad \text{for } k \geq 0. \tag{A8.51}$$

$\beta_1 = \beta_2 = (1 - \gamma)/2$ is frequently used in practical applications. Fig. 7.6 gives the results obtained from Eqs. (A8.50) and (A8.51) for $\beta_1 = \beta_2 = (1 - \gamma)/2$.

One-sided confidence intervals are given as in the previous section by

$$0 \leq \lambda \leq \hat{\lambda}_u, \quad \text{with } \gamma = 1 - \beta_1 \quad \text{and} \quad \lambda \geq \hat{\lambda}_l, \quad \text{with } \gamma = 1 - \beta_2. \tag{A8.52}$$

The situation considered by Eqs. (A8.47) to (A8.51) corresponds also to that of a sampling plan with n elements *with replacement*, each of them with failure rate $\lambda' = \lambda/n$, terminated at a fixed test time $T_{test} = T$. This situation is basically different from that presented by Eq. (A8.34) and in Section A8.2.2.3.

A8.2.2.3 Estimation of the Parameter λ for an Exponential Distribution: Fixed Number n of Failures (Failure Censoring), no Replacement

Let τ_1, \dots, τ_n be independent random variables distributed according to a common distribution function $F(t) = \text{Pr}\{\tau_i \leq t\} = 1 - e^{-\lambda t}$, $i = 1, \dots, n$. From Eq. (A6.102),

$$\text{Pr}\{\tau_1 + \dots + \tau_n \leq t\} = 1 - \sum_{i=0}^{n-1} \frac{(\lambda t)^i}{i!} e^{-\lambda t} = \frac{1}{(n-1)!} \int_0^{\lambda t} x^{n-1} e^{-x} dx \tag{A8.53}$$

and thus

$$\text{Pr}\{a < \tau_1 + \dots + \tau_n \leq b\} = \frac{1}{(n-1)!} \int_{a\lambda}^{b\lambda} x^{n-1} e^{-x} dx.$$

Setting $a = n(1 - \varepsilon_2)/\lambda$ and $b = n(1 + \varepsilon_1)/\lambda$ it follows that

$$\text{Pr}\left\{\frac{1 - \varepsilon_2}{\lambda} < \frac{\tau_1 + \dots + \tau_n}{n} \leq \frac{1 + \varepsilon_1}{\lambda}\right\} = \frac{1}{(n-1)!} \int_{n(1-\varepsilon_2)}^{n(1+\varepsilon_1)} x^{n-1} e^{-x} dx. \tag{A8.54}$$

Reversing the role of λ & $\hat{\lambda} = n/(t_1, \dots, t_n)$, i.e. considering $\hat{\lambda}$ given and λ as random variable, Eq. (A8.54) can be used to compute the confidence limits $\hat{\lambda}_l$ and $\hat{\lambda}_u$ (see also pp. 459, 530, 542). For $\beta_1, \beta_2, \gamma = 1 - \beta_1 - \beta_2$ ($0 < \beta_1 < 1 - \beta_2 < 1$), this leads to

$$\text{Pr}\{(1 - \varepsilon_2)\hat{\lambda} < \lambda \leq (1 + \varepsilon_1)\hat{\lambda}\} = \frac{1}{(n-1)!} \int_{n(1-\varepsilon_2)}^{n(1+\varepsilon_1)} x^{n-1} e^{-x} dx \tag{A8.55}$$

i. e.

$$\hat{\lambda}_l = (1 - \varepsilon_2)\hat{\lambda} \quad \& \quad \hat{\lambda}_u = (1 + \varepsilon_1)\hat{\lambda}, \quad \text{with } \hat{\lambda} = n / (t_1, \dots, t_n), \quad (\text{A8.56})$$

and $\varepsilon_1, \varepsilon_2$ given by (see also Fig. A8.3 with $\theta = \lambda$)

$$\frac{1}{(n-1)!} \int_{n(1+\varepsilon_1)}^{\infty} x^{n-1} e^{-x} dx = \beta_1 \quad \text{and} \quad \frac{1}{(n-1)!} \int_0^{n(1-\varepsilon_2)} x^{n-1} e^{-x} dx = \beta_2. \quad (\text{A8.57})$$

Using the definition of the chi-square distribution (Appendix A9.2), it follows that $1 + \varepsilon_1 = (\chi_{2n, 1-\beta_1}^2) / 2n$ and $1 - \varepsilon_2 = (\chi_{2n, \beta_2}^2) / 2n$ and thus

$$\hat{\lambda}_l = \frac{\chi_{2n, \beta_2}^2}{2(t_1 + \dots + t_n)} \quad \text{and} \quad \hat{\lambda}_u = \frac{\chi_{2n, 1-\beta_1}^2}{2(t_1 + \dots + t_n)}. \quad (\text{A8.58})$$

$\varepsilon_2 = 1$ or $\varepsilon_1 = \infty$ lead to *one-sided confidence intervals* $[0, \hat{\lambda}_u]$ or $[\hat{\lambda}_l, \infty)$. Figure A8.6 gives the graphical relationship between n, γ , and $\varepsilon_1 = \varepsilon_2 = \varepsilon$ (Example A8.7).

The case considered by Eqs. (A8.53) to (A8.58) corresponds to the situation described in Example A8.2 (sampling plan with n elements *without replacement*, terminated at the n th failure), and differs statistically from that in Section A8.2.2.2.

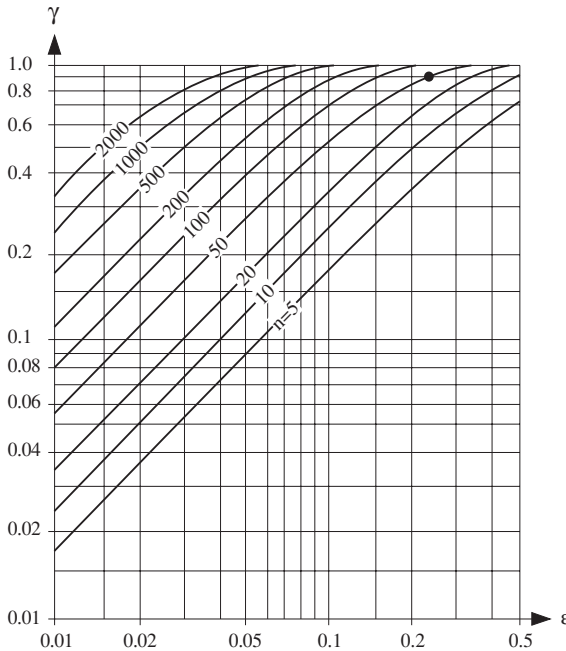


Figure A8.6 Probability γ that the interval $(1 \pm \varepsilon)\hat{\lambda}$ overlaps the true value of λ for the case of a fixed number n of failures ($\hat{\lambda} = n / (t_1 + \dots + t_n)$, $\text{Pr}\{\tau \leq t\} = 1 - e^{-\lambda t}$, • for Example A8.7)

Example A8.7

For the case considered by Eqs. (A8.53) to (A8.58), give for $n = 50$ and $\gamma = 0.9$ the two-sided confidence interval for the parameter λ of an exponential distribution as a function of $\hat{\lambda}$.

Solution

From Figure A8.6, $\varepsilon = 0.24$ yielding the confidence interval $[0.76\hat{\lambda}, 1.24\hat{\lambda}]$.

A8.2.2.4 Availability Estimation (Erlangian Failure-Free and/or Repair Times)

Considerations of Section A8.2.2.3 can be extended to estimate the availability of a repairable item (described by the alternating renewal process of Fig. 6.2) for the case of Erlangian distributed failure-free and/or repair times (Appendix A6.10.3), and in particular for the case of constant failure and repair rates (Appendix A6.10.1).

Consider a repairable item in continuous operation, new at $t=0$ (Fig. 6.2), and assume constant failure and repair rates $\lambda(x)=\lambda, \mu(x)=\mu$ (x starting by 0 at the beginning of each operating or repair time, respectively). For this case, point and average *unavailability* converge (Tables 6.3 & 6.4) to the asymptotic & steady-state value $1 - PA_S = 1 - AA_S = \lambda / (\lambda + \mu)$, given here as $\overline{PA} = \overline{AA}$ to simplify notation

$$\overline{PA} = 1 - PA = 1 - AA = \overline{AA} = \lambda / (\lambda + \mu).$$

$\lambda / (\lambda + \mu)$ is a probabilistic value and has his statistical counterpart in $DT / (UT + DT)$, where DT is the *down* (repair) time and $UT = t - DT$ the *up* (operating) time observed in $(0, t]$. To simplify considerations, it will be assumed in the following $t \gg MTTR = 1/\mu$ and that at the time point t a repair is terminated and k failure-free and repair times have occurred ($k=1, 2, \dots$). Furthermore,

$$\overline{PA}_a = \lambda / \mu \quad \text{instead of} \quad \overline{PA} = \overline{PA}_a / (1 + \lambda / \mu) \approx \overline{PA}_a (1 - \lambda / \mu) \tag{A8.59}$$

will be used here, yielding the counterpart DT / UT ($\overline{PA}_a - (\lambda / \mu)^2 < \overline{PA} < \overline{PA}_a$).^{+) Considering that at the time point t a repair is terminated, it holds that}

$$UT / DT = (t_1 + \dots + t_k) / (t'_1 + \dots + t'_k),$$

where t_i & t'_i are the observed values of failure-free and repair times τ_i & τ'_i , respectively. According to Eqs. (A6.102) - (A6.104), the quantity $2\lambda(\tau_1 + \dots + \tau_k)$ has a χ^2 -distribution with $\nu = 2k$ degrees of freedom; same for the repair times $2\mu(\tau'_1 + \dots + \tau'_k)$. From this, it follows (Appendix A9.4, footnote on p. 526) that

$$\overline{PA}_a \cdot \frac{UT}{DT} = \frac{\lambda}{\mu} \cdot \frac{\tau_1 + \dots + \tau_k}{\tau'_1 + \dots + \tau'_k} = \frac{2\lambda(\tau_1 + \dots + \tau_k) / 2k}{2\mu(\tau'_1 + \dots + \tau'_k) / 2k} \tag{A8.60}$$

is distributed according to a Fisher (**F**-) distribution with $\nu_1 = \nu_2 = 2k$ degrees of freedom (UT/DT is a random variable, $\overline{PA}_a = \lambda/\mu$ is regarded as an unknown parameter)

$$\Pr\left\{ \overline{PA}_a \frac{UT}{DT} \leq x \right\} = \frac{(2k-1)!}{[(k-1)!]^2} \int_0^x \frac{y^{k-1}}{(1+y)^{2k}} dy. \tag{A8.61}$$

Having observed for a repairable item described by Fig. 6.2 with constant failure rate λ and repair rate $\mu \gg \lambda$, an operating time $UT = t_1 + \dots + t_k$ and a repair time $DT = t'_1 + \dots + t'_k$, the maximum likelihood estimate for $\overline{PA}_a = \lambda / \mu$ is

$$\widehat{PA}_a = (\widehat{\lambda} / \widehat{\mu}) = DT / UT = (t'_1 + \dots + t'_k) / (t_1 + \dots + t_k) \tag{A8.62}$$

(Eq. (A8.25) with $L(UT/DT, \overline{PA}_a) \sim [(UT/DT)^{k-1} \overline{PA}_a^k] / (1 + (UT/DT) \overline{PA}_a)^{2k}$ per Eq. (A8.61)); DT / UT is biased, unbiased is $(1 - 1/k) DT / UT$, $k > 1$ (Example A8.10).

With the same considerations as for Eq. (A8.54), Eq. (A8.61) yields ($k=1, 2, \dots$)

$$\Pr\left\{ \frac{DT}{UT} (1 - \varepsilon_2) < \overline{PA}_a \leq \frac{DT}{UT} (1 + \varepsilon_1) \right\} = \frac{(2k - 1)!}{(k - 1)!^2} \int_{1 - \varepsilon_2}^{1 + \varepsilon_1} \frac{x^{k - 1}}{(1 + x)^{2k}} dx, \tag{A8.63}$$

and thus to the confidence limits $\widehat{PA}_{a_l} = (1 - \varepsilon_2) \widehat{PA}_a$ and $\widehat{PA}_{a_u} = (1 + \varepsilon_1) \widehat{PA}_a$, with \widehat{PA}_a as in Eq. (A8.62) and $\varepsilon_1, \varepsilon_2$ related to the confidence level $\gamma = 1 - \beta_1 - \beta_2$ by

$$\frac{(2k - 1)!}{[(k - 1)!]^2} \int_{1 + \varepsilon_1}^{\infty} \frac{x^{k - 1}}{(1 + x)^{2k}} dx = \beta_1 \quad \text{and} \quad \frac{(2k - 1)!}{[(k - 1)!]^2} \int_0^{1 - \varepsilon_2} \frac{x^{k - 1}}{(1 + x)^{2k}} dx = \beta_2. \tag{A8.64}$$

From the definition of the Fisher (F -) distribution (Appendix A9.4), it follows that $\varepsilon_1 = F_{2k, 2k, 1 - \beta_1} - 1$ and $\varepsilon_2 = 1 - F_{2k, 2k, \beta_2}$; and thus, using $F_{\nu_1, \nu_2, \beta_2} = 1 / F_{\nu_2, \nu_1, 1 - \beta_2}$,

$$\widehat{PA}_{a_l} = \widehat{PA}_a / F_{2k, 2k, 1 - \beta_2} \quad \text{and} \quad \widehat{PA}_{a_u} = \widehat{PA}_a \cdot F_{2k, 2k, 1 - \beta_1}, \tag{A8.65}$$

where $F_{2k, 2k, 1 - \beta_2}$ and $F_{2k, 2k, 1 - \beta_1}$ are the $1 - \beta_2$ and $1 - \beta_1$ quantiles of the Fisher (F -) distribution with $2k$ degrees of freedom (Appendix A9.4). $\overline{PA}_{a_l} / \overline{PA}_a \approx \widehat{PA}_{a_l} / \widehat{PA}_a \approx \overline{PA}_a / \overline{PA}_a = 1 + \lambda / \mu \approx 1$ can often be used. Figure 7.5 gives the confidence limits for $\beta_1 = \beta_2 = (1 - \gamma) / 2$, useful for practical applications (Example A8.8). One sided confidence intervals are

$$0 \leq \overline{PA} \leq \widehat{PA}_u, \quad \text{with } \gamma = 1 - \beta_1 \quad \text{and} \quad \widehat{PA}_l \leq \overline{PA} < 1, \quad \text{with } \gamma = 1 - \beta_2. \tag{A8.66}$$

Corresponding values for the availability can be obtained using $PA = 1 - \overline{PA}$.

If failure free and/or repair times are Erlangian distributed (Eq. (A6.102)) with $\beta_\lambda = n_\lambda$ & $\beta_\mu = n_\mu$, $F_{2k, 2k, 1 - \beta_2}$ and $F_{2k, 2k, 1 - \beta_1}$ have to be replaced by $F_{2kn_\mu, 2kn_\lambda, 1 - \beta_2}$ and $F_{2kn_\lambda, 2kn_\mu, 1 - \beta_1}$, for unchanged $MTTF$ & $MTRR$ (Example A8.11). Results based on the distribution of DT (Eq. (7.22)) are not free of parameters (Section 7.2.2.3).

Example A8.8

For the estimation of an availability PA , $UT = 1750h$, $DT = 35h$ and $k = 5$ failures and repairs have been observed. Give for const. failure & repair rates the 90% lower limit of PA (Fig. 7.5, $\gamma = 0.8$).

Solution

From Eqs. (A862), (A8.65), (A8.66) & Tab. A9.4a follows $\widehat{PA}_u \approx 2\% \cdot 2.323$ and thus $PA > 95.3\%$.

Suppl. results: Erlangian distrib. times yield $\widehat{PA}_u \approx 2\% \cdot 1.819, n_\mu = 3$ and $\approx 2\% \cdot 1.61, n_\lambda = n_\lambda = 3$.

A8.3 Testing Statistical Hypotheses

When testing a statistical hypothesis, the objective is to solve the following problem:

From one's own experience, the nature of the problem, or simply as a basic hypothesis, a specific null hypothesis H_0 is formulated for the statistical properties of the random variable considered; asked is a rule (test plan) which allows rejection or acceptance of H_0 on the basis of the (totally) independent realizations of this random variable in a suitable sample.

If R is the unknown reliability of an item, following null hypotheses H_0 are possible:

- 1a) $H_0: R = R_0$,
- 1b) $H_0: R > R_0$,
- 1c) $H_0: R < R_0$.

To test whether the failure-free time of an item is distributed according to an exponential distribution $F_0(t) = 1 - e^{-\lambda t}$ with unknown λ , or $F_0(t) = 1 - e^{-\lambda_0 t}$ with known λ_0 , the following null hypotheses H_0 can be formulated:

- 2a) H_0 : the distribution function is $F_0(t)$,
- 2b) H_0 : the distribution function is different from $F_0(t)$,
- 2c) H_0 : $\lambda = \lambda_0$, provided the distribution is exponential,
- 2d) H_0 : $\lambda < \lambda_0$, provided the distribution is exponential,
- 2e) H_0 : the distribution function is $1 - e^{-\lambda t}$, parameter λ unknown.

It is usual to subdivide hypotheses into *parametric* (1a, 1b, 1c, 2c, 2d) and *non-parametric* ones (2a, 2b, and 2e). For each of these types, a distinction is also made between *simple hypotheses* (1a, 2a, 2c) and *composite hypotheses* (1b, 1c, 2b, 2d, 2e).

When testing a hypothesis, *two kinds of errors can occur* (Table A8.2):

- *type I error*, when rejecting a true hypothesis H_0 ; the probability of this error is denoted by α
- *type II error*, when accepting a false hypothesis H_0 ; the probability of this error is denoted by β (to compute β , an *alternative hypothesis* H_1 is necessary, β is then the probability of accepting H_0 assuming H_1 is true).

If the sample space is divided into two complementary sets, \mathcal{A} for acceptance and $\bar{\mathcal{A}}$ for rejection, the type I and type II errors are given by

$$\alpha = \Pr\{\text{sample in } \bar{\mathcal{A}} \mid H_0 \text{ true}\}, \quad (\text{A8.67})$$

$$\beta = \Pr\{\text{sample in } \mathcal{A} \mid H_0 \text{ false } (H_1 \text{ true})\}. \quad (\text{A8.68})$$

Both kinds of error are possible and cannot be minimized simultaneously. Often α

Table A8.2 Possible errors when testing a statistical hypothesis

	H_0 is rejected	H_0 is accepted
H_0 is true	false → type I error (α)	correct
H_0 is false (H_1 is true)	correct	false → type II error (β)

is selected and a test is sought so that, for a given H_1 , β will be minimized. It can be shown that such a test always exists if H_0 and H_1 are simple hypotheses [A8.22]. For given alternative hypothesis H_1 , β can often be calculated and the quantity $1 - \beta = \Pr\{\text{sample in } \bar{A} \mid H_1 \text{ true}\}$ is referred as the *power of the test*.

The following sections consider some procedures for quality control and reliability tests, see Chapter 7 for refinements and applications. Such procedures are basically obtained by investigating suitable quantities observed in the sample.

A8.3.1 Testing an Unknown Probability p

Let A be an event which can occur at every independent trial with the constant, unknown probability p . A rule (test plan) is sought which allows testing the hypothesis

$$H_0: p < p_0, \quad \begin{array}{c} H_0 \\ \text{---} \\ 0 \quad p_0 \quad 1 \end{array} \rightarrow p \quad (\text{A8.69})$$

against the alternative hypothesis

$$H_1: p > p_1 \quad (p_1 \geq p_0). \quad \begin{array}{c} H_1 \\ \text{---} \\ 0 \quad p_1 \quad 1 \end{array} \rightarrow p \quad (\text{A8.70})$$

The *type I error* should be nearly equal to (but not greater than) α for $p = p_0$. The *type II error* should be nearly equal to (but not greater than) β for $p = p_1$. Such a situation often occurs in practical applications, in particular in:

- *quality control*, where p refers to the *defective probability* or fraction of defective items,
- *reliability tests for a given fixed mission*, where it is usual to set $p = 1 - R$ (R =reliability).

In both cases, α is the *producer's risk* and β the *consumer's risk*.⁺⁾ The two most frequently used procedures for testing hypotheses defined by (A8.69) and (A8.70), with $p_1 > p_0$, are the simple two-sided sampling plan and the sequential test (*one-sided sampling plans* are considered in Appendix A8.3.1.3).

⁺⁾ Considering the visualization given with Eqs. (A8.69) & (A8.70), H_0 is true for $p < p_0$ and H_1 is true for $p > p_1$; between p_0 and p_1 both hypothesis are false.

A8.3.1.1 Simple Two-sided Sampling Plan

The rule for the *simple two-sided sampling plan* (simple two-sided test) is:

1. For given p_0 , $p_1 > p_0$, α , and β ($0 < \alpha < 1 - \beta < 1$), compute the smallest integers c and n which satisfy

$$\sum_{i=0}^c \binom{n}{i} p_0^i (1-p_0)^{n-i} \geq 1 - \alpha \quad (\text{A8.71})$$

and

$$\sum_{i=0}^c \binom{n}{i} p_1^i (1-p_1)^{n-i} \leq \beta. \quad (\text{A8.72})$$

2. Perform n independent trials (Bernoulli trials), determine the number k in which the event A (component defective for example) has occurred, and

- reject $H_0: p < p_0$, if $k > c$,
- accept $H_0: p < p_0$, if $k \leq c$. (A8.73)

As in the case of Eqs. (A8.37) and (A8.38), the proof of the above rule is based on the monotonic property of $B_n(c, p) = \sum_{i=0}^c \binom{n}{i} p^i (1-p)^{n-i}$, see also Fig A8.4. For known n, c , and p , $B_n(c, p)$ gives the probability of having up to c defectives in a sample of size n . Thus, assuming H_0 true, it follows that the probability of rejecting H_0 (i.e., the probability of having more than c defectives in a sample of size n) is smaller than α

$$\Pr\{\text{rejection of } H_0 \mid H_0 \text{ true}\} = \sum_{i=c+1}^n \binom{n}{i} p^i (1-p)^{n-i} \Big|_{p < p_0} < \alpha.$$

Similarly, if H_1 is true ($p > p_1$), it follows that the probability of accepting H_0 is smaller than β

$$\Pr\{\text{acceptance of } H_0 \mid H_1 \text{ true}\} = \sum_{i=0}^c \binom{n}{i} p^i (1-p)^{n-i} \Big|_{p > p_1} < \beta.$$

The assumptions made with Eqs. (A8.71) and (A8.72) are thus satisfied. As shown by the above inequalities, the type I error and the type II error are *for this case* $< \alpha$ for $p < p_0$ and $< \beta$ for $p > p_1$, respectively. Figure A8.7 shows the results for $p_0 = 1\%$, $p_1 = 2\%$, and $\alpha = \beta \approx 20\%$. The curve of Fig. A8.7 is known as the *operating characteristic curve* (OC). If p_0 and p_1 are small (up to a few %) or close to 1, the *Poisson approximation* (Eq. (A6.129))

$$\binom{n}{i} p^i (1-p)^{n-i} \approx \frac{m^k}{k!} e^{-m}, \quad m = np$$

is generally used.

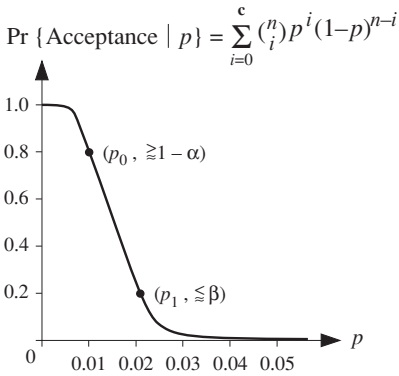


Figure A8.7 Operating characteristic curve (acceptance probability curve) as a function of the unknown probability p for fixed n & c ($p_0=1\%$, $p_1=2\%$, $\alpha \approx \beta \approx 0.185$, $n=462$, $c=6$ as per Tab. 7.3)

A8.3.1.2 Sequential Test

Assume that in a two-sided sampling plan with $n = 50$ and $c = 2$, a 3rd defect, i.e. $k = 3$, occurs at the 12th trial. Since $k > c$, the hypothesis H_0 will be rejected as per procedure (A8.73), independent of how often the event A will occur during the remaining 38 trials. This example brings up the question of whether a plan can be established for testing H_0 in which *no unnecessary trials* (the remaining 38 in the above example) have to be performed. To solve this problem, A. Wald proposed the *sequential test* [A8.33]. For this test, one element after another is taken from the lot and tested. Depending upon the actual frequency of the observed event, the decision is made to either

- reject H_0 ,
- accept H_0 ,
- perform a further trial.

The testing procedure can be described as follows (Fig. A8.8):

In a system of Cartesian coordinates, the number n of trials is recorded on the abscissa and the number k of trials in which the event A occurred on the ordinate; the test is stopped with acceptance or rejection as soon as the resulting staircase curve $k = f(n)$ crosses the acceptance or the rejection line given in the Cartesian coordinates for specified values of p_0 , p_1 , α , and β .

The acceptance and rejection lines can be determined from:

Acceptance line : $k = an - b_1$, (A8.74)

Rejection line : $k = an + b_2$, (A8.75)

with

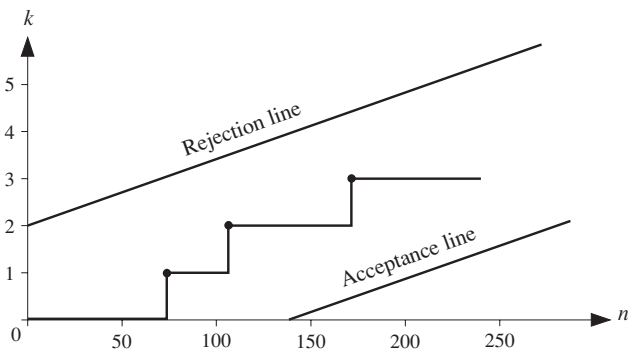


Figure A8.8 Sequential test for $p_0 = 1\%$, $p_1 = 2\%$, and $\alpha = \beta \approx 20\%$

$$a = \frac{\ln \frac{1-p_0}{1-p_1}}{\ln \frac{p_1}{p_0} + \ln \frac{1-p_0}{1-p_1}}, \quad b_1 = \frac{\ln \frac{1-\alpha}{\beta}}{\ln \frac{p_1}{p_0} + \ln \frac{1-p_0}{1-p_1}}, \quad b_2 = \frac{\ln \frac{1-\beta}{\alpha}}{\ln \frac{p_1}{p_0} + \ln \frac{1-p_0}{1-p_1}}. \quad (A8.76)$$

Figure A8.8 shows acceptance and rejection lines for $p_0=1\%$, $p_1=2\%$, $\alpha=\beta=20\%$. Practical remarks to sequential tests are given in Sections 7.1.2.2 and 7.2.3.2.

A8.3.1.3 Simple One-sided Sampling Plan

In many practical applications only p_0 and α or p_1 and β are specified; i. e., one want to test $H_0: p < p_0$ against $H_1: p > p_0$ with given type I error α , or $H_0: p < p_1$ against $H_1: p > p_1$ with given type II error β . For these cases, only Eq. (A8.71) or Eq. (A8.72) can be used and the test plan is a pair (c, n) for each selected value of $c=0,1,\dots$ and calculated value of n . Such plans are termed *one-sided sampling plans*.

Setting $p_1 = p_0$ in the relationship (A8.70) or in other words, testing

$$H_0: p < p_0, \quad (A8.77)$$

against

$$H_1: p > p_0, \quad (A8.78)$$

with type I error α , i. e., using one (c, n) pair (for $c = 0, 1, \dots$) from Eq. (A8.71) and the test procedure (A8.73), the *type II error* can become very large and reach the value $1-\alpha$ for $p=p_0$. Depending upon the value selected for $c = 0, 1, \dots$ and that calculated for n (the smallest integer n which satisfies Eq. (A8.71)), different plans (pairs of (c, n)) are possible. Each of these plans yields different type II errors. Figure A8.9 shows this for some values of c (the type II error is the ordinate of the

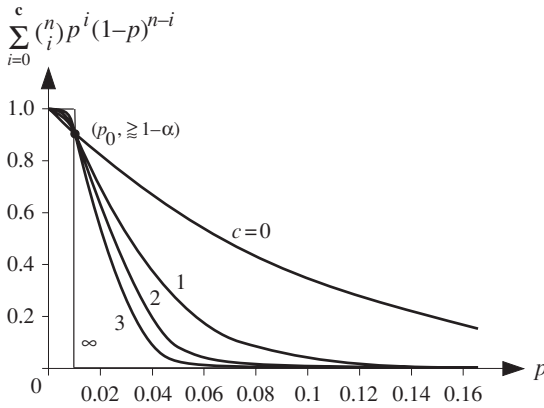


Figure A8.9 Operating characteristics curves (acceptance probability curves) as a function of the unknown probability p for $p_0 = AQL = 1\%$, producer risk $\alpha \approx 0.1$ and $c = 0$ ($n = 10$), $c = 1$ ($n = 53$), $c = 2$ ($n = 110$), $c = 3$ ($n = 174$) and $c = \infty$ ($n = \infty$) as per Fig. 7.3

operating characteristic curve for $p > p_0$). In practical applications, it is common usage to define

$$p_0 = AQL, \tag{A8.79}$$

where AQL stands for *Acceptable Quality Level*. The above considerations show that with the choice of only p_0 and α (instead of p_0, p_1, α , and β) the *producer can realize an advantage*, particularly if small values of c are used.

On the other hand, setting $p_0 = p_1$ in the relationship (A8.69), or testing

$$H_0: p < p_1, \tag{A8.80}$$

against

$$H_1: p > p_1, \tag{A8.81}$$

with type II error β , i. e., using one (c, n) pair (for $c = 0, 1, \dots$) from Eq. (A8.72) and the test procedure (A8.73), the *type I error* can become very large and reach the value $1 - \beta$ for $p = p_1$. Depending upon the value selected for $c = 0, 1, \dots$ and that calculated for n (the largest integer n which satisfies Eq. (A8.72)), different plans (pairs of (c, n)) are possible. Considerations here are similar to those of the previous case, where only p_0 and α were selected. For small values of c the *consumer can realize an advantage*. In practical applications, it is common usage to define

$$p_1 = LTPD, \tag{A8.82}$$

where LTPD stands for *Lot Tolerance Percent Defective*. Further remarks on one-sided sampling plans are in Section 7.1.3.

A8.3.1.4 Availability Demonstration (Erlangian Failure-Free and/or Repair Times)

Considerations of Section A8.2.2.4 on availability estimation can be extended to demonstrate the availability of a repairable item, described by the alternating renewal process of Fig. 6.2, for the case of Erlangian distributed failure-free and/or repair times (Appendix A6.10.3). In particular thus, for the case of constant failure and repair rates (exponentially distributed failure-free and repair times).

Consider a repairable item in continuous operation, new at $t = 0$ (Fig. 6.2), and assume constant failure and repair rates $\lambda(x)=\lambda, \mu(x)=\mu$ (x starting by 0 at the beginning of each operating or repair time, respectively). For this case, point and average *unavailability* converge (Tables 6.3, 6.4) to the asymptotic & steady-state value $1 - PA_S = 1 - AA_S = \lambda / (\lambda + \mu)$, given here as $\overline{PA} = \overline{AA}$ to simplify notation

$$\overline{PA} = 1 - PA = 1 - AA = \overline{AA} = \lambda / (\lambda + \mu). \tag{A8.83}$$

$\lambda / (\lambda + \mu)$ is a probabilistic value of the asymptotic & steady-state unavailability and has his statistical counterpart in $DT / (UT + DT)$, where DT is the *down* (repair) time and UT the *up* (operating) time observed in $(0, t]$. From Eq. (A8.83) it follows that

$$\frac{\overline{PA}}{1 - \overline{PA}} = \frac{\overline{PA}}{PA} = \frac{\lambda}{\mu}.$$

As in Appendix A8.2.2.4, it will be assumed that at the time point t a repair is terminated, and exactly n failure free and n repair times have occurred. However, for a demonstration test, PA or \overline{PA} will be specified (Eqs. (A.8.88) - (A8.89)) and DT/UT observed. Similar as for Eq. (A8.60), the quantity (see footnote on p. 526)

$$\frac{PA}{\overline{PA}} \cdot \frac{DT}{UT} = \frac{\mu}{\lambda} \cdot \frac{\tau_1' + \dots + \tau_n'}{\tau_1 + \dots + \tau_n} = \frac{2\mu (\tau_1' + \dots + \tau_n') / 2n}{2\lambda (\tau_1 + \dots + \tau_n) / 2n} \tag{A8.84}$$

is distributed according to a Fisher (**F**-) distribution with $\nu_1 = \nu_2 = 2n$ degrees of freedom (Appendix A9.4). From this (with DT/UT as a random variable),

$$\Pr\left\{ \frac{PA}{\overline{PA}} \cdot \frac{DT}{UT} \leq x \right\} = \Pr\left\{ \frac{DT}{UT} \leq x \frac{\overline{PA}}{PA} \right\} = \frac{(2n-1)!}{[(n-1)!]^2} \int_0^x \frac{y^{n-1}}{(1+y)^{2n}} dy. \tag{A8.85}$$

Setting

$$\delta = x \cdot \overline{PA} / PA, \tag{A8.86}$$

Eq. (A8.85) yields

$$\Pr\left\{ \frac{DT}{UT} \leq \delta \right\} = \frac{(2n-1)!}{[(n-1)!]^2} \int_0^{\delta \cdot PA / \overline{PA}} \frac{y^{n-1}}{(1+y)^{2n}} dy. \tag{A8.87}$$

Considering $DT / UT = (\tau_1' + \dots + \tau_n') / (\tau_1 + \dots + \tau_n)$, i. e., the sum of n repair times divided by the sum of the corresponding n failure-free times, a rule for testing

$$H_0: \overline{PA} < \overline{PA}_0 \tag{A8.88}$$

against the alternative hypothesis

$$H_1: \overline{PA} > \overline{PA}_1 \quad (\overline{PA}_1 \geq \overline{PA}_0) \tag{A8.89}$$

can be established (as in Appendix A8.3.1.1) for given *type I error* (producer risk) nearly equal to (but not greater than) α for $\overline{PA} = \overline{PA}_0$ and *type II error* (consumer risk) nearly equal to (but not greater than) β for $\overline{PA} = \overline{PA}_1$ (Table A8.2)

$$\Pr\left\{\frac{DT}{UT} > \delta \mid \overline{PA} = \overline{PA}_0\right\} \leq \alpha \quad \text{and} \quad \Pr\left\{\frac{DT}{UT} \leq \delta \mid \overline{PA} = \overline{PA}_1\right\} \leq \beta. \tag{A8.90}$$

From Eqs. (A8.87) & (A8.90), and considering the Fisher (F -) distribution (Appendix A9.4), it follows that $\delta \cdot PA_0 / \overline{PA}_0 \geq F_{2n, 2n, 1-\alpha}$ and $\delta \cdot PA_1 / \overline{PA}_1 \leq F_{2n, 2n, \beta}$. Eliminating δ (using $F_{v_1, v_2, \beta} = 1 / F_{v_2, v_1, 1-\beta}$ and taking the sign = for $F_{2n, 2n, 1-\alpha}$ or for $F_{2n, 2n, \beta}$), the rule for testing $H_0: \overline{PA} = \overline{PA}_0$ against $H_1: \overline{PA} = \overline{PA}_1$ follows as (see also [A8.29, A2.6 (IEC 61070)]):

1. For given $\overline{PA}_0, \overline{PA}_1, \alpha,$ and β ($0 < \alpha < 1 - \beta < 1$), find the smallest integer n (1, 2, ...) which satisfy

$$F_{2n, 2n, 1-\alpha} \cdot F_{2n, 2n, 1-\beta} \leq \frac{\overline{PA}_1}{\overline{PA}_0} \cdot \frac{PA_0}{PA_1} = \frac{(1 - PA_1)PA_0}{(1 - PA_0)PA_1}, \tag{A8.91}$$

where $F_{2n, 2n, 1-\alpha}$ and $F_{2n, 2n, 1-\beta}$ are the $1-\alpha$ and $1-\beta$ quantiles of the F -distribution with $2n$ degrees of freedom (Appendix A9.4, [A9.2- A9.6]), and compute the limiting value

$$\delta = F_{2n, 2n, 1-\alpha} \overline{PA}_0 / PA_0 = F_{2n, 2n, 1-\alpha} (1 - PA_0) / PA_0. \tag{A8.92}$$

2. Observe n failure free times t_1, \dots, t_n and corresponding repair times t'_1, \dots, t'_n and

- reject $H_0: \overline{PA} < \overline{PA}_0$, if $\frac{t'_1 + \dots + t'_n}{t_1 + \dots + t_n} > \delta$
- accept $H_0: \overline{PA} < \overline{PA}_0$, if $\frac{t'_1 + \dots + t'_n}{t_1 + \dots + t_n} \leq \delta$.

$$\tag{A8.93}$$

Corresponding values for the *availability* can be obtained using $PA = 1 - \overline{PA}$.

If failure free and/or repair times are Erlangian distributed (Eq. (A6.102)) with $\beta_{\lambda} = n_{\lambda}$ & $\beta_{\mu} = n_{\mu}$, $F_{2n, 2n, 1-\alpha}$ and $F_{2n, 2n, 1-\beta}$ have to be replaced by $F_{2n \cdot n_{\mu}, 2n \cdot n_{\lambda}, 1-\alpha}$ and $F_{2n \cdot n_{\lambda}, 2n \cdot n_{\mu}, 1-\beta}$, for unchanged *MTTF* & *MTTR* (Example A8.11). Results based on the distribution of DT (Eq. 7.22) are not parameter free (Section 7.2.2.3).

Example A8.9

For the demonstration of an availability PA , customer and producer agree the following parameters: $PA_0 = 1\%$, $\overline{PA}_1 = 6\%$, $\alpha = \beta = 10\%$. Give for the case of constant failure and repair rates ($\lambda(x) = \lambda$ and $\mu(x) = \mu \gg \lambda$) the number n of failures and repairs that have to be observed and the acceptance limit $\delta = (t'_1 + \dots + t'_n) / (t_1 + \dots + t_n)$.

Solution

Eq. (A8.91) & Table A9.4a yields $n = 5$ ($(F_{10, 10, 0.9})^2 = 2.32^2 < (6 \cdot 99 / 1 \cdot 94) < 2.59^2 = (F_{8, 8, 0.9})^2$), see also Tab. 7.2. $\delta = F_{10, 10, 0.9} \overline{PA}_0 / PA_0 = 2.32 \cdot 1 / 99 = 0.0235$ follows from Eq. (A8.92).

Suppl. result: Erlangian distr. repair times with $n_{\mu} = 3$ yields $n = 3$, $\delta = 0.0288$ ($2.85 \cdot 2.13 < 6.32$).

Example A8.10

Give an unbiased estimate for $\overline{PA}_a = \lambda / \mu$.

Solution

Considering λ / μ as a random variable, Eq. (A8.61) yields

$$\Pr \left\{ \frac{\lambda}{\mu} \cdot \frac{UT}{DT} \leq x \right\} = \frac{(2k-1)!}{[(k-1)!]^2} \int_0^x \frac{y^{k-1}}{(1+y)^{2k}} dy.$$

From this, one recognizes (Table A9.4) that $\lambda UT / \mu DT$ has a F -distribution with $\nu_1 = \nu_2 = 2k$. Thus, $E[\lambda UT / \mu DT] = k / (k - 1)$, $k > 1$ (Table A9.4), and

$$E[\lambda \hat{\lambda} / \mu] = \frac{DT}{UT} \cdot \frac{k}{k-1}, \quad k > 1.$$

$\lambda \hat{\lambda} / \mu = DT / UT$ is biased; unbiased is $(1 - 1/k) DT / UT$, $k > 1$.

Example A8.11

Give the degrees of freedom of the F -distribution for the case of Erlangian distributed failure-free & repair times with parameters λ^* , n_λ & μ^* , n_μ , respectively ($\lambda^* = \lambda n_\lambda$ & $\mu^* = \mu n_\mu$ because of the unchanged $MTTF = 1/\lambda = n_\lambda / \lambda^*$ & $MTTR = 1/\mu = n_\mu / \mu^*$ as per Eqs. (A6.84), (A6.106), (A6.99)).

Solution

Let $\tau_1 + \dots + \tau_k$ be the exponentially distributed failure-free times with mean $MTTF = 1/\lambda$. If the actual failure-free times are Erlangian distributed with parameters λ^* , n_λ and mean $MTTF = n_\lambda / \lambda^* = 1/\lambda$, Eqs. A(6.102)-(A6.104) show that the quantity

$$2\lambda^* (\tau_{11} + \tau_{12} + \dots + \tau_{1n_\lambda} + \dots + \tau_{k1} + \tau_{k2} + \dots + \tau_{kn_\lambda}),$$

corresponding to the sum of k Erlangian (λ^* , n_λ) distributed failure-free times, has a χ^2 -distribution with $\nu = 2k n_\lambda$ degrees of freedom (Eq. (A6.102)). Similar is for the repair times τ'_i . Thus, the quantity (Eq. (A8.60))

$$\overline{PA}_a \cdot \frac{UT}{DT} = \frac{\lambda^* / n_\lambda}{\mu^* / n_\mu} \cdot \frac{UT}{DT} = \frac{2\lambda^* (\tau_{11} + \tau_{12} + \dots + \tau_{1n_\lambda} + \dots + \tau_{k1} + \tau_{k2} + \dots + \tau_{kn_\lambda}) / 2k n_\lambda}{2\mu^* (\tau'_{11} + \tau'_{12} + \dots + \tau'_{1n_\mu} + \dots + \tau'_{k1} + \tau'_{k2} + \dots + \tau'_{kn_\mu}) / 2k n_\mu},$$

obtained by considering $\lambda = \lambda^* / n_\lambda$, $\mu = \mu^* / n_\mu$ (to conserve $MTTF = 1/\lambda = n_\lambda / \lambda^*$, $MTTR = 1/\mu = n_\mu / \mu^*$), has a F -distribution with $\nu_1 = 2k \cdot n_\lambda$ and $\nu_2 = 2k \cdot n_\mu$ degrees of freedom (Appendix A9.4). Similarly (Eq. (A8.84)),

$$\frac{PA}{\overline{PA}} \cdot \frac{DT}{UT} = \frac{\mu^* / n_\mu}{\lambda^* / n_\lambda} \cdot \frac{DT}{UT} = \frac{2\mu^* (\tau'_{11} + \tau'_{12} + \dots + \tau'_{1n_\mu} + \dots + \tau'_{n1} + \tau'_{n2} + \dots + \tau'_{nn_\mu}) / 2n n_\mu}{2\lambda^* (\tau_{11} + \tau_{12} + \dots + \tau_{1n_\lambda} + \dots + \tau_{n1} + \tau_{n2} + \dots + \tau_{nn_\lambda}) / 2n n_\lambda}$$

has a F -distribution with $\nu_1 = 2n \cdot n_\mu$ and $\nu_2 = 2n \cdot n_\lambda$ degrees of freedom (Appendix A9.4)

A8.3.2 Goodness-of-fit Tests for Completely Specified $F_0(t)$

Goodness-of-fit tests have the purpose to verify agreement of observed data with a postulated (completely specified or only partially known) model, see e. g. [A8.9]. A typical example is as follows: Given t_1, \dots, t_n as n independent observations of a random variable τ , a rule is sought to test the null hypothesis

$$H_0: \quad \text{the distribution function of } \tau \text{ is } F_0(t), \tag{A8.94}$$

against the alternative hypothesis

$$H_1: \quad \text{the distribution function of } \tau \text{ is not } F_0(t). \tag{A8.95}$$

$F_0(t)$ can be *completely defined* (as in this section) or depend on some unknown parameters which must be estimated from the observed data (as in the next section). In general, less can be said about the risk of accepting a false hypothesis H_0 (to compute the type II error β , a specific alternative hypothesis H_1 must be assumed). For some distribution functions used in reliability theory, particular procedures have been developed, often with different alternative hypotheses H_1 and investigation of the corresponding test power, see e.g. [A8.1, A8.9, A8.23]. Among the distribution-free procedures, the Kolmogorov-Smirnov, Cramér - von Mises, and chi-square (χ^2) tests are frequently used in practical applications to solve the goodness-of-fit problem given by Eqs. (A8.94) & (A8.95). These tests are based upon comparison of the *empirical distribution function* (EDF) $\hat{F}_n(t)$, defined by Eq. (A8.1), with a postulated distribution function $F_0(t)$.

1. The *Kolmogorov-Smirnov test* uses the (supremum) statistic

$$D_n = \sup_{-\infty < t < \infty} \left| \hat{F}_n(t) - F(t) \right| \quad (\text{A8.96})$$

introduced in Appendix A8.1.1. A. N. Kolmogorov showed [A8.20] that if $F_0(t)$ is *continuous*, the distribution of D_n under the hypothesis H_0 is independent of $F_0(t)$. For a given *type I error* α , the hypothesis H_0 must be rejected for

$$D_n > y_{1-\alpha}, \quad (\text{A8.97})$$

where $y_{1-\alpha}$ is defined by

$$\Pr\{D_n > y_{1-\alpha} \mid H_0 \text{ is true}\} = \alpha. \quad (\text{A8.98})$$

Values for $y_{1-\alpha}$ are given in Tables A8.1 and A9.5. Figure A8.10 illustrates the Kolmogorov-Smirnov test with hypothesis H_0 not rejected. Because of its graphical visualization, in particular when *probability charts* are used (Appendix A8.1.3, Section 7.5, Appendix A9.8), the Kolmogorov-Smirnov test is often used in reliability data analysis.

2. The *Cramér - von Mises test* uses the statistic

$$W_n^2 = n \int_{-\infty}^{+\infty} \left[\hat{F}_n(t) - F_0(t) \right]^2 dF_0(t). \quad (\text{A8.99})$$

As in the case of the D_n statistic, for $F_0(t)$ continuous the distribution of W_n^2 is independent of $F_0(t)$ and tabulated (see for instance [A9.5]). The Cramér - von Mises statistic belongs to the so-called *quadratic statistics* defined by

$$Q_n = n \int_{-\infty}^{+\infty} \left[\hat{F}_n(t) - F_0(t) \right]^2 \psi(t) dF_0(t), \quad (\text{A8.100})$$

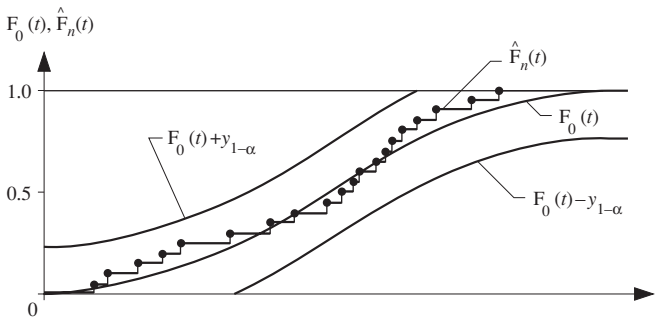


Figure A8.10 Kolmogorov-Smirnov test ($n = 20, \alpha = 20\%$)

where $\psi(t)$ is a suitable weight function. $\psi(t) \equiv 1$ yields the W_n^2 statistic and $\psi(t) = [F_0(t)(1 - F_0(t))]^{-1}$ yields the *Anderson-Darling statistic* A_n^2 . Using the transformation $z_{(i)} = F_0(t_{(i)})$, calculation of W_n^2 and in particular of A_n^2 becomes easy, see e.g. [A8.10]. This transformation can also be used for the Kolmogorov-Smirnov test, although here no change occurs in D_n .

3. The *chi-square (χ^2) goodness-of-fit test* starts from a selected partition $(a_1, a_2], (a_2, a_3], \dots, (a_k, a_{k+1}]$ of the set of possible values of τ and uses the statistic

$$X_n^2 = \sum_{i=1}^k \frac{(k_i - n p_i)^2}{n p_i} = \sum_{i=1}^k \frac{k_i^2}{n p_i} - n, \tag{A8.101}$$

where

$$k_i = n(\hat{F}_n(a_{i+1}) - \hat{F}_n(a_i)) \tag{A8.102}$$

is the number of observations (realizations of τ) in $(a_i, a_{i+1}]$ and

$$n p_i = n(F_0(a_{i+1}) - F_0(a_i)) \tag{A8.103}$$

is the expected number of observations in $(a_i, a_{i+1}]$; obviously, $k_1 + \dots + k_k = n$ and $p_1 + \dots + p_k = 1$. Under the hypothesis H_0 , K. Pearson [A8.28] has shown that the asymptotic distribution of X_n^2 for $n \rightarrow \infty$ is a χ^2 -distribution with $k - 1$ degrees of freedom. Thus, for given type I error α ,

$$\lim_{n \rightarrow \infty} \Pr\{X_n^2 > \chi_{k-1, 1-\alpha}^2 \mid H_0 \text{ true}\} = \alpha \tag{A8.104}$$

holds, and the hypothesis H_0 must be rejected if

$$X_n^2 > \chi_{k-1, 1-\alpha}^2. \tag{A8.105}$$

$\chi_{k-1, 1-\alpha}^2$ is the $(1 - \alpha)$ quantile of the χ^2 -distribution with $k - 1$ degrees of

freedom (Table A9.3). The classes $(a_1, a_2]$, $(a_2, a_3]$, ..., $(a_k, a_{k+1}]$ have to be chosen *before* the test is performed, in such a way that all p_i are approximately equal. Convergence is generally good, even for relatively small values of n ($np_i \geq 5$). Thus,

by selecting the classes $(a_1, a_2]$, $(a_2, a_3]$, ..., $(a_k, a_{k+1}]$ (before the test is performed) one should take care that all np_i are almost equal and ≥ 5 .

Example A8.12 shows an application of the chi-square test.

When in a goodness-of-fit test, the deviation between $\hat{F}_n(t)$ and $F_0(t)$ seems abnormally small, a verification against *superconform* (superuniform if the transformation $z_{(i)} = F_0(t_{(i)})$ is used) can become necessary. Tabulated values for the lower limit $l_{1-\alpha}$ for D_n are e.g. in [A8.1] (for instance, $\alpha = 0.1 \rightarrow l_{1-\alpha} = 0.57 / \sqrt{n}$).

Example A8.12

Accelerated life testing of a wet Al electrolytic capacitor leads to the following 13 ordered observations of lifetime: 59, 71, 153, 235, 347, 589, 837, 913, 1185, 1273, 1399, 1713, and 2567 h. Using the chi-square test and the 4 classes (0, 200], (200, 600], (600, 1200], (1200, ∞), verify at the level $\alpha = 0.1$ (i. e. with first kind error $\alpha = 0.1$) whether or not the failure-free time τ of the capacitors is distributed according to the Weibull distribution $F_0(t) = \Pr\{\tau \leq t\} = 1 - e^{-(10^{-3}t)^{1.2}}$ (hypothesis $H_0: F_0(t) = 1 - e^{-(10^{-3}t)^{1.2}}$).

Solution

The given classes yield number of observations of $k_1 = 3$, $k_2 = 3$, $k_3 = 3$, and $k_4 = 4$. The numbers of expected observations in each classes are, according to Eq. (A8.103), $np_1 = 1.754$, $np_2 = 3.684$, $np_3 = 3.817$, and $np_4 = 3.745$. From Eq. (A8.101) it follows that $X_{13}^2 = 1.204$ and from Table A9.2, $\chi_{3,0.9}^2 = 6.251$. $H_0: F_0(t) = 1 - e^{-(10^{-3}t)^{1.2}}$ can be accepted since $X_n^2 < \chi_{k-1,1-\alpha}^2$ (see also Fig. 7.12).

A8.3.3 Goodness-of-fit Tests for a Distribution $F_0(t)$ with Unknown Parameters

The Kolmogorov-Smirnov test and the tests based on quadratic statistics can be used with some modification when the underlying distribution function $F_0(t)$ is not completely known (unknown parameters). The distribution of the involved statistic D_n , W_n^2 , A_n^2 must be calculated (often using Monte Carlo simulation) for each type of distribution and can depend on the true values of the parameters [A8.1]. For instance, in the case of an exponential distribution $F_0(t, \lambda) = 1 - e^{-\lambda t}$ with parameter λ estimated as per Eq. (A8.28) $\hat{\lambda} = n / (t_1 + \dots + t_n)$, the values of $y_{1-\alpha}$ for the Kolmogorov-Smirnov test have to be modified from those given in Table A8.1, e.g. from $y_{1-\alpha} = 1.36 / \sqrt{n}$ for $\alpha = 0.05$ and $y_{1-\alpha} = 1.22 / \sqrt{n}$ for $\alpha = 0.1$ to [A8.1]

$$\alpha = 0.05 \rightarrow y_{1-\alpha} = 1.09/\sqrt{n},$$

$$\alpha = 0.10 \rightarrow y_{1-\alpha} = 1.0/\sqrt{n}. \tag{A8.106}$$

Also a modification of D_n in $D'_n = (D_n - 0.2/n)(1 + 0.26/\sqrt{n} + 0.5/n)$ is recommended [A8.1]. A heuristic procedure is to use half of the sample (randomly selected) to estimate the parameters and continue with the whole sample and the basic procedure given in Appendix A8.3.2 [A8.11, A8.32].

The chi-square (χ^2) test offers a more general approach. Let $F_0(t, \theta_1, \dots, \theta_r)$ be the assumed distribution function, known up to the parameters $\theta_1, \dots, \theta_r$ ($r < k-1$). If

- the unknown parameters $\theta_1, \dots, \theta_r$ are estimated according to the *maximum likelihood method* on the basis of the observed frequencies k_i using the *multinomial distribution* (Eq. (A6.124)), i.e. from the following system of algebraic equations (Example A8.13)

$$\sum_{i=1}^k \frac{k_i}{p_i(\theta_1, \dots, \theta_r)} \cdot \frac{\partial p_i(\theta_1, \dots, \theta_r)}{\partial \theta_j} \Big|_{\theta_j = \hat{\theta}_j} = 0, \quad j = 1, \dots, r, \tag{A8.107}$$

with

$$p_i = F_0(a_{i+1}, \theta_1, \dots, \theta_r) - F_0(a_i, \theta_1, \dots, \theta_r) > 0,$$

$$p_1 + \dots + p_k = 1,$$

and

$$k_1 + \dots + k_k = n,$$

- $\frac{\partial p_i}{\partial \theta_j}$ and $\frac{\partial^2 p_i}{\partial \theta_j \partial \theta_m}$ exist ($i = 1, \dots, k; j, m = 1, \dots, r < k-1$),
- the matrix with elements $\frac{\partial p_i}{\partial \theta_j}$ is of rank r ,

then the statistic

$$\hat{X}_n^2 = \sum_{i=1}^k \frac{(k_i - n \hat{p}_i)^2}{n \hat{p}_i} = \sum_{i=1}^k \frac{k_i^2}{n \hat{p}_i} - n, \tag{A8.108}$$

calculated with $\hat{p}_i = F_0(a_{i+1}, \hat{\theta}_1, \dots, \hat{\theta}_r) - F_0(a_i, \hat{\theta}_1, \dots, \hat{\theta}_r)$, has under H_0 asymptotically for $n \rightarrow \infty$ a χ^2 -distribution with $k-1-r$ degrees of freedom (R. A. Fisher [A8.15 (1924)]), see Example 7.18 for a practical application. Thus, for a given type I error α ,

$$\lim_{n \rightarrow \infty} \Pr\{\hat{X}_n^2 > \chi_{k-1-r, 1-\alpha}^2 \mid H_0 \text{ true}\} = \alpha, \tag{A8.109}$$

holds, and the hypothesis H_0 must be rejected if

$$\hat{X}_n^2 > \chi_{k-1-r, 1-\alpha}^2. \tag{A8.110}$$

$\chi_{k-1-r, 1-\alpha}^2$ is the $(1-\alpha)$ quantile of the χ^2 -distribution with $k-1-r$ degrees of freedom. Calculation of the parameters $\theta_1, \dots, \theta_r$ directly from the observations t_1, \dots, t_n can lead to wrong decisions.

Example A8.13

Prove Eq. (A8.107).

Solution

The observed frequencies k_1, \dots, k_k in the classes $(a_1, a_2], (a_2, a_3], \dots, (a_k, a_{k+1}]$ result from n trials, where each observation falls into one of the classes $(a_i, a_{i+1}]$ with probability $p_i = F_0(a_{i+1}, \theta_1, \dots, \theta_r) - F_0(a_i, \theta_1, \dots, \theta_r)$, $i = 1, \dots, k$. The *multinomial distribution* applies. Taking into account Eq. (A6.124),

$$\Pr\{\text{in } n \text{ trials } A_1 \text{ occurs } k_1 \text{ times, } \dots, A_k \text{ occurs } k_k \text{ times}\} = \frac{n!}{k_1! \dots k_k!} p_1^{k_1} \dots p_k^{k_k}$$

with

$$k_1 + \dots + k_k = n \text{ and } p_1 + \dots + p_k = 1,$$

the likelihood function (Eq. (A8.23)) becomes

$$L(p_1, \dots, p_k) = \frac{n!}{k_1! \dots k_k!} p_1^{k_1} \dots p_k^{k_k} \quad (\text{A8.111})$$

or

$$\ln L(p_1, \dots, p_k) = \ln \frac{n!}{k_1! \dots k_k!} + k_1 \ln p_1 + \dots + k_k \ln p_k,$$

with

$$p_i = p_i(\theta_1, \dots, \theta_r), \quad p_1 + \dots + p_k = 1, \text{ and } k_1 + \dots + k_k = n.$$

Equation (A8.107) follows then from

$$\frac{\partial \ln L}{\partial \theta_j} = 0 \text{ for } \theta_j = \hat{\theta}_j \text{ and } j = 1, \dots, r,$$

which complete the proof. A practical application with $r = 1$ is given in Example 7.18.

A9 Tables and Charts

A9.1 Standard Normal Distribution

Definition: $\Phi(t) = \Pr\{\tau \leq t\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^t e^{-x^2/2} dx, \quad -\infty < t < \infty$

Parameters: $E[\tau] = 0, \quad \text{Var}[\tau] = 1, \quad \text{Modal value} = E[\tau]$

Properties: • $\Phi(0)=0.5, \quad d\Phi(t)/dt \sim e^{-t^2/2} \rightarrow$ symmetric about $t=0 \rightarrow \Phi(-t) = 1 - \Phi(t)$

• For $E[\tau] = m$ and $\text{Var}[\tau] = \sigma^2, \quad (\tau - m)/\sigma$ has distribution $\Phi(t),$ i.e.

$$F(t) = \Pr\{\tau \leq t\} = \frac{1}{\sigma \sqrt{2\pi}} \int_{-\infty}^t e^{-\frac{(y-m)^2}{2\sigma^2}} dy = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{(t-m)/\sigma} e^{-x^2/2} dx = \Phi\left(\frac{t-m}{\sigma}\right)$$

Characteristic function: $\phi(t) = E[e^{it\tau}] = \frac{1}{\sigma \sqrt{2\pi}} \int_{-\infty}^{\infty} e^{ity} e^{-\frac{(y-m)^2}{2\sigma^2}} dy = e^{itm - (\sigma t)^2/2} \quad ((y-m)/\sigma = z + it\sigma, \quad i = (-1)^{1/2})$

Table A9.1 Standard normal distribution $\Phi(t), 0 \leq t < 3 \quad (t \geq 3, \Phi(t) \approx 1 - e^{-t^2/2} / t \sqrt{2\pi})$ [A9.1-A9.6]

t	0	1	2	3	4	5	6	7	8	9
0.0	.5000	.5040	.5080	.5120	.5160	.5199	.5239	.5279	.5319	.5359
0.1	.5398	.5438	.5478	.5517	.5557	.5596	.5636	.5675	.5714	.5753
0.2	.5793	.5832	.5871	.5910	.5948	.5987	.6026	.6064	.6103	.6141
0.3	.6179	.6217	.6255	.6293	.6331	.6368	.6406	.6443	.6480	.6517
0.4	.6554	.6591	.6628	.6664	.6700	.6736	.6772	.6808	.6844	.6879
0.5	.6915	.6950	.6985	.7019	.7054	.7088	.7123	.7157	.7190	.7224
0.6	.7257	.7291	.7324	.7357	.7389	.7422	.7454	.7486	.7517	.7549
0.7	.7580	.7611	.7642	.7673	.7703	.7734	.7764	.7794	.7823	.7852
0.8	.7881	.7910	.7939	.7967	.7995	.8023	.8051	.8078	.8106	.8133
0.9	.8159	.8186	.8212	.8238	.8264	.8289	.8315	.8340	.8365	.8389
1.0	.8413	.8438	.8461	.8485	.8508	.8531	.8554	.8577	.8599	.8621
1.1	.8643	.8665	.8686	.8708	.8729	.8749	.8770	.8790	.8810	.8830
1.2	.8849	.8869	.8888	.8907	.8925	.8944	.8962	.8980	.8997	.9015
1.3	.9032	.9049	.9066	.9082	.9099	.9115	.9131	.9147	.9162	.9177
1.4	.9192	.9207	.9222	.9236	.9251	.9265	.9279	.9292	.9306	.9319
1.5	.9332	.9345	.9357	.9370	.9382	.9394	.9406	.9418	.9429	.9441
1.6	.9452	.9463	.9474	.9484	.9495	.9505	.9515	.9525	.9535	.9545
1.7	.9554	.9564	.9573	.9582	.9591	.9599	.9608	.9616	.9625	.9633
1.8	.9641	.9649	.9656	.9664	.9671	.9678	.9686	.9693	.9699	.9706
1.9	.9713	.9719	.9726	.9732	.9738	.9744	.9750	.9756	.9761	.9767
2.0	.9772	.9778	.9783	.9788	.9793	.9798	.9803	.9808	.9812	.9817
2.1	.9821	.9826	.9830	.9834	.9838	.9842	.9846	.9850	.9854	.9857
2.2	.9861	.9864	.9868	.9871	.9875	.9878	.9881	.9884	.9887	.9890
2.3	.9893	.9896	.9898	.9901	.9904	.9906	.9909	.9911	.9913	.9916
2.4	.9918	.9920	.9922	.9925	.9927	.9929	.9931	.9932	.9934	.9936
2.5	.9938	.9940	.9941	.9943	.9945	.9946	.9948	.9949	.9951	.9952
2.6	.9953	.9955	.9956	.9957	.9959	.9960	.9961	.9962	.9963	.9964
2.7	.9965	.9966	.9967	.9968	.9969	.9970	.9971	.9972	.9973	.9974
2.8	.9974	.9975	.9976	.9977	.9977	.9978	.9979	.9979	.9980	.9981
2.9	.9981	.9982	.9982	.9983	.9984	.9984	.9985	.9985	.9986	.9986

Examples: $\Pr\{\tau \leq 2.33\} = 0.9901; \quad \Pr\{\tau \leq -1\} = 1 - \Pr\{\tau \leq 1\} = 1 - 0.8413 = 0.1587$

A9.2 χ^2 -Distribution (Chi-Square Distribution)

Definition:
$$F(t) = \Pr\{\chi_v^2 \leq t\} = \frac{1}{2^{v/2}\Gamma(\frac{v}{2})} \int_0^t x^{\frac{v}{2}-1} e^{-x/2} dx = \frac{1}{\Gamma(\frac{v}{2})} \int_0^{t/2} y^{\frac{v}{2}-1} e^{-y} dy,$$

 $t > 0$ ($F(t) = 0$ for $t \leq 0$), $v = 1, 2, \dots$ (degrees of freedom)

Parameters: $E[\chi_v^2] = v, \quad \text{Var}[\chi_v^2] = 2v, \quad \text{Modal value} = v - 2 \quad (v > 2)$

- Relationships:* • Normal distribution: $\chi_v^2 = \frac{1}{\sigma^2} \sum_{i=1}^v (\xi_i - m)^2$, ξ_1, \dots, ξ_v independent normal distrib. with $E[\xi_i] = m, \text{Var}[\xi_i] = \sigma^2$
 (see also Appendices A9.4 & A9.6)
- Exponential distrib.: $\chi_{2n}^2 = 2\lambda(\tau_1 + \dots + \tau_n)$, τ_1, \dots, τ_n indep.exp.distrib.
- Poisson distribution: $\sum_{i=0}^{v/2-1} \frac{(t/2)^i}{i!} e^{-t/2} = 1 - F(t), \quad v = 2, 4, \dots$
- For $\chi_{v_1}^2, \dots, \chi_{v_n}^2$ independent, it holds that $\chi_{v_1}^2 + \dots + \chi_{v_n}^2 = \chi_{v_1+\dots+v_n}^2$

Table A9.2 0.05, 0.1, 0.2, 0.4, 0.6, 0.8, 0.9, 0.95, 0.975 quantiles of the χ^2 -distribution ($t_{v,q} = \chi_{v,q}^2$ for which $F(\chi_{v,q}^2) = q$; $\chi_{v,q}^2 \approx (x + \sqrt{2v-1})^2/2$ for $v > 100$) [A9.1-A9.6]

$v \backslash q$	0.05	0.10	0.20	0.40	0.60	0.80	0.90	0.95	0.975
1	0.0039	0.0158	0.0642	0.275	0.708	1.642	2.706	3.841	5.024
2	0.103	0.211	0.446	1.022	1.833	3.219	4.605	5.991	7.378
3	0.352	0.584	1.005	1.869	2.946	4.642	6.251	7.815	9.348
4	0.711	1.064	1.649	2.753	4.045	5.989	7.779	9.488	11.143
5	1.145	1.610	2.343	3.655	5.132	7.289	9.236	11.070	12.833
6	1.635	2.204	3.070	4.570	6.211	8.558	10.645	12.592	14.449
7	2.167	2.833	3.822	5.493	7.283	9.803	12.017	14.067	16.013
8	2.733	3.490	4.594	6.423	8.351	11.030	13.362	15.507	17.535
9	3.325	4.168	5.380	7.357	9.414	12.242	14.684	16.919	19.023
10	3.940	4.865	6.179	8.295	10.473	13.442	15.987	18.307	20.483
11	4.575	5.578	6.989	9.237	11.530	14.631	17.275	19.675	21.920
12	5.226	6.304	7.807	10.182	12.584	15.812	18.549	21.026	23.337
13	5.892	7.042	8.634	11.129	13.636	16.985	19.812	22.362	24.736
14	6.571	7.790	9.467	12.078	14.685	18.151	21.064	23.685	26.119
15	7.261	8.547	10.307	13.030	15.733	19.311	22.307	24.996	27.488
16	7.962	9.312	11.152	13.983	16.780	20.465	23.542	26.296	28.845
17	8.672	10.085	12.002	14.937	17.824	21.615	24.769	27.587	30.191
18	9.390	10.865	12.857	15.893	18.868	22.760	25.989	28.869	31.526
19	10.117	11.651	13.716	16.850	19.910	23.900	27.204	30.144	32.852
20	10.851	12.443	14.578	17.809	20.951	25.038	28.412	31.410	34.170
22	12.338	14.041	16.314	19.729	23.031	27.301	30.813	33.924	36.781
24	13.848	15.659	18.062	21.652	25.106	29.553	33.196	36.415	39.364
26	15.379	17.292	19.820	23.579	27.179	31.795	35.563	38.885	41.923
28	16.928	18.939	21.588	25.509	29.249	34.027	37.916	41.337	44.461
30	18.493	20.599	23.364	27.442	31.316	36.250	40.256	43.773	46.979
40	26.509	29.051	32.345	37.134	41.622	47.269	51.805	55.758	59.342
60	43.188	46.459	50.641	56.620	62.135	68.972	74.397	79.082	83.298
80	60.391	64.278	69.207	76.188	82.566	90.405	96.578	101.879	106.629
100	77.929	82.358	87.945	95.808	102.946	111.667	118.498	124.342	129.561
x	-1.645	-1.282	-0.842	-0.253	0.253	0.842	1.282	1.645	1.960

Examples: $F(t_{16,0.9}) = 0.9 \rightarrow t_{16,0.9} = \chi_{16,0.9}^2 = 23.542; \quad \sum_{i=0}^8 \frac{13^i}{i!} e^{-13} = 1 - F(26)$ for $v = 18 \approx 0.10$

A9.3 *t* - Distribution (Student Distribution)

Definition: $F(t) = \Pr\{t_v \leq t\} = \frac{\Gamma(\frac{v+1}{2})}{\sqrt{v\pi} \Gamma(\frac{v}{2})} \int_{-\infty}^t (1 + \frac{x^2}{v})^{-(v+1)/2} dx, \quad -\infty < t < \infty,$
 $v = 1, 2, \dots$ (degrees of freedom)

Parameters: $E[t_v] = 0 \quad (v > 1), \quad \text{Var}[t_v] = \frac{v}{v-2} \quad (v > 2), \quad \text{Modal value} = 0$

Properties: $F(0)=0.5, \quad f(t) \sim (v+t^2)^{-\eta} \rightarrow$ symmetric about $t=0 \rightarrow F(-t)=1-F(t)$

- Relationships:*
- Normal distribution and χ^2 -distribution: $t_v = \xi / \sqrt{\chi_v^2 / v}$
 ξ is normal distributed with $E[\xi] = 0$ and $\text{Var}[\xi] = 1$; χ_v^2 is χ^2 distributed with v degrees of freedom, ξ and χ_v^2 independent
 - Cauchy distribution: $F(t)$ with $v = 1$

Table A9.3 0.7, 0.8, 0.9, 0.95, 0.975, 0.99, 0.995, 0.999 quantiles of the *t* - distribution
 $(t_{v,q} = t_{v,q}$ for which $F(t_{v,q}) = q)$ [A9.1-A9.6]

$v \setminus q$	0.7	0.8	0.9	0.95	0.975	0.99	0.995	0.999
1	0.7265	1.3764	3.0777	6.3138	12.7062	31.8207	63.6574	318.3088
2	0.6172	1.0607	1.8856	2.9200	4.3027	6.9646	9.9248	22.3271
3	0.5844	0.9785	1.6377	2.3534	3.1824	4.5407	5.8409	10.2145
4	0.5686	0.9410	1.5332	2.1318	2.7764	3.7469	4.6041	7.1732
5	0.5594	0.9195	1.4759	2.0150	2.5706	3.3649	4.0321	5.8934
6	0.5534	0.9057	1.4398	1.9432	2.4469	3.1427	3.7074	5.2076
7	0.5491	0.8960	1.4149	1.8946	2.3646	2.9980	3.4995	4.7853
8	0.5459	0.8889	1.3968	1.8595	2.3060	2.8965	3.3554	4.5008
9	0.5435	0.8834	1.3839	1.8331	2.2622	2.8214	3.2498	4.2968
10	0.5415	0.8791	1.3722	1.8125	2.2281	2.7638	3.1693	4.1437
11	0.5399	0.8755	1.3634	1.7959	2.2010	2.7181	3.1058	4.0247
12	0.5386	0.8726	1.3562	1.7823	2.1788	2.6810	3.0545	3.9296
13	0.5375	0.8702	1.3502	1.7709	2.1604	2.6503	3.0123	3.8520
14	0.5366	0.8681	1.3450	1.7613	2.1448	2.6245	2.9768	3.7874
15	0.5357	0.8662	1.3406	1.7531	2.1315	2.6025	2.9467	3.7328
16	0.5350	0.8647	1.3368	1.7459	2.1199	2.5835	2.9208	3.6862
17	0.5344	0.8633	1.3334	1.7396	2.1098	2.5669	2.8982	3.6458
18	0.5338	0.8620	1.3304	1.7341	2.1009	2.5524	2.8784	3.6105
19	0.5333	0.8610	1.3277	1.7291	2.0930	2.5395	2.8609	3.5794
20	0.5329	0.8600	1.3253	1.7247	2.0860	2.5280	2.8453	3.5518
22	0.5321	0.8583	1.3212	1.7171	2.0739	2.5083	2.8188	3.5050
24	0.5314	0.8569	1.3178	1.7109	2.0639	2.4922	2.7969	3.4668
26	0.5309	0.8557	1.3150	1.7056	2.0555	2.4786	2.7787	3.4350
28	0.5304	0.8546	1.3125	1.7011	2.0484	2.4671	2.7633	3.4082
30	0.5300	0.8538	1.3104	1.6973	2.0423	2.4573	2.7500	3.3852
40	0.5286	0.8507	1.3031	1.6839	2.0211	2.4233	2.7045	3.3069
60	0.5272	0.8477	1.2958	1.6706	2.0003	2.3901	2.6603	3.2317
80	0.5265	0.8461	1.2922	1.6641	1.9901	2.3739	2.6387	3.1953
100	0.5261	0.8452	1.2901	1.6602	1.9840	2.3642	2.6259	3.1737
∞	0.5240	0.8418	1.2820	1.6450	1.9600	2.3260	2.5760	3.0900

Examples: $F(t_{16, 0.9}) = 0.9 \rightarrow t_{16, 0.9} = t_{16, 0.9} = 1.3368; \quad F(t_{16, 0.1}) = 0.1 \rightarrow t_{16, 0.1} = t_{16, 0.1} = -1.3368$

A9.4 F - Distribution (Fisher Distribution)

Definition:
$$F(t) = \Pr\{F_{v_1, v_2} \leq t\} = \frac{\Gamma(\frac{v_1+v_2}{2})}{\Gamma(\frac{v_1}{2})\Gamma(\frac{v_2}{2})} \frac{v_1}{v_1^2} \frac{v_2}{v_2^2} \frac{t}{0} \int \frac{x^{(v_1-2)/2}}{(v_1x + v_2)^{(v_1+v_2)/2}} dx,$$

 $t > 0$ ($F(t) = 0$ for $t \leq 0$), $v_1, v_2 = 1, 2, \dots$ (degrees of freedom)

Parameters:
$$E[F_{v_1, v_2}] = \frac{v_2}{v_2 - 2} \quad (v_2 > 2), \quad \text{Var}[F_{v_1, v_2}] = \frac{2v_2^2(v_1 + v_2 - 2)}{v_1(v_2 - 2)^2(v_2 - 4)} \quad (v_2 > 4),$$

 Modal value = $v_2(v_1 - 2) / v_1(v_2 + 2)$ ($v_1 > 2$)

Quantiles: $t_{v_1, v_2, \alpha} = F_{v_1, v_2, \alpha} = 1 / t_{v_2, v_1, 1-\alpha} = 1 / F_{v_2, v_1, 1-\alpha}$

Relationships: • χ^2 -distribution: $F_{v_1, v_2} = \frac{\chi_{v_1}^2 / v_1}{\chi_{v_2}^2 / v_2}$, $\chi_{v_1}^2, \chi_{v_2}^2$ independent χ^2 distributed

• Binomial distribution: $\sum_{i=0}^k \binom{n}{i} p^i (1-p)^{n-i} = F\left(\frac{(1-p)(k+1)}{p(n-k)}\right)$
 with $v_1 = 2(n-k)$ and $v_2 = 2(k+1)$

• Beta distribution: $B_{v_1/2, v_2/2} = \frac{v_1 F_{v_1, v_2}}{v_2 + v_1 F_{v_1, v_2}} = \chi_{v_1}^2 / (\chi_{v_1}^2 + \chi_{v_2}^2)$

$B_{a,b}$ has a Beta distribution with density $f(t) = \frac{t^{a-1}(1-t)^{b-1}}{\Gamma(a)\Gamma(b)/\Gamma(a+b)}$, $0 < t < 1$

Table A9.4a 0.90 quantiles of the F-distribution ($t_{v_1, v_2, 0.9} = F_{v_1, v_2, 0.9}$ for which $F(F_{v_1, v_2, 0.9}) = 0.9$) [A9.1 - A9.6]

$v_2 \setminus v_1$	1	2	3	4	5	6	8	10	20	50	∞
1	39.86	49.50	53.59	55.83	57.24	58.20	59.44	60.19	61.74	62.69	63.33
2	8.526	9.000	9.162	9.243	9.293	9.325	9.367	9.392	9.441	9.471	9.491
3	5.538	5.462	5.391	5.343	5.309	5.285	5.252	5.230	5.184	5.155	5.134
4	4.545	4.325	4.191	4.107	4.051	4.010	3.955	3.920	3.844	3.795	3.761
5	4.060	3.780	3.619	3.520	3.453	3.404	3.339	3.297	3.207	3.147	3.105
6	3.776	3.463	3.289	3.181	3.107	3.055	2.983	2.937	2.836	2.770	2.722
7	3.589	3.257	3.074	2.960	2.883	2.827	2.752	2.702	2.595	2.523	2.471
8	3.458	3.113	2.924	2.806	2.726	2.668	2.589	2.538	2.425	2.348	2.293
9	3.360	3.006	2.813	2.693	2.611	2.551	2.469	2.416	2.298	2.218	2.159
10	3.285	2.924	2.728	2.605	2.522	2.461	2.377	2.323	2.201	2.117	2.055
12	3.176	2.807	2.605	2.480	2.394	2.331	2.245	2.188	2.060	1.970	1.904
14	3.102	2.726	2.522	2.395	2.307	2.243	2.154	2.095	1.962	1.869	1.797
16	3.048	2.668	2.462	2.333	2.244	2.178	2.088	2.028	1.891	1.793	1.718
18	3.007	2.624	2.416	2.286	2.196	2.130	2.038	1.977	1.837	1.736	1.657
20	2.975	2.589	2.380	2.249	2.158	2.091	1.998	1.937	1.794	1.690	1.607
30	2.881	2.489	2.276	2.142	2.049	1.980	1.884	1.819	1.667	1.552	1.456
50	2.809	2.412	2.197	2.061	1.966	1.895	1.796	1.729	1.568	1.441	1.327
100	2.756	2.356	2.139	2.002	1.906	1.834	1.732	1.663	1.494	1.355	1.214
1000	2.711	2.308	2.089	1.950	1.853	1.780	1.676	1.605	1.428	1.273	1.060
∞	2.705	2.303	2.084	1.945	1.847	1.774	1.670	1.599	1.421	1.263	1.000

Example: $v_1 = 10, v_2 = 16 \rightarrow t_{10, 16, 0.9} = F_{10, 16, 0.9} = 2.028$

Table A9.4b 0.95 quantiles of the F -distribution ($t_{v_1, v_2, 0.95} = F_{v_1, v_2, 0.95}$ for which $F(F_{v_1, v_2, 0.95}) = 0.95$) [A9.1 - A9.6]

$v_2 \setminus v_1$	1	2	3	4	5	6	8	10	20	50	∞
1	161.4	199.5	215.7	224.6	230.2	234.0	238.9	241.9	248.0	251.8	254.3
2	18.51	19.00	19.16	19.25	19.30	19.33	19.37	19.40	19.45	19.48	19.50
3	10.13	9.552	9.277	9.117	9.013	8.941	8.845	8.785	8.660	8.581	8.526
4	7.709	6.944	6.591	6.388	6.256	6.163	6.041	5.964	5.802	5.699	5.628
5	6.608	5.786	5.409	5.192	5.050	4.950	4.818	4.735	4.558	4.444	4.365
6	5.987	5.143	4.757	4.534	4.387	4.284	4.147	4.060	3.874	3.754	3.669
7	5.591	4.737	4.347	4.120	3.971	3.866	3.726	3.636	3.444	3.319	3.230
8	5.318	4.459	4.066	3.838	3.687	3.580	3.438	3.347	3.150	3.020	2.928
9	5.117	4.256	3.863	3.633	3.482	3.374	3.230	3.137	2.936	2.803	2.707
10	4.965	4.103	3.708	3.478	3.326	3.217	3.072	2.978	2.774	2.637	2.538
12	4.747	3.885	3.490	3.259	3.106	2.996	2.849	2.753	2.544	2.401	2.296
14	4.600	3.739	3.344	3.112	2.958	2.848	2.699	2.602	2.388	2.240	2.131
16	4.494	3.634	3.239	3.007	2.852	2.741	2.591	2.493	2.276	2.124	2.010
18	4.414	3.555	3.160	2.928	2.773	2.661	2.510	2.412	2.191	2.035	1.917
20	4.351	3.493	3.098	2.866	2.711	2.599	2.447	2.348	2.124	1.966	1.843
30	4.171	3.316	2.922	2.690	2.534	2.420	2.266	2.165	1.932	1.761	1.622
50	4.034	3.183	2.790	2.557	2.400	2.286	2.130	2.026	1.784	1.599	1.438
100	3.936	3.087	2.695	2.463	2.305	2.191	2.032	1.927	1.676	1.477	1.283
1000	3.851	3.005	2.614	2.381	2.223	2.108	1.948	1.840	1.581	1.363	1.078
∞	3.841	2.996	2.605	2.372	2.214	2.099	1.938	1.831	1.570	1.350	1.000

A9.5 Table for the Kolmogorov - Smirnov Test

$$D_n = \sup_{-\infty < t < \infty} | \hat{F}_n(t) - F_0(t) | , \quad \hat{F}_n(t) = \text{empirical distribution function (Eq. (A8.1))}$$

$$F_0(t) = \text{postulated continuous distribution function}$$

Table A9.5 $1 - \alpha$ quantiles of the distrib. funct. of D_n ($\Pr\{D_n \leq y_{1-\alpha} \mid H_0 \text{ true}\} = 1 - \alpha$) [A9.2 - A9.6]

n	$\alpha = 0.20$	0.10	0.05	0.02	0.01	n	$\alpha = 0.20$	0.10	0.05	0.02	0.01
1	0.900	0.950	0.975	0.990	0.993	21	0.226	0.259	0.287	0.321	0.344
2	684	776	842	900	929	22	221	253	281	314	337
3	565	636	708	785	829	23	216	247	275	307	330
4	493	565	624	689	734	24	212	242	269	301	323
5	447	509	563	627	669	25	208	238	264	295	317
6	410	468	519	577	617	26	204	233	259	290	311
7	381	436	483	538	576	27	200	229	254	284	305
8	358	410	454	507	542	28	197	225	250	279	300
9	339	387	430	480	513	29	193	221	246	275	295
10	323	369	409	457	489	30	190	218	242	270	290
11	308	352	391	437	468	32	184	211	234	262	281
12	296	338	375	419	449	34	179	205	227	254	273
13	285	325	361	404	432	36	174	199	221	247	265
14	275	314	349	390	418	38	170	194	215	241	258
15	266	304	338	377	404	40	165	189	210	235	252
16	258	295	327	366	392	42	162	185	205	229	246
17	250	286	318	355	381	44	158	181	201	224	241
18	244	279	300	346	371	46	155	177	196	219	235
19	237	271	301	337	361	48	151	173	192	215	231
20	232	265	294	329	352	50	148	170	188	211	226

Example: $n = 20, \alpha = 0.10 \rightarrow y_{1-\alpha} = 0.265$ for $n > 50$ $\approx \frac{1.070}{n^{1/2}}$ $\approx \frac{1.220}{n^{1/2}}$ $\approx \frac{1.360}{n^{1/2}}$ $\approx \frac{1.520}{n^{1/2}}$ $\approx \frac{1.630}{n^{1/2}}$

A9.6 Gamma Function

Definition: $\Gamma(z) = \int_0^{\infty} x^{z-1} e^{-x} dx, \quad \text{Re}(z) > 0$ (Euler's integral), solution of $\Gamma(z+1) = z\Gamma(z)$ with $\Gamma(1) = 1$

Special values: $\Gamma(0) = \infty, \quad \Gamma(\frac{1}{2}) = \sqrt{\pi}, \quad \Gamma(1) = \Gamma(2) = 1, \quad \Gamma(\infty) = \infty$
 $(\Gamma(\frac{1}{2}) \Rightarrow \int_0^{\infty} x^{-1/2} e^{-x} dx = 2 \int_0^{\infty} e^{-y^2} dy = \sqrt{\pi}, \text{ Poisson's integral;}$
 yielding $\int_0^{\infty} e^{-a^2 t^2} dt = \frac{\sqrt{\pi}}{2a}$ and, using $\frac{d}{da}, \int_0^{\infty} t^2 e^{-a^2 t^2} dt = \frac{\sqrt{\pi}}{4a^3}, a > 0)$

Factorial: $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n = \Gamma(n+1)$
 $= \sqrt{2\pi} n^{n+1/2} e^{-n+\theta/12n}, \quad 0 < \theta < 1 \quad (\text{Stirling's formula})$

Relationships:

- Beta function: $B(z, w) = \int_0^1 x^{z-1} (1-x)^{w-1} dx = \frac{\Gamma(z)\Gamma(w)}{\Gamma(z+w)}$
- Psi function: $\psi(z) = d(\ln \Gamma(z))/dz = (d\Gamma(z)/dz)/\Gamma(z)$
- Duplication: $\Gamma(2z) = (2\pi)^{-1/2} 2^{2z-1/2} \Gamma(z)\Gamma(z+1/2)$
- Incomplete Gamma function:
 $\gamma(z, t) = \int_0^t x^{z-1} e^{-x} dx = \Gamma(z) - \int_t^{\infty} x^{z-1} e^{-x} dx, \quad \text{Re}(z) > 0$
- χ^2 -distribution (F(t) as in Appendix A9.2): $\gamma(\frac{v}{2}, \frac{t}{2}) = F(t) \Gamma(\frac{v}{2})$

Table A9.6 Gamma function for $1.00 \leq t \leq 1.99$ (t real), for other values use $\Gamma(z+1) = z\Gamma(z)$ [A9.1 - A9.6]

t	0	1	2	3	4	5	6	7	8	9
1.00	1.0000	.9943	.9888	.9835	.9784	.9735	.9687	.9641	.9597	.9554
1.10	.9513	.9474	.9436	.9399	.9364	.9330	.9298	.9267	.9237	.9209
1.20	.9182	.9156	.9131	.9107	.9085	.9064	.9044	.9025	.9007	.8990
1.30	.8975	.8960	.8946	.8934	.8922	.8911	.8902	.8893	.8885	.8878
1.40	.8873	.8868	.8863	.8860	.8858	.8857	.8856	.8856	.8857	.8859
1.50	.8862	.8866	.8870	.8876	.8882	.8889	.8896	.8905	.8914	.8924
1.60	.8935	.8947	.8959	.8972	.8986	.9001	.9017	.9033	.9050	.9068
1.70	.9086	.9106	.9126	.9147	.9168	.9191	.9214	.9238	.9262	.9288
1.80	.9314	.9341	.9368	.9397	.9426	.9456	.9487	.9518	.9551	.9584
1.90	.9618	.9652	.9688	.9724	.9761	.9799	.9837	.9877	.9917	.9958

Examples: $\Gamma(1.25) = 0.9064; \quad \Gamma(0.25) = \Gamma(1.25) / 0.25 = 3.6256; \quad \Gamma(2.25) = 1.25 \cdot \Gamma(1.25) = 1.133$

A9.7 Laplace Transform

Definition: $\tilde{F}(s) = \int_0^\infty e^{-st} F(t) dt$ $F(t)$ defined for $t \geq 0$, piecewise continuous,
 $|F(t)| < A e^{Bt}$ ($0 < A, B < \infty$)

Inverse transf.: $F(t) = \frac{1}{2\pi i} \int_{C-i\infty}^{C+i\infty} \tilde{F}(s) e^{st} ds$ exists in the halfplan $\text{Re}(s) = C > B$, $i = \sqrt{-1}$

Moment generating function: Considering $f(t)$ as density of $\tau > 0$, it follows (under weak conditions) that

$$\tilde{f}(s) = \int_0^\infty e^{-st} f(t) dt = E[e^{-s\tau}] = E\left[\sum_{k=0}^\infty \frac{(-s)^k \tau^k}{k!}\right] = \sum_{k=0}^\infty \frac{s^k}{k!} (-1)^k E[\tau^k];$$

thus, except for the sign, the k th coefficient of the MacLaurin expansion of $\tilde{f}(s)$,

$$\text{or } \frac{d^k \tilde{f}(s)}{ds^k} \Big|_{s=0}, \text{ is } E[\tau^k] \quad (f(t) = \lambda e^{-\lambda t} \Rightarrow \tilde{f}(s) = \frac{\lambda}{s+\lambda} = \sum_{k=0}^\infty \frac{s^k}{k!} (-1)^k \frac{\lambda^k}{\lambda^k} \Rightarrow E[\tau^k] = \frac{k!}{\lambda^k};$$

for arbitrary τ , the characteristic function $E[e^{it\tau}] = \int_{-\infty}^\infty e^{itx} f(x) dx$ applies)

Table A9.7a Properties of the Laplace Transform

	Transform Domain	Time Domain
Linearity	$a_1 \tilde{F}_1(s) + a_2 \tilde{F}_2(s)$	$a_1 F_1(t) + a_2 F_2(t)$
Scale Change	$\tilde{F}(s/a)$	$a F(at), \quad a > 0$
Shift	$\tilde{F}(s-a)$	$e^{at} F(t)$
	$e^{-as} \tilde{F}(s)$	$F(t-a) u(t-a), ** \quad a > 0$
Differentiation	$s^n \tilde{F}(s) - s^{n-1} F(+0) - \dots - F^{(n-1)}(+0)$	$d^n F(t) / dt^n$
	$d^n \tilde{F}(s) / ds^n$	$(-1)^n t^n F(t)$
Integration	$\frac{1}{s} \tilde{F}(s); \quad \frac{1}{s} \tilde{F}(s+\alpha)$	$\int_0^t F(x) dx; \quad \int_0^t F(x) e^{-\alpha x} dx$
	$\int_s^\infty \tilde{F}(z) dz$	$\frac{F(t)}{t}$
Convolution ($F_1 * F_2$)	$\tilde{F}_1(s) \tilde{F}_2(s)$	$\int_0^t F_1(x) F_2(t-x) dx$
Initial Val. Theorem	$\lim_{s \rightarrow \infty} s \tilde{F}(s)$	$\lim_{t \downarrow 0} F(t) = F(+0)$
Final Val. Theorem *	$\lim_{s \downarrow 0} s \tilde{F}(s)$	$\lim_{t \rightarrow \infty} F(t)$

* Existence of the limit is assumed; ** $u(t)$ is the unit step function (see Table A9.7b)

Table A9.7b Important Laplace Transforms

Transform Domain	Time Domain
$\tilde{F}(s) = \int_0^{\infty} F(t) e^{-s t} dt$	$F(t)$ (understood as $u(t) \cdot F(t)$, with $u(t)$ as unit step)
1	Impulse $\delta(t)$ (for $a > 0$, $\delta(t - a) \Rightarrow e^{-sa}$)
$\frac{1}{s}$	Unit step $u(t)$ ($u(t) = 0$ for $t < 0$, $u(t) = 1$ for $t \geq 0$; e.g. $\lambda e^{-\lambda t} (1 - u(t-a)) \Rightarrow \frac{\lambda}{s+\lambda} (1 - e^{-(s+\lambda)a})$ and $\lambda e^{-\lambda t} u(t-a) \Rightarrow \frac{\lambda}{s+\lambda} e^{-(s+\lambda)a}$)
$\frac{1}{s^n}$, $n = 1, 2, \dots$	$\frac{t^{n-1}}{(n-1)!}$, ($n! = 1 \cdot 2 \cdot \dots \cdot n$, $0! = 1$)
$\frac{1}{(s+a)^n}$, $n = 1, 2, \dots$	$\frac{t^{n-1}}{(n-1)!} e^{-at}$, ($n! = 1 \cdot 2 \cdot \dots \cdot n$, $0! = 1$)
$\frac{1}{(s+a)^\beta}$, $\beta > 0$	$\frac{t^{\beta-1} e^{-at}}{\Gamma(\beta)}$, ($\beta = n \rightarrow \Gamma(\beta) = (n-1)!$, $0! = 1$)
$\frac{1}{(s+a)(s+b)}$, $a \neq b$	$\frac{e^{-bt} - e^{-at}}{a-b}$ (e.g. $\frac{\lambda}{s(s+\lambda)} \Rightarrow 1 - e^{-\lambda t}$)
$\frac{s}{(s+a)(s+b)}$, $a \neq b$	$\frac{a e^{-at} - b e^{-bt}}{a-b}$
$\frac{s+a}{s^2(s+b)}$, $a \neq b$	$\frac{a}{b} t + \frac{b-a}{b^2} (1 - e^{-bt})$
$\frac{1}{(s+\beta)^2 + \alpha^2}$	$\frac{1}{\alpha} e^{-\beta t} \sin(\alpha t)$
$\frac{s+\beta}{(s+\beta)^2 + \alpha^2}$	$e^{-\beta t} \cos(\alpha t)$
$\frac{P(s)}{Q(s)}$, $Q(s) = \prod_{k=1}^n (s - a_k)$, degree $P(s) < n$	$\sum_{k=1}^n \frac{P(a_k)}{Q'(a_k)} e^{a_k t}$, $Q'(a_k) = \left. \frac{dQ(s)}{ds} \right _{s=a_k}$
$\frac{\mu + s \cdot e^{-(s+\mu)\Delta}}{s(s+\mu)}$	$\begin{cases} 1 - e^{-\mu t} & \text{for } 0 < t < \Delta \\ 1 & \text{for } t \geq \Delta \end{cases}$ (truncated exponential distribution function)

A9.8 Probability Charts

A distribution function appears as a straight line when plotted on a probability chart belonging to its family. The use of probability charts (probability plot papers), simplifies the analysis and interpretation of data, in particular of life times or failure-free times (failure-free operating time). In the following the charts for *lognormal*, *Weibull*, and *normal* distributions are given.

A9.8.1 Lognormal Probability Chart

The distribution function (Eq. (A6.110), Table A6.1)

$$F(t) = \frac{1}{\sigma\sqrt{2\pi}} \int_0^t \frac{1}{y} e^{-\frac{(\ln y + \ln \lambda)^2}{2\sigma^2}} dy = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{\ln(\lambda t)}{\sigma}} e^{-x^2/2} dx \quad \begin{matrix} t > 0; \lambda, \sigma > 0 \\ (F(t) = 0 \text{ for } t \leq 0) \end{matrix}$$

appears as a straight line on the chart of Fig. A9.1 (λ in h^{-1} for t in h), see Fig. 7.14. $F(t)=0.5$, yielding $\lambda = 1/t_{0.5}$, and $F(t)=0.99$, yielding $\ln(t_{0.99}/t_{0.5})/\sigma \approx 2.33$, can be used for a graphical estimation of $\hat{\lambda}$ and $\hat{\sigma}$.

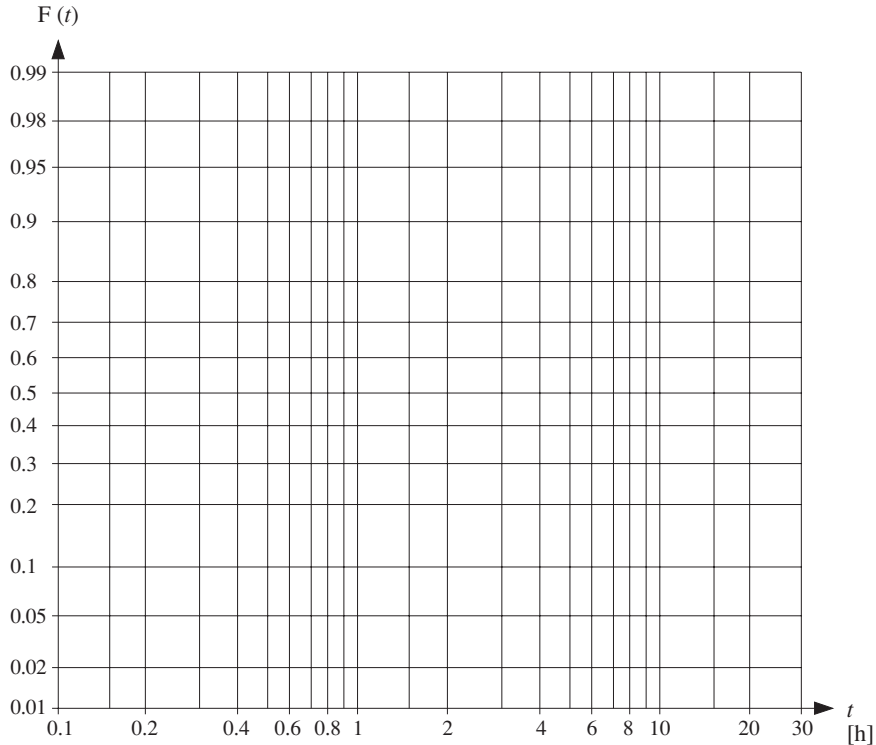


Figure A9.1 Lognormal probability chart

A9.8.2 Weibull Probability Chart

The distribution function $F(t) = 1 - e^{-(\lambda t)^\beta}$, $t > 0$ ($F(t) = 0$ for $t \leq 0$), $\lambda, \beta > 0$ (Eq. (A6.89), Table A6.1) appears as a straight line on the chart of Fig. A9.2 (λ in h^{-1} for t in h), see Fig. A8.2. On the dashed line, $\lambda = 1/t$; furthermore, β appears on the scale $\log_{10} \log_{10}(\frac{1}{1-F(t)})$ when t is varied by one decade (Figs. A8.2, 7.12, 7.13).

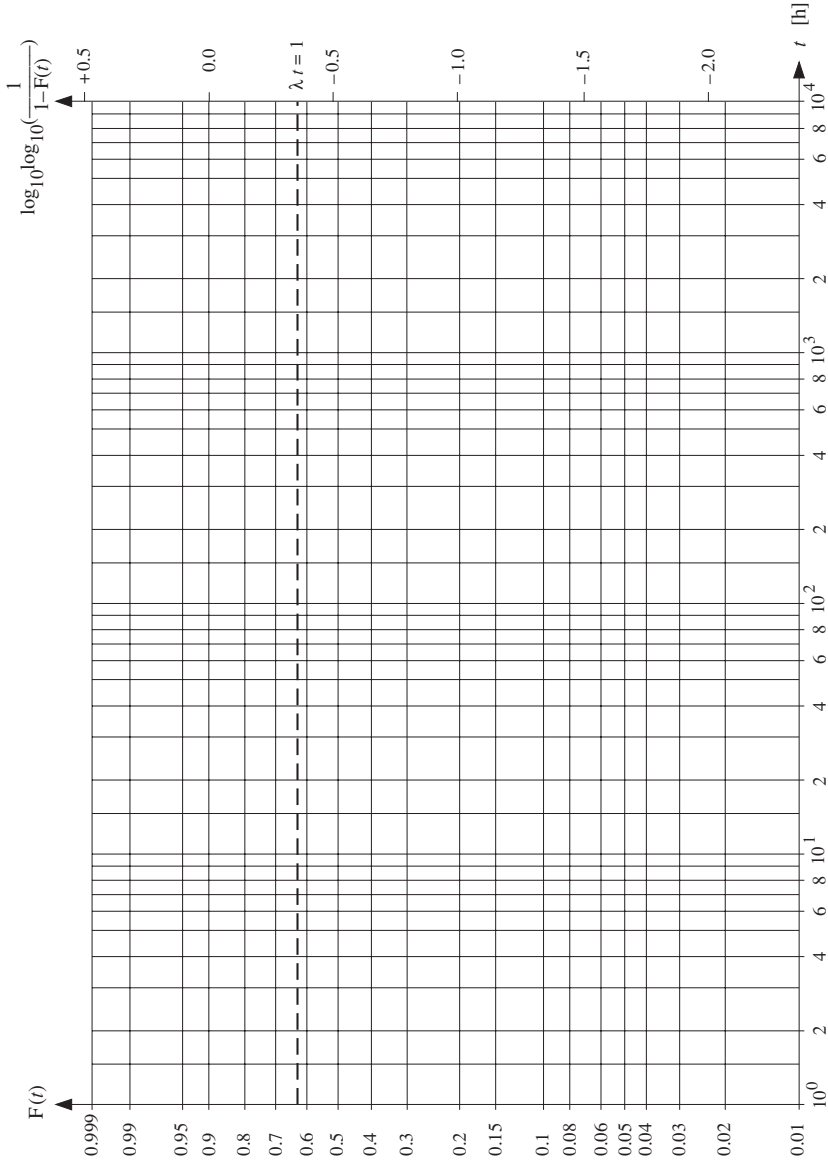


Figure A9.2 Weibull probability chart

A9.8.3 Normal Probability Chart

The distribution function (Eq. (A6.105), Table A6.1)

$$F(t) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^t e^{-\frac{(y-m)^2}{2\sigma^2}} dy = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{t-m}{\sigma}} e^{-x^2/2} dx = \Phi\left(\frac{t-m}{\sigma}\right), \quad -\infty < t, m < \infty, \sigma > 0$$

appears as a straight line on the chart of Fig. A9.3. $F(t) = 0.5$, yielding $m = t_{0.5}$, and $F(t) = 0.99$, yielding $\sigma \approx (t_{0.99} - t_{0.5}) / 2.33$, can be used for a graphical estimation of \hat{m} and $\hat{\sigma}$. However, it is often more useful to estimate \hat{m} and $\hat{\sigma}$ as per Eqs. (A8.6), (A8.10) and to operate with $\Phi\left(\frac{t-\hat{m}}{\hat{\sigma}}\right)$.

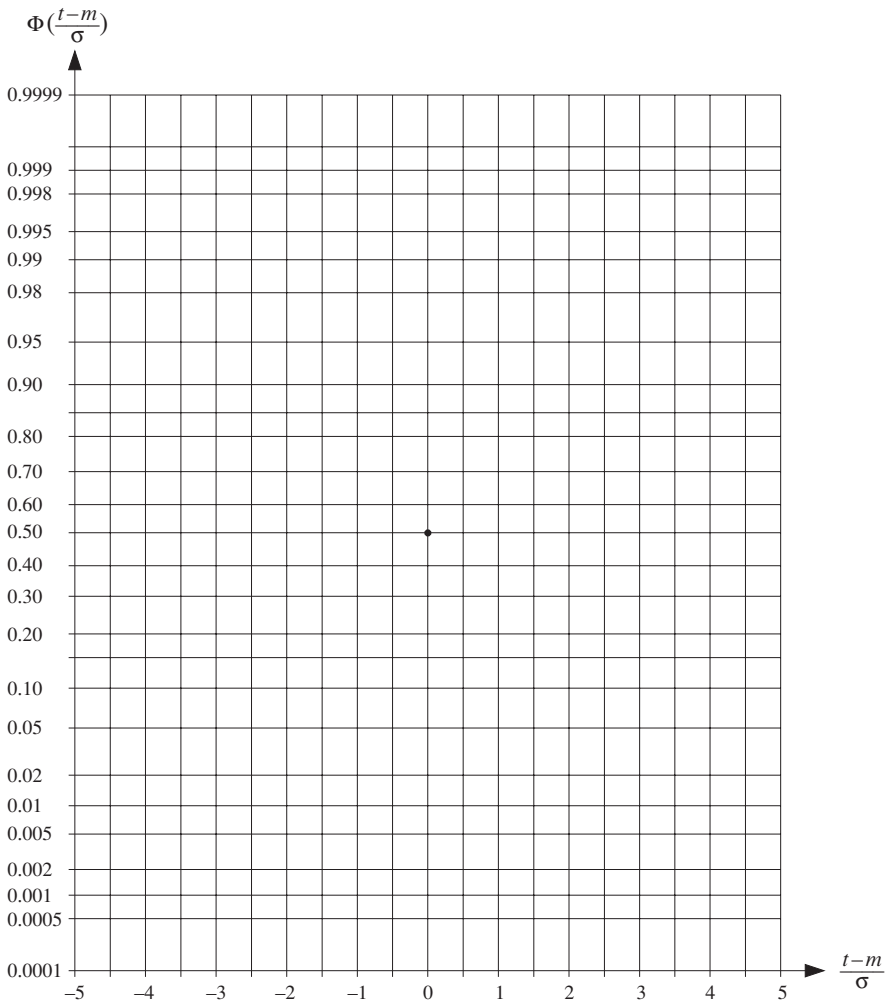


Figure A9.3 Normal probability chart (standard normal distribution)

A10 Basic Technological Component's Properties

Table A10.1 gives some basic technological properties of electronic components to support reliability evaluations (see also Chapters 3 & 5, and e.g. [3.1, 3.10, 3.23, 3.58]).

Table A10.1 Basic technological properties of electronic components

Component	Technology, Characteristics	Sensitive to	Application
Fixed resistors			
• Carbon film	A layer of carbon film deposited at high temperature on ceramic rods; $\pm 5\%$ usual; medium TC; relatively low drift (-1 to $+4\%$); failure modes: opens, drift, rarely shorts; elevated noise; 1Ω to $22 \text{ M}\Omega$; low λ (0.2 to 0.4 FIT)	Load, temperature, overvoltage, freq. ($> 50 \text{ MHz}$), moisture	Low power ($\leq 1 \text{ W}$), moderate temperature ($< 85^\circ \text{C}$) and frequency ($\leq 50 \text{ MHz}$)
• Metal film	Evaporated NiCr film deposited on aluminum oxide ceramic; $\pm 5\%$ usual; low TC; low drift ($\pm 1\%$); failure modes: drift, opens, rarely shorts; low noise; 10Ω to $2.4 \text{ M}\Omega$; low λ (0.2 FIT)	Load, temperature, current peaks, ESD, moisture	Low power ($\leq 0.5 \text{ W}$), high accuracy and stability, high freq. ($\leq 500 \text{ MHz}$)
• Wire-wound	Usually NiCr wire wound on glass fiber substrate (sometimes ceramic); precision ($\pm 0.1\%$) or power ($\pm 5\%$); low TC; failure modes: opens, rarely shorts between adjacent windings; low noise; 0.1Ω to $250 \text{ k}\Omega$; medium λ (2 to 4 FIT)	Load, temperature, overvoltage, mechanical stress (wire $< 25 \mu\text{m}$), moisture	High power, high stability, low frequency ($\leq 20 \text{ kHz}$)
• Thermistors (PTC, NTC)	PTC: Ceramic materials (BaTiO_3 or SrTiO_3 with metal salts) sintered at high temperatures, showing strong increase of resistance (10^3 to 10^4) within 50°C ; medium λ (4 to 10 FIT, large values for disk and rod packages) NTC: Rods pressed from metal oxides and sintered at high temperature, large neg. TC ($\text{TC} \sim -1/T^2$); failure rate as for PTC	Current and voltage load, moisture	PTC: Temperature sensor, overload protection, etc. NTC: Compensation, control, regulation, stabilization
Variable resist.			
• Cermet Pot., Cermet Trim	Metallic glazing (often ruthenium oxide) deposited as a thick film on ceramic rods and fired at about 800°C ; usually $\pm 10\%$; poor linearity (5%); medium TC; failure modes: opens, localized wear-out, drift; relatively high noise (increases with age); 20Ω - $2 \text{ M}\Omega$; low to medium λ (5-20 FIT)	Load, current, fritting voltage ($< 1.5 \text{ V}$), temperature, vibration,	Should only be employed when there is a need for adjustment during operation, fixed resistors have to be preferred for calibration during testing; load capability proportional to the part of the resistor used
• Wirewound Pot.	CuNi / NiCr wire wound on ceramic rings or cylinders (spindle-operated potentiom.); normally $\pm 10\%$; good linearity (1%); precision or power; low, nonlinear TC; low drift; failure modes: opens, localized wear-out, relatively low noise; 10Ω to $50 \text{ k}\Omega$; medium to large λ (10 to 100 FIT)	noise, dust, moisture, frequency (wire)	

Table A10.1 (cont.)

Component	Technology, Characteristics	Sensitive to	Application
<p>Capacitors</p> <ul style="list-style-type: none"> Plastic (KS, KP, KT, KC) 	Wound capacitors with plastic film (K) of polystyrene (S), polypropylene (P), polyethylene-terephthalate (T) or polycarbonate (C) as dielectric and Al foil; very low loss factor (S, P, C); failure modes: opens, shorts, drift; pF to μ F; low λ (1 to 3 FIT)	Voltage stress, pulse stress (T, C), temperature (S, P), moisture* (S, P), cleaning agents (S)	Tight capacitance tolerances, high stability (S, P), low loss (S, P), well-defined temperature coefficient
<ul style="list-style-type: none"> Metallized plastic (MKP, MKT, MKC, MKU) 	Wound capacitors with metallized film (MK) of polypropylene (P), polyethylene-terephthalate (T), polycarbonate (C) or cellulose acetate (U); self-healing; low loss factor; failure modes: opens, shorts; nF to μ F; low λ (1 to 2 FIT)	Voltage stress, frequency (T, C, U), temperature (P), moisture* (P, U)	High capacitance values, low loss, relatively low frequencies (< 20 kHz for T, U)
<ul style="list-style-type: none"> Metallized paper (MP, MKV) 	Wound capacitors with metallized paper (MP) and in addition polypropylene film as dielectric (MKV); self-healing; low loss factor; failure modes: shorts, opens, drift; 0.1 μ F to mF; low λ (1 to 3 FIT)	Voltage stress and temperature (MP), moisture*	Coupling, smoothing, blocking (MP), oscillator circuits, commutation, attenuation (MKV)
<ul style="list-style-type: none"> Ceramic 	Often manufactured as multilayer capacitors with metallized ceramic layers by sintering at high temperature with controlled firing process (class 1: $\epsilon_r < 200$, class 2: $\epsilon_r \geq 200$); very low loss factor (class 1); temperature compensation (class 1); high resonance frequency; failure modes: shorts, drift, opens; pF to μ F; low λ (0.5 to 2 FIT)	Voltage stress, temperature (even during soldering) moisture*, aging at high temperature (class 2)	Class 1: high stability, low loss, low aging; class 2: coupling, smoothing, buffering, etc.
<ul style="list-style-type: none"> Tantalum (solid, dry) 	Manufactured from a porous, oxidized cylinder (sintered tantalum powder) as anode, with manganese dioxide as electrolyte and a metal case as cathode; polarized; medium frequency-dependent loss factor; failure modes: shorts, opens, drift; 0.1 μ F to mF; low to medium λ (1 to 5 FIT, 20 to 40 FIT for bead)	Incorrect polarity, voltage stress, AC resistance (Z_0) of the el. circuit (new types less sensitive), temperature, frequency (>1kHz), moisture*	Relatively high capacitance per unit volume, high requirements with respect to reliability, $Z_0 \geq 1 \Omega/V$
<ul style="list-style-type: none"> Aluminum (wet) 	Wound capacitors with oxidized Al foil (anode and dielectric) and conducting electrolyte (cathode); also available with two formed foils (nonpolarized); large, frequency and temperature dependent loss factor; failure modes: drift, shorts, opens; μ F to 200 mF; medium to large λ (5 to 10 FIT); limited useful life (function of temperature and ripple)	Incorrect polarity (if polarized), voltage stress, temperature, cleaning agent (halogen), storage time, frequency (> 1 kHz), moisture*	Very high capacitance per unit volume, uncritical applications with respect to stability, relatively low ambient temperature (0 to 55°C)

Table A10.1 (cont.)

Component	Technology, Characteristics	Sensitive to	Application
Diodes (Si)			
• General purpose	PN junction produced from high purity Si by diffusion; diode function based on the recombination of minority carriers in the depletion regions; failure modes: shorts, opens; low λ (1 to 3 FIT, $\theta_J = 40^\circ\text{C}$, 10 FIT for rectifiers with $\theta_J = 100^\circ\text{C}$)	Forward current, reverse voltage, temperature, transients, moisture*	Signal diodes (analog, switch), rectifier, fast switching diodes (Schottky, avalanche)
• Zener	Heavily doped PN junction (charge carrier generation in strong electric field and rapid increase of the reverse current at low reverse voltages); failure modes: shorts, opens, drift; low to medium λ (2 to 4 FIT for voltage regulators ($\theta_J = 40^\circ\text{C}$), 20 to 50 FIT for voltage ref. ($\theta_J = 100^\circ\text{C}$))	Load, temperature, moisture*	Level control, voltage reference (allow for $\pm 5\%$ drift)
Transistors			
• Bipolar	PNP or NPN junctions manufactured using planar technology (diffusion or ion implantation); failure modes: shorts, opens, thermal fatigue for power trans.; transistor function based on minority carrier transport; low to medium λ (2 to 6 FIT for $\theta_J = 40^\circ\text{C}$, 20 to 60 FIT for power transistors and $\theta_J = 100^\circ\text{C}$)	Load, temperature, breakdown voltage (V _{CEO} , V _{BEBO}), moisture*	Switch, amplifier, power stage (allow for $\pm 20\%$ drift, $\pm 500\%$ for ICBO)
• FET	Voltage controlled semicond. resistance, with control via diode (JFET) or isolated layer (MOSFET); transist. function based on majority carrier transport; N or P channel; depletion or enhancement type (MOSFET); failure modes: shorts, opens, drift; medium λ (3 to 10 FIT for $\theta_J = 40^\circ\text{C}$, 30 to 60 FIT for power transistors and $\theta_J = 100^\circ\text{C}$)	Load, temperature, breakdown voltage, ESD, radiation, moisture*	Switch (MOS) and amplifier (JFET) for high-resistance circuits (allow for $\pm 20\%$ drift)
Controlled rectifiers (Thyristors, triacs, etc.)	NPNP junctions with lightly doped inner zones (P, N), which can be triggered by a control pulse (thyristor), or a special antiparallel circuit consisting of two thyristors with a single firing circuit (triac); failure modes: drift, shorts, opens; large λ (20 to 100 FIT for $\theta_J = 100^\circ\text{C}$)	Temperature, reverse voltage, rise rate of voltage and current, commutation effects, moisture*	Controlled rectifier, overvoltage and overcurrent protection (allow for $\pm 20\%$ drift)
Opto-semiconductors (LED, IRED, photo-sensitive devices, optocouplers, etc.)	Electrical/optical or optical/electrical converter made with photosensitive semiconductor components; transmitter (LED, IRED, laser diode etc.), receiver (photo-resistor, photo-transistor, solar cells etc.), optocoupler, displays; failure modes: opens, drift, shorts; medium to large λ (2 to 100 FIT, $20\sqrt{\text{no. of pixels}}$ for LCD); limited useful life	Temperature, current, ESD, moisture*, mechanical stress	Displays, sensors, galvanic separation, noise rejection (allow for $\pm 30\%$ drift)

Table A10.1 (cont.)

Component	Technology, Characteristics	Sensitive to	Application
Digital ICs • Bipolar	Monolithic ICs with bipolar transistors (TTL, ECL, I^2L), important AS TTL (6 mW, 2 ns, 1.3 V) and ALS TTL (1 mW, 3 ns, 1.8 V); $V_{CC} = 4.5 - 5.5$ V; $Z_{out} < 150 \Omega$ for both states; low to medium λ (2 to 6 FIT for SSI/MSI, 20 to 100 FIT for LSI/VLSI)	Supply voltage, noise (> 1 V), temperature (0.5 eV), ESD, rise and fall times, breakdown BE diode, moisture*	Fast logic (LS TTL ECL) with uncritical power consump., rel. high cap. loading, $\theta_J < 175^\circ\text{C}$ ($< 200^\circ\text{C}$ for SOI)
• MOS	Monolithic ICs with MOS transistors, mainly N channel depletion type (formerly also P channel); often TTL compatible and therefore $V_{DD} = 4.5 - 5.5$ V (100 μ W, 10 ns); very high Z_{in} ; medium Z_{out} (1 to 10 k Ω); medium to high λ (50 to 200 FIT)	ESD, noise (> 2 V), temperature (0.4 eV), rise and fall times, radiation, moisture*	Memories and microprocessors high source impedance, low capacitive loading
• CMOS	Monolithic ICs with complementary enhancement-type MOS transistors; often TTL compatible and therefore $V_{DD} = 4.5 - 5.5$ V; power consumption $\sim f$ (10 μ W at 10 kHz, $V_{DD} = 5.5$ V, $C_L = 15$ pF); fast CMOS (HCMOS, HCT) for 2 to 6 V with 6 ns at 5 V and 20 μ W at 10 kHz: large static noise immunity ($0.4 V_{DD}$); very high Z_{in} ; medium Z_{out} (0.5 to 5 k Ω); low to medium λ (2 to 6 FIT for SSI/MSI, 10 to 100 FIT for LSI/VLSI)	ESD, latch-up, temperature (0.4 eV), rise and fall times, noise ($> 0.4 V_{DD}$), moisture*	Low power consumption, high noise immunity, not extremely high frequency, high source impedance, low cap. load, $\theta_J < 175^\circ\text{C}$, for memories: $< 125^\circ\text{C}$
• BiCMOS	Monolithic ICs with bipolar and CMOS devices; trend to less than 2 V supplies; combine the advantages of both bipolar and CMOS technologies	similar to CMOS	similar to CMOS but also for very high frequencies
Analog ICs • Operational amplifiers, comparators, voltage regulators, etc.	Monolithic ICs with bipolar and/or FET transistors for processing analog signals (operational amplifiers, special amplifiers, comparators, voltage regulators, etc.); up to about 200 transistors; often in metal packages; medium to high λ (10-50 FIT)	Temperature (0.6 eV), input voltage, load current, moisture*	Signal processing, voltage reg., low to medium power consump. (allow for $\pm 20\%$ drift), $\theta_J < 175^\circ\text{C}$ (< 125 for low power)
Hybrid ICs • Thick film, thin film	Combination of chip components (ICs, transistors, diodes, capacitors) on a thick film 5–20 μ m or thin film 0.2–0.4 μ m substrate with deposited resistors and connections; substrate area up to 10 cm ² ; medium to high λ (usually determined by the chip components)	Manufacturing quality, temperature, mechanical stress, moisture*	Compact and reliable devices e. g. for avionics or automotive (allow for $\pm 20\%$ drift)

ESD = electrostatic discharge; TC = temperature coefficient; λ in 10^{-9} h^{-1} , indicative values for standard industrial environment ($\theta_A = 40^\circ\text{C}$, G_B); failure modes given in decreasing probability of occurrence (see also Table 3.4); * nonhermetic packages

A11 Problems for Homework

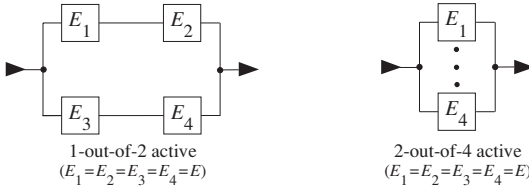
In addition to the 140 Examples, the following are 70 selected problems for homework, ordered for Chapters 2, 4, 6, 7, A6, A7, A8 (* means can be time-consuming).

Problem 2.1

Draw the reliability block diagram corresponding to the fault tree given by Fig. 6.40b (p. 282).

Problem 2.2

Compare the mean time to failure $MTTF_S$ and reliability function $R_S(t)$ of the following reliability block diagrams for the case nonrepairable and constant failure rate λ for elements E_1, \dots, E_4 .



Problem 2.3

Compare the mean time to failure $MTTF_S$ for cases 7 and 8 of Table 2.1 (p. 31) for $E_1 = \dots = E_5 = E$ and constant failure rates $\lambda_1 = \dots = \lambda_5 = \lambda$.

Problem 2.4

Compute the reliability function $R_S(t)$ for case 4 of Table 2.1 (p. 31) for $n=3, k=2, E_1 \neq E_2 \neq E_3$.

Problem 2.5

Investigate $R_{S0}(t)$ for $t \ll 1/\lambda$ for different k -out-of- n active redundancies (Fig. 2.7 on p. 44).

Problem 2.6*

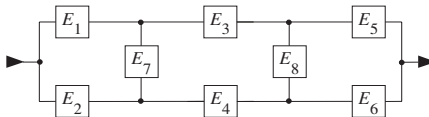
Give a realization for the circuit to detect the occurrence of the second failure in a majority redundancy 2-out-of-3 (Example 2.5, p. 49), allowing an expansion of a 2-out-of-3 to a 1-out-of-3 redundancy. (Hint: Isolate the first failure and detect the occurrence of the second failure using e.g. 6 two-input AND, 3 two-input EXOR, 1 three-input OR, and adding a delay δ for an output pulse of width δ .)

Problem 2.7*

Demonstrate the result given by Eq. (2.62) and apply this to the active redundancy.

Problem 2.8*

Compute the reliability function $R_S(t)$ for the Π circuit with bi-directional connections given below,



(Hint: Use the key item method (Eq. (2.29)) on E_7 & E_8).

Problem 2.9*

Problem 2.8 using the minimal path set or cut set method (Section 2.3.4), compare computation times.

Problem 2.10*

Prove Eq. (2.73).

Problem 2.11*

Investigate practically applicable truncation possibilities for stress and/or strength distributions.

Problem 4.1

Compute the $MTTR_S$ for the structure of case 5 in Table 2.1 on p. 31, assumed repairable with $\lambda_1 = 10^{-3} \text{ h}^{-1}$, $\lambda_2 = 10^{-4} \text{ h}^{-1}$, $\lambda_3 = 10^{-2} \text{ h}^{-1}$, $\lambda_4 = 10^{-3} \text{ h}^{-1}$, $\lambda_5 = 10^{-2} \text{ h}^{-1}$, $\lambda_6 = 10^{-4} \text{ h}^{-1}$, $\lambda_7 = 10^{-5} \text{ h}^{-1}$, and $\mu_1 = \mu_4 = 0.5 \text{ h}^{-1}$, $\mu_3 = \mu_5 = 0.2 \text{ h}^{-1}$, $\mu_2 = \mu_6 = 1 \text{ h}^{-1}$, $\mu_7 = 2 \text{ h}^{-1}$. Compare the obtained $MTTR_S$ with the mean down time at system level MDT_S per Eq. (6.295). (Hint: consider Example 4.2, use Table 6.10 to compute $MTTF_{S0}$ & PA_S , and assume $MUT_S = MTTF_{S0}$.)

Problem 4.2

Give the number of spare parts necessary to cover with a probability $\gamma \geq 0.9$ an operating time of 50,000h for the system given by case 6 of Table 2.1 (p.31) for $\lambda_1 = \lambda_2 = \lambda_3 = 10^{-3} \text{ h}^{-1}$, $\lambda_v = 10^{-5} \text{ h}^{-1}$. (Hint: Assume equal allocation of γ between E_v and the 2-out-of-3 active redundancy.)

Problem 4.3

Same as for Problem 4.2 by assuming that spare parts are repairable with $\mu_1 = \mu_2 = \mu_3 = \mu_v = 0.5 \text{ h}^{-1}$. (Hint: consider only the case with $R_{S0}(t)$ and assume equal allocation of γ between E_v and the 2-out-of-3 active redundancy.)

Problem 4.4

Give the number of spare parts necessary to cover with a probability $\gamma \geq 0.9$ an operating time of 50,000h for an item with Erlangian distributed failure-free times with $\lambda = 10^{-3} \text{ h}^{-1}$ and $n = 3$. (Hint: Consider Appendix A6.10.3.)

Problem 4.5

Develop the expression allowing the computation of the number of spare parts necessary to cover with a probability $\geq \gamma$ an operating time T for an item with failure-free times distributed according to a Gamma distribution. (Hint: Consider Appendix A6.10.3, and Table A9.7b.)

Problem 4.6*

Give the number of spare parts necessary to cover with a probability $\gamma \geq 0.9$ an operating time of 50,000h for a 1-out-of-2 standby redundancy with constant failure rate $\lambda = 10^{-3} \text{ h}^{-1}$ for the operating element ($\lambda \equiv 0$ for the reserve element). Compare the results with those obtained for an active 1-out-of-2 redundancy with failure rate $\lambda = 10^{-3} \text{ h}^{-1}$ for the active and the reserve element.

Problem 4.7*

A series-system consists of operationally independent elements E_1, \dots, E_n with constant failure rates $\lambda_1, \dots, \lambda_n$. Let c_i be the cost for a repair of element E_i . Give the mean (expected value) of the repair cost for the whole system during a total operating time T for all elements. (Hint: Consider Appendix A7.2.5 and assume negligible repair (renewal) times.)

Problem 4.8*

An item has a constant failure rate λ and a constant repair rate μ . Compute the mean of the repair cost during a total operating time T_0 given the fixed cost c_0 for each repair. Assuming that down time for repair has a cost c_d per hour, compute the mean value of the total cost for repair and down time during a total operating time T_0 . (Hint: Consider Appendices A7.2.5 and A7.8.4.)

Problem 4.9*

Prove that for the case of constant failure rate $\lambda(x) = \lambda$ and negligible repair (renewal) times, the optimal repair strategy is repair at failure.

Problem 4.10*

Investigate the comparison between age and block replacement (Section 4.6.1).

Problem 4.11*

Investigate the practical applicability of the concept as-bad-as-old. (Hint: consider Appendix A7.8.2.)

Problem 6.1

Compare the mean time to failure $MTTF_{S0}$ and the asymptotic & steady-state point and average availability $PA_S = AA_S$ for the two reliability block diagrams of Problem 2.2, by assuming constant failure rate λ and constant repair rate μ for each element and only one repair crew. (Hint: Use the results of Table 6.10.)

Problem 6.2

Give the asymptotic & steady-state point and average availability $PA_S = AA_S$ for the bridge given by Fig. 2.10, p. 53, by assuming identical and independent elements (each element has its own repair crew) with constant failure rate λ and constant repair rate μ . (Hint: Use results of Section 2.3.4.)

Problem 6.3

Develop Eqs. (6.32) & (6.33) and discuss (prove) the remarks to Eq. (6.33).

Problem 6.4

investigate the structure of Fig. 6.15 (p. 221) by assuming that E_V is a main equipment controlled by E_1 and E_2 in which E_2 is an operator in standby redundancy, active only at a failure of E_1 ($\mu_2 \gg \mu_1 \gg \mu_V \gg \lambda_1, \lambda_2, \lambda_3$, no further failure at system down, 3 repair crews available).

Problem 6.5

For the 1-out-of-2 warm redundancy of Fig. 6.8 (p. 197) show that $\sum P_i MTTF_{Si} = P_0 MTTF_{S0} + P_1 MTTF_{S1}$ differs from MUT_S . (Hint: Consider Appendix A7.5.4.1.)

Problem 6.6*

Give the mean time to failure $MTTF_{S0}$ and the asymptotic & steady-state point and average availability $PA_S = AA_S$ for the reliability block diagram given by case 5 of Table 2.1 (p. 31) by assuming constant failure rates $\lambda_1, \dots, \lambda_7$ and constant repair rates μ_1, \dots, μ_7 : (i) For independent elements (Table 6.9); (ii) Using results for macro-structures (Table 6.10); (iii) Using a Markov model with only one repair crew, repair priority on elements E_6 and E_7 , and no further failure at system down. Compare results by means of numerical examples. (Hint: For (iii), consider Point 2 of Section 6.8.9 and Eqs (6.157) & (6.159).)

Problem 6.7*

Prove the results in Point 5 of Table 6.3 (p. 183), theoretically, from Eq. (6.37), and just by considering the memoryless property given by a constant (time independent) failure rate $\lambda(x) = \lambda$.

Problem 6.8*

Give the asymptotic & steady-state point and average availability $PA_S = AA_S$ for the Π circuit of Problem 2.8, by assuming identical and independent elements with constant failure rate λ and constant repair rate μ , each element has its own repair crew. (Hint: Use results of Section 2.3.4.)

Problem 6.9*

For the 1-out-of-2 warm redundancy given by Fig. 6.8 (p. 197) compute for states Z_0, Z_1, Z_2 : (i) The states probabilities P_0, P_1, P_2 of the embedded Markov chain; (ii) The steady-state probabilities P_0, P_1, P_2 ; (iii) The mean stay (sojourn) times T_0, T_1, T_2 ; (iv) The mean recurrence times T_{00}, T_{11}, T_{22} . (Hint: Consider Appendices A7.5.3.3, A7.5.4.1, and A7.6.)

Problem 6.10*

Prove Eqs. (6.130) and (6.131).

Problem 6.11*

Prove Eqs. (6.166) and (6.168).

Problem 6.12*

Prove the conclusions as per Eqs. (6.207) & (6.212), i. e. prove Eqs. (6.206), (6.209), (6.211), and (6.214).

Problem 7.1

For an incoming inspection one has to demonstrate a defective probability $p = 0.01$. An $AQL = 0.01$ with producer risk $\alpha = 0.1$ is agreed. Give the sample size n for a number of acceptable defectives $c = 0, 1, 2, 5, 10$. Compute the consumer risk β for the corresponding values of c . (Hint: Use Fig. 7.3.)

Problem 7.2

For the demonstration of an $MTBF = 1/\lambda = 4'000\text{h}$ one agrees with the producer the following rule: $MTBF_0 = 4'000\text{h}$, $MTBF_1 = 2'000\text{h}$, $\alpha = \beta = 0.2$. Give the cumulative test time T and the number c of allowed failures. How large would the acceptance probability be for a true $MTBF$ of $5'000\text{h}$ and of $1'500\text{h}$, respectively? (Hint: Use Table 7.3 and Fig. 7.3.)

Problem 7.3

For the demonstration of an $MTTR$ one agrees with the producer the following rule: $MTTR_0 = 1\text{h}$, $MTTR_1 = 1.5\text{h}$, $\alpha = \beta = 0.2$. Assuming a lognormal distribution for the repair times with $\sigma^2 = 0.2$, give the number of repair and the allowed cumulative repair time. Draw the operating characteristic curve as a function of the true $MTTR$. (Hint: Use results of Section 7.3.2.)

Problem 7.4

During an accelerated reliability test at $\theta_J = 125^\circ\text{C}$, 3 failures have occurred within the cumulative test time of $100'000\text{h}$ (failed devices have been replaced). Assuming an activation energy $E_a = 0.5\text{eV}$, give for a constant failure rate λ the maximum likelihood point estimate and the confidence limits at the confidence levels $\gamma = 0.8$ and $\gamma = 0.2$ for $\theta_J = 35^\circ\text{C}$. How large is the upper confidence limit at the confidence levels $\gamma = 0.9$ and $\gamma = 0.6$? (Hint: Use Eq. (7.56) & Fig. 7.6.)

Problem 7.5

For the demonstration of an $MTBF = 1/\lambda = 10'000\text{h}$ one agrees with the producer the following rule: $MTBF = 10'000\text{h}$, acceptance risk 20%. Give the cumulative test time T for a number of allowed failures $c = 0, 1, 2, 6$ by assuming that the acceptance risk is: (i) The producer risk α (AQL case); (ii) The consumer risk β ($LTPD$ case). (Hint: Use Fig. 7.3.)

Problem 7.6

Compare the amount of time necessary to test with $c=1$ $MTBF = 1/\lambda > 500\text{h}$ against $MTBF < 500\text{h}$ with: (i) $\alpha=0.1$ ($\beta=0.9$) and (ii) $\beta=0.1$ ($\alpha=0.9$). For which values of true $MTBF$, producer and consumer have the same risk (0.5) to make a false decision in cases (i) and (ii)? (Hint: Use Fig. 7.3.)

Problem 7.7

For a reliability test of a nonrepairable item, the following 20 failure-free times have been observed 300, 580, 700, 900, 1'300, 1'500, 1'800, 2'000, 2'200, 3'000, 3'300, 3'800, 4'200, 4'600, 4'800, 5'000, 6'400, 8'000, 9'100, 9'800h. Assuming a Weibull distribution, plot the values on a Weibull probability chart (p. 570) and determine graphically the parameters λ & β . Compute the maximum likelihood estimates for λ & β and draw the corresponding straight line. Draw the random band obtained using the Kolmogorov theorem (p. 530) for $\alpha = 0.2$. It is possible to affirm that the observed distribution function belongs to the Weibull family? (Hint: Use results of Section 7.5.1.)

Problem 7.8*

Prove the statements given in the footnote ⁺⁺) on p. 330.

Problem 7.9*

Prove the procedures given in Sections 7.6.3.1 & 7.6.3.2 (Eqs.(7.86), (7.87), (7.90), (7.91), (7.93-96)).

Problem 7.10*

For a repairable electromechanical system, the following arrival times t_i^* of successive failures have been observed during $T = 3'000\text{h}$: 450, 800, 1'400, 1'700, 1'950, 2'150, 2'450, 2'600, 2'850, 2'950h. Test the hypothesis H_0 : the underlying point process is an HPP, against H_1 : the underlying process is an NHPP with increasing density. Fit a possible $M(t)$. (Hint: Use results of Section 7.6.3.)

Problem A6.1

Devices are delivered from source A with probability p and B with probability $1-p$. Devices from source A have constant failure rate λ_A , those from source B have early failures and their failure-free time is Gamma distributed (Eq. (A6.97)) with parameters λ_B and $\beta < 1$. The devices are mixed. Give the resulting distribution of the failure-free time and the *MTTF* for a device randomly selected.

Problem A6.2

Show that only the exponential distribution (Eq. (A6.81)), in continuous time, and the geometric distribution (Eq. (A6.131)), in discrete time, possess the memoryless property. (Hint: Use Eq. (A6.27) and the considerations in Appendices A6.5 and A7.2.)

Problem A6.3

Show that the failure-free time of a series-system with independent elements E_1, \dots, E_n , each with Weibull distributed failure-free times with parameters λ_i and β , is distributed according to a Weibull distribution with parameters λ_S and β , give λ_S . (Hint: Consider Appendix A6.10.2.)

Problem A6.4

Show that the probability to have exactly k failures in the operating time T of a system with constant failure rate λ , repaired as-good-as-new at each failure, is given by $(\lambda T)^k e^{-\lambda T} / k!$

Problem A6.5

Prove cases (i), (iii), and (v) given in Example A6. 18 (p. 448).

Problem A6.6*

Show that the sum of independent random variables having a common exponential distribution are Erlangian distributed. Same for Gamma distributed random variables, giving a Gamma distribution. Same for normal distributed random variables, giving a normal distribution.

Problem A6.7*

Show that the square of a standard normal distributed random variable (Eq.(A6.109)) is χ^2 distributed with $\nu=1$. (Hint: Use $f_{\eta}(t)$ per Eq. (A6.31), $u(t)=t^2$, & consider $-\infty < \tau < \infty$ & $0 < \eta = \tau^2 < \infty$.)

Problem A6.8*

Show that mean & variance of a lognormally distributed random variable are given by Eqs.(A6.112), (A6.113). (Hint: Use $x = (\ln \lambda t) / \sigma\sqrt{2}$ and then $y = x - \sigma/\sqrt{2}$ for mean, $y = x + \sigma/\sqrt{2}$ for variance.)

Problem A7.1

Prove that for a homogeneous Poisson process with parameter λ , the probability to have k events (failures) in $(0, T]$ is Poisson distributed with parameter λT .

Problem A7.2

Determine graphically from Fig. A7.2 (p. 468) the mean time to failure of the item considered in Case V of Example A7.1. (Hint: Use Eq. (A7.30).) Compare this result with that obtained for Case V with $\lambda_w = 0$, i. e., as if no early failures were present. Same for Case IV, and compare the result with that obtained for Case IV with $\psi \rightarrow \infty$, i. e., as if the wear-out period would never occur.

Problem A7.3

Prove Eq.(A7.33) for the mean of the forward recurrence time $\tau_R(t)$ in a renewal process for $t \rightarrow \infty$. Show that for a homogeneous Poisson process it holds that the mean of $\tau_R(t)$ is independent of t and equal the mean of the successive interarrival times $(1/\lambda)$. Explain the waiting time paradox (p. 470).

Problem A7.4

Prove Equation (5.3) and give an explication for the validity of Eq. (5.4). (Hint: use results of Section 2.3.5 with $v_i = (n-i)\lambda$, $i=0, 1, \dots, n-1$, and, for Eq. (5.4), consider a series model with $E_1 = \dots = E_n$.

Problem A7.5

Prove that for a nonhomogeneous Poisson process with intensity $m(t) = dM(t)/dt$, the probability to have k events (failures) in the interval $(0, T]$ is Poisson distributed with parameter $M(T) - M(0)$.

Problem A7.6

Investigate the cumulative damage caused by Poisson distributed shocks with intensity λ , each of which causes a damage $\xi > 0$ exponentially distributed with parameter $\eta > 0$, independent of the shock and of the cumulated damage. (Hint: Consider Appendix A7.8.4.)

Problem A7.7

Investigate the renewal densities $h_{ud}(t)$ and $h_{du}(t)$ (Eqs. (A7.52), (A7.53)) for the case of constant failure and repair (restoration) rates λ and μ . Show that they converge exponentially for $t \rightarrow \infty$ with a time constant $1/(\lambda + \mu) \approx 1/\mu$ toward their final value $\lambda\mu/(\lambda + \mu) \approx \lambda$. (Hint: Use Table A9.7b.)

Problem A7.8

Let $0 < \tau_1^* < \tau_2^* < \dots$ be the occurrence times (failure times of a repairable system) of a non-homogeneous Poisson process with intensity $m(t) = dM(t)/dt > 0$ (from the origin $t = \tau_0^* = 0$), show that the quantities $\Psi_1^* = M(\tau_1^*) < \Psi_2^* = M(\tau_2^*) < \dots$ are the occurrence times in a homog. Poisson process with intensity one, i.e with $M(t) = t$. (Hint: Consider the remarks to Eq. (A7.200).)

Problem A7.9

Let $\tau_1^* < \dots < \tau_n^* < T$ be the failure times (arrival times) in the interval $(0, T]$ of a repairable system. Assuming a nonhomogeneous Poisson process with intensity $m(t) = dM(t)/dt > 0$, show that (for given T and $v(T) = n$), the quantities $0 < M(\tau_1^*)/M(T) < \dots < M(\tau_n^*)/M(T) < 1$ have the same distribution as if they were the order statistics of n independent identically distributed random variables uniformly distributed on $(0, 1)$. (Hint: Consider the remarks to Eq. (A7.206).)

Problem A7.10*

Using Eqs. (A7.186), (A7.187), (A7.171), (A7.173), prove for $g(x) = \mu e^{-\mu x}$ results in Tab. 6.8 ($n-k=2$).

Problem A7.11*

Prove Eq. (A7.220). (Hint: use Eqs. (A6.38) and (A6.45).)

Problem A8.1

Prove Eqs. (A8.10) and (A8.11).

Problem A8.2

Give the maximum likelihood point estimate for the parameters λ and β of a Gamma distribution (Eq. (A6.97)) and for m and σ of a normal distribution (Eq. (A6.105)).

Problem A8.3*

Investigate mean and variance of the point estimate $\hat{\lambda} = k/T$ given by Eq. (7.28).

Problem A8.4*

Investigate mean and variance of the point estimate $\hat{\lambda} = (k-1)/(t_1 + \dots + t_k + (n-k)t_k)$ given by Eq. (A8.35). Same for $\hat{\lambda} = n/(t_1 + \dots + t_n)$ given by Eq. (A8.28).

Problem A8.5*

Prove Eq. (A8.32). (Hint: use Eq. (A8.27).)

Problem A8.6*

Prove Eq. (A8.62). (Hint: use Eqs. (A8.61) & (A8.24).)

Problem A8.7*

Develop the procedure (Eqs. (A8.91) - (A8.93)) for the demonstration of an availability PA for the case of constant failure rate and Erlangian distributed repair times with parameter $\beta_\mu = n_\mu$.

Acronyms

(see also the Index)

ACM	: Association for Computing Machinery, New York, NY 10036
AFCIQ	: Association Française pour le Contrôle Industriel de la Qualité, F-92080 Paris
ANSI	: American National Standards Institute, New York, NY 10036
AQAP	: Allied Quality Assurance Publications (NATO-Countries)
ASQ	: American Society for Quality, Milwaukee, WI 53203
CECC	: Cenelec Electronic Components Committee, B-1050 Brussels
CEEES	: Confederation of European Environmental Engineering Societies (www.cee.es.org/)
CENELEC	: European Committee for Electrotechnical Standardization, B-1050 Brussels
CNET	: Centre National d'Etudes des Telecommunications, F-22301 Lannion
DGQ	: Deutsche Gesellschaft für Qualität, D-60549 Frankfurt a. M.
DIN	: Deutsches Institut für Normung, D-14129 Berlin 30
DOD	: Department of Defense, Washington, D.C. 20301
EOQC	: European Organization for Quality Control, B-1000 Brussels
EOS/ESD	: Electrical Overstress/Electrostatic Discharge
ESA	: European Space Agency, NL-2200 AG Noordwijk
ESREF	: European Symp. on Rel. of Electron. Devices, Failure Physics and Analysis
ETH	: Swiss Federal Institute of Technology, CH-8092 Zurich
EXACT	: Int. Exchange of Authentic. Electronic Comp. Perf. Test Data, London, NW4 4AP
FRACAS	: Failure Reporting and Corrective Actions System
GEIA	: Government Electronics and Information Association, Ann Arbor, MI 48108
GIDEP	: Government-Industry Data Exchange Program, Corona, CA 91720
GPO	: Government Printing Office, Washington, D.C. 20402
GRD	: Gruppe Rüstung, CH-3000 Bern 25
IEC (CEI)	: International Electrotechnical Commission, CH-1211 Geneva 20, P.. Box131
IECEE	: IEC System for Conformity Testing & Certif. of Electrical Equip., CH-1211 Geneva20
IECQ	: IEC Quality Assessment System for Electronic Components, CH-1211 Geneva 20
IEEE	: Institute of Electrical and Electronics Engineers, Piscataway, NJ 08855-0459
IES	: Institute of Environmental Sciences, Mount Prospect, IL 60056
IPC	: Institute for Interconnecting and Packaging El. Circuits, Lincolnwood, IL 60646
IRPS	: International Reliability Physics Symposium (IEEE), USA
ISO	: International Organization for Standardization, CH-1211 Geneva 20, P.. Box56
MIL-STD	: Military (USA) Standard, Standardiz. Doc. Order Desk, Philadelphia, PA19111-5094
NASA	: National Aeronautics and Space Administration, Washington, D.C. 20546
NTIS	: National Technical Information Service, Springfield, VA 22161-2171
NUREG	: US. Nuclear Regulatory Commission, Washington DC 20555-0001
RAC	: Reliability Analysis Center, Rome, NY 13442-4700 (now RIAC)
RAMS	: Reliability, Availability, Maintainability, Safety (also Rel. & Maint. Symp., IEEE)
RIAC	: Reliability Information Analysis Center, Utica, NY 13502-1348 (formerly. RAC)
Rel. Lab.	: Reliability Laboratory at the ETH (now at EMPA S173, CH-8600 Dübendorf)
RL	: Rome Laboratory, Griffins AFB, NY 13441-4505
SAQ	: Schweizerische Arbeitsgemeinschaft für Qualitätsförderung, CH-4600 Olten
SEV	: Schweizerischer Elektrotechnischer Verein, CH-8320 Fehraltorf
SNV	: Schweizerische Normen-Vereinigung, CH-8008 Zurich
SOLE	: Society of Logistic Engineers, Huntsville, AL 35806
VDI/VDE	: Verein Deutscher Ing./Verband Deut. Elektrotechniker, D-60549 Frankfurt a. M.

References

(see Acronyms on p. 582)

1 Basic Concepts, Historical Development, Quality & Reliability Assurance

- [1.0] Bacivarov I.C., "Prof. A. Birolini, a Guru of European Reliability" & "Lesson from a life dedicated to reliability", *Asigurarea Calitatii- Quality Assurance*, 16(2010)63, pp. 2-3 & 16(2010)64, pp. 5-7; "A. Birolini, Reliability Engineering - A Bible of Reliability", *Proc.CCF2010*, 4pp.
- [1.1] Birnbaum Z.W. et al., "Multi-component systems & structures and their reliability", *Technometrics*, 3(1961), pp. 55-77.
- [1.2] Birolini A., "Product assurance tasks and organization", *Proc. 21st EOQC Conf.*, Varna 1977, Vol.1, pp. 316-29; "Qualitäts- und Zuverlässigkeitssicherung komplexer Systeme: Teil 1 und 2", *Bull. SEV/VSE*, 70 (1979), pp. 142-48 and 237-43; "Reliability engineering: Cooperation between University and Industry at the ETH Zurich", *Quality Eng.*, 8(1996)4, pp. 659-74; "Lesson from a life dedicated to reliability", *Quality Assurance* (Asigurarea Calitatii), 16(2010)64, pp. 5-7.
- [1.3] Braband J., *Risiko analysen in der Eisenbahn-Automatisierung*, 2005, Eurailpress, Hamburg.
- [1.4] Buckley F.J., *Configuration Manag.: Hardware, Software, Firmware*, 1993, IEEE Press, Piscataway NJ.
- [1.5] Condra L.W. et al., "Electronic components obsolescence", *IEEE Trans. Comp., Pack.. & Manuf. Technol.*, 20(1997), pp. 368-71.
- [1.6] Dersin P., "Predicting the expected duration and cost of reliability-related warranty extension", *Proc. λ/μ 15 Conf.*, Lille, France, Oct. 2006, Section 2D, 4 pp.
- [1.7] Dougherty M.E. et al., *Human Reliability Analysis*, 1988, Wiley, NY.
- [1.8] Feigenbaum A.V., *Total Quality Control*, 3rd Ed. 1983, McGraw-Hill, NY.
- [1.9] Frenkel M. et al., *Risk Management*, 2000, Springer, Berlin.
- [1.10] Gay T.F. (Ed.), *Product Liability in Europe*, 1993, 2nd Ed., ORGALIME, Brussels, see also EUR Council Directive 85/374/EEC (Regulations concerning liability for defective products).
- [1.11] Haug S. et al., "Impact of electronic comp. obsolescence on commercial aerospace", *Aerospace Mag.*, 1999, March, pp. 26-31; see also CENELEC ES 59010 (2001) and IEC 62402 (2007).
- [1.12] IEEE, Special issue on: 50th Anniversary IEEE Rel. Soc., *IEEE Trans. Rel.*, 47(1998)3-SP.
- [1.13] Irland E. A., "Assuring quality and reliability of complex electronic systems: Hardware and software", *Proc. IEEE*, 76(1988)1, pp. 5-18.
- [1.14] Juran J.M., et al., (Eds.), *Quality Control Handbook*, 4th Ed. 1988, McGraw-Hill, NY.
- [1.15] Kuehn R., "Four decades of reliability experience", *Proc. Ann. Rel. & Maint. Symp.*, 1991, pp. 76-81.
- [1.16] Kusiak A. (Ed.), *Concurrent Engineering: Automation, Tools and Techniques*, 1993, Wiley, NY.
- [1.17] LaSala K.P., "Book review - *Rel. Eng. 4th Ed.*", *IEEE Rel. Newslette*, 50(2004)3 Aug. 2004, 2pp.; Book review - *Rel. Eng. 6th Ed.*", *IEEE Rel. Newslette*, 57(2011)1 Feb. 2011, 3pp.
- [1.18] Mattana G., *Qualità, Affidabilità, Certificazione*, 15th Ed. 2005, Angeli, Milano.
- [1.19] Meindi J.D. (Ed.), Special Issue on Limits of Semiconductor Technology, *Proc. IEEE*, 89(2001)3.
- [1.20] Moore E.F. et al., "Reliable circuits using less reliable relays", *J. of the Franklin Inst.*, 262(1956), pp. 191-208 and 281-297.
- [1.21] Peters G.A., "Risk analysis", *Technology, Law and Insurance*, (1997) 2, pp. 97-110.
- [1.22] RAC, *Reliability Toolkit: Commercial Practices Edition*, 1995; *Maintainability Toolkit*, 1999, RAC, Rome NY (now RIAC, Utica, NY).
- [1.23] Roeser S. et al. (Ed.), *Handbook of Risk Theory*, 2012, Springer, Berlin-Heidelberg-NY.
- [1.24] Taguchi G., *System of Experimental Design-Engineering Methods to Optimize Quality and Minimize Costs*, Vol. 1 & 2., 1987, Unipub, White Plains NY.
- [1.25] Turconi G., "Ulysses, Scylla, Charybdis - story of rel.", *Proc. Ann. Rel. & Main. Symp.*, 2002, pp. 135-9.
- [1.26] Umiker B. et al., "Wie lassen sich grosse Industriekatastrophen verhüten?", *Manag. Zeitschrift*, 1(1987), pp. 15-22; "Innovation and resistance to it", *7th Bbuilding Congress*, Zurich, Nov. 13, 2008; Umiker B. (www.wuco.ch), "The modern art of a discourse on risk", *4th Europ. Conf. on Safety Anal. & Risk Manag.*, Rome, Oct. 19, 1993; "Risk management: Concept and implementation", *ASCOM Tech. Mag.*, 3(1994), pp. 33-36; "The coconut effect", *Amer. Soc. for Ind. Security Meeting*, Zurich ETH, June 4, 1997; "Krisenbewältigung durch Innovation", 2009, *Bau & Architektur* 4(2009), pp. 2-4.
- [1.27] Von Neumann J., "Probabilistic logic's and the synthesis of reliable organisms from unreliable components", *Ann. of Math. Studies*, 34(1956), pp. 43-98.
- [1.28] Wang J.X. et al., *Risk Engineering and Management*, 2000, Dekker, NY.

see also [A1.1 to A5.6]

2 Reliability Analysis

Reliability Techniques

- [2.1] Arlat J. et al., "Fault injection and dependability evaluation of fault tolerant systems", *IEEE Trans. Comp.*, 42(1993)8, pp. 913-23.
- [2.2] Birolini A., *Zuverlässigkeit von Schaltungen und Systemen*, 1982, ETH Zurich; *Modelle zur Berechnung der Rentabilität der Q.- und Z.-Sicherung komplexer Waffensysteme*, 1986, GRD, Bern; *Zuverlässigkeit von Geräten und Systemen*, 1985, 1988, 1991, 1997, Springer, Berlin.
- [2.3] Catuneanu V.M. et al., *Reliability Fundamentals*, 1989, Elsevier, Amsterdam.
- [2.4] Denson W., "The history of reliability prediction", *IEEE Trans. Rel.*, 47(1998)3-SP, pp. SP-321-28.
- [2.5] Dhillon B.S. et al., "Common-cause failures in engineering systems: A review", *Int. J. Rel., Qual. & Safety Eng.*, 1(1994), pp. 103-29.
- [2.6] Dugan J.B., "Automated analysis of phased-mission reliability", *IEEE Trans. Rel.*, 40(1991), pp. 45-52.
- [2.7] Esary J.D. et al., "Rel. an. of phased missions", *Proc. Conf. Rel. & Fault Tree An.*, 1975, pp. 213-36.
- [2.8] Friedman M.A. et al., "Reliability techniques for combined hardware/software systems", *Proc. Ann. Rel. & Maint. Symp.*, 1992, pp. 290-293.
- [2.9] Klaassen K., "Active red. in analog el. systems", *Proc. Ann. Rel. & M. Symp.*, 1975, pp. 573-78.
- [2.10] MIL-HDBK-338B (1998): *Electronic Reliability Design Handbook*.
- [2.11] Mitra S. et al., "Common-mode failures in redundant VLSI systems: A survey", *IEEE Trans. Rel.*, 49(2000)3, pp. 285-95.
- [2.12] O' Connor P.D.T., *Practical Reliability Engineering*, 3th Ed. 1991, Wiley, NY.
- [2.13] Pahl H., ed. *Handbook of Reliability Engineering*, 2003, Springer, Berlin & NY.
- [2.14] RAC, WCCA: *Worst Case Circuit Analysis Appl. Guidelines*, 1993; RTMG: *Thermal Manag. Guidebook*, 1994; RADC-TR-90-109: *Integration of Sneak Analysis with Design*, 1990; *Reliability Toolkit: Commercial Practices Edition*, 1995, RAC, Rome NY (now RIAC, Utica NY).
- [2.15] Rhoads M.J., *Design for Rel. Handbook*, AMSAA TR-2011-24, AMSAA, Aberdeen Prov. G., Maryland.
- [2.16] Roush M.L. et al., *Applied Reliability Engineering*, 2002, Center for Rel. Eng., Maryland.
- [2.17] Siewiorek D.P., "Architecture of fault-tolerant computers", *Proc. IEEE*, 79(1991)12, pp. 1710-34; -et al., *Reliable Computer Systems Design and Evaluation*, 1992 (3d Ed. 1998), Dig. Press, Bedford MA.
- [2.18] Somani A.K. et al., "Computational-efficient phased-mission reliability analysis for systems with variable configurations", *IEEE Trans. Rel.*, 41(1992)4, pp. 504-11.
- [2.19] Tomek L. et al., "Rel. models of life-critical real-time systems", *Proc IEEE*, 79(1994)1, pp. 108-21.

see also [1.22, 2.31-2.49, 2.61-2.98, 5.0-5.83, 6.0-6.90, A2.0-A2.13]

Component Failure Rate Models & Data

- [2.20] ESA ECSS-Q-HB-30-08A: *Comp. Rel. Data Sources & their Use*, 2011; Q-ST-30-11C: *Derating*, 2011.
- [2.21] FIDES Guide 2009A (2010): *Rel. Methodology for Electronic Systems*, Paris (www.fides-reliability.org).
- [2.22] IEC 61709 (1996, Ed. 2 2011): *Electronic Components - Reliability - Reference Condition for Failure Rates and Stress Models for Conversion*.
- [2.23] IEC/TR 62380 (2004): *Reliability Data Handbook* (formerly RDF 2000/UTE C80-810: *Recueil de Données de Fiabilité*, CNET Lannion).
- [2.24] IRPH 2003: *Italtel Reliability Prediction HDBK*, 2003, Italtel, Milano.
- [2.25] MIL-HDBK-217G (draft): *Reliability Prediction of Electronic Equipment* (Rev. H planned, see also McLeish J.C., Enhancing MIL-HDBK-217 Rel. Predictions with Physics of Failure Methods, *Proc. Ann. Rel. & Maint. Symp.*, 2010, pp. 6-10).
- [2.26] NSWC-11: *HDBK of Reliability Prediction Procedures for Mechanical Equipment*, 2011, Naval Surface Warfare Center-Carderock Division, West Bethesda MA.
- [2.27] RAC, NONOP-1: *Nonoperating Rel. Data*, 1992; NPRD-2011: *Nonelectronic Parts Rel. Data*, 2011; TR-89-177: *VHSIC/ VHSIC Rel. Modeling*; TR-90-72: *Rel. Analysis Assessment of Adv. Technologies*, RAC, Rome, NY (now RIAC, Utica NY).
- [2.28] RDF 96: *Recueil Données de Fiabilité des Comp. Electroniques*, 1996, Thomson-CSF, Grenoble.
- [2.29] RIAC-HDBK-217Plus: *Handbook 217Plus Rel. Prediction Models*, 2008, RIAC, Utica, NY
- [2.30] SR-332: *Rel. Prediction Procedure for El. Equip.*, Issue 3, 2011, Telcordia Technol., Red Bank NJ.

see also [1.22, 3.1, 3.10, 3.15, 3.58, 3.66, 3.67, A2.7]; for Bellcore see [2.30]

Reliability of Large / Complex Structures

- [2.31] Agarwal M. et al., "CERT analysis of cons. k -out-of- n : F systems", *IEEE Trans. Rel.*, 56(2007)1, pp. 26-34.
- [2.32] Arunkumar S. et al., "Enumeration of all minimal cut-sets for a node pair in a graph", *IEEE Trans. Rel.*, 28(1987)1, pp. 51-55.
- [2.33] Bansal V.K., "Minimal path-sets and minimal cut-sets using search techniques", *Microel. & Rel.*, 22(1982)6, pp. 1067-1075.
- [2.34] Barlow R.E. et al., *Mathematical Theory of Reliability*, 1965, Wiley, NY; *Statistical Theory of Reliability and Life Testing*, 1975, Holt Rinehart, NY.
- [2.35] Bellcore SR-TSY-001171, *Methods and Procedures for System Reliability Analysis*, 1989.
- [2.36] Bryant R.E., "A graph based algorithm for Boolean function manip.", *IEEE Trans. Comp.*, 35(1986)8, pp. 677-91; "Symbolic Boolean manip. with ordered BDD", *ACM Comp. Surv.*, 24(1992), pp. 293-318..
- [2.37] Carrasco J.A. et al., "An algorithm to find minimal cuts of coherent fault-trees with event-classes using a decision tree", *IEEE Trans. Rel.*, 48(1999)1, pp. 31-41.
- [2.38] Cluzeau, T. et al., "An efficient algorithm for computing the rel. of consecutive k -out-of- n : F systems", *IEEE Trans. Rel.*, 57(2008)1, pp. 84-87.
- [2.39] Esary J.D. et al., "Relationship between system failure rate and component failure rates", *Technometrics* 5(1963)2, pp. 183-189; "Coherent structures of non-identical components" *Technometrics* 5(1963)2, pp. 191-209.
- [2.40] Hura G.S., "A Petri net approach to enumerate all system success paths for rel. evaluation of complex systems"; "Petri net approach to the analysis of a structured program"; "Petri net as a mod. tool", *Microel. & Rel.*, 22 (1982)3, pp. 427-39, (1983) pp. 157-59, 467-75, 851-53.
- [2.41] Keymeulen D. et al., "Fault-tolerant evolvable hardware using field-programmable transistor arrays", *IEEE Trans. Rel.*, 49(2000)3, pp. 306-16.
- [2.42] Kossow A. et al., "Failure probability of strict consecutive- k -out-of- n : F systems", *IEEE Trans. Rel.*, 36(1987)5, pp. 551-53; "Rel. of consecutive- k -out-of- n : F systems with nonidentical component rel.", *IEEE Trans. Rel.*, 38(1989), pp. 229-33; "Mean time to failure for linear-consec- k -out-of- n : F systems", *IEEE Trans. Rel.*, 40(1991)3, pp. 271-72; "Rel. of linear consecutive connected systems with multistate comp.", *IEEE Trans. Rel.*, 44(1995)3, pp. 518-22.
- [2.43] Krishna C.M. et al., "Optimal configuration of redundant real-time systems in the face of correlated failures", *IEEE Trans. Rel.*, 44(1995)4, pp. 587-94.
- [2.44] Kuo W. et al., "An annotated overview of system reliability optimization", *IEEE Trans. Rel.*, 49(2000)2, pp. 176-87.
- [2.45] Luo T. et al., "Improved alg. for coherent-system rel.", *IEEE Trans. Rel.*, 47(1998)1, pp. 73-78.
- [2.46] Myers A.F., " k -out-of- n :G system reliability with imperfect fault coverage", *IEEE Trans. Rel.*, 56(2007)3, pp. 464-73.
- [2.47] Prasad V.R. et al. "Rel. optimiz. of coherent systems", *IEEE Trans. Rel.*, 49(2000), pp. 323-30.
- [2.48] Schneeweiss W., *Boolean Functions with Eng. Applications & Comp. Progr.* 1989, Springer, Berlin.
- [2.49] Xing L., "Rel. evaluation of phased-mission systems with imperfect fault coverage and common-cause failures", *IEEE Trans. Rel.*, 56(2007)1, pp. 58-68.

see also [2.97, 6.0-6.90]

Software Tools

- [2.50] Bernet R., "CARP - A program to calculate the predicted reliability", *6th Int. Conf. on Rel. & Maint.*, Strasbourg 1988, pp. 306-10; *Modellierung reparierbarer Systeme durch Markoff- und Semiregenerative Prozesse*, 1992, Ph.D.Thesis 9682, ETH Zurich; Birolini A. et al, *CARAP ETH Technical Spec.*, 1995, Report S10, ETH Zürich, Rel. Lab.; Kovalenko I. and Kuznetov N., *Basis of the RS-Program/Guidance to the RS-Program*, 1997, Rep. S13/S14, ETH Zurich, Rel. Lab.
- [2.51] Bowles J.B. et al., "Comparison of commercial reliability-prediction programs", *Proc. Ann. Rel. & Maint. Symp.*, 1990, pp. 450-55.
- [2.52] Dylis D.D. et al., "A comprehensive reliability assessment tool for electronic systems", *Proc. Ann. Rel. & Maint. Symp.*, 2001, pp. 308-13.
- [2.53] Gymayr J., et al., "Fault-tree analysis: a knowledge-engineering approach", *IEEE Trans. Rel.*, 44(1995)1, pp. 37-45.
- [2.54] Item, *Item Toolkit for RAMS*, 2001, Item Software, Fareham, Hampshire UK.
- [2.55] Jaeger H., "RAMTOOL", *Proc. ETH/IEEE Int. Symp. on Rel. Eng. 2'000*, ETH Zurich, Rel. Lab., Oct. 17, 1996; *Zuverlässigkeit und Materialerhaltbarkeit*, Bundesakad. W.W., Mannheim, 1998.

- [2.56] Lindemann C., et al., "Numerical methods for reliability evaluation of Markov closed fault-tolerant systems", *IEEE Trans. Rel.*, 44(1995)4, pp. 694-704.
- [2.57] RAC, *PRISM System Reliability Assessment Software*, 2001, RAC Rome, NY (s. also [1.22]).
- [2.58] Relx, *Visual Reliability Software*, 2001, Relx Software, Greensburg PA.
- [2.59] Sahner R. et al., "Rel. modeling using SHARPE", *IEEE Trans. Rel.* 36(1987), pp. 186-93.
- [2.60] Telcordia, *Automated Rel. Prediction Procedure*, Telcordia Technology, Red Bank NJ.
- see also [1.22, 2.6, 2.18, 2.74, 2.76, 4.24, 4.32, 6.18, 6.43]

Mechanical Reliability

- [2.61] Barer R.D., *Why Metals Fail*, 3rd Ed. 1974, Gordon & Breach, NY.
- [2.62] Beitz W. et al. (Ed.), *Handbook of Mechanical Engineering*, 1994, Springer, Berlin.
- [2.63] Bogdanoff J.L. et al., *Probabilistic Models for Cumulative Damage*, 1985, Wiley, NY.
- [2.64] Carter A.D.S., *Mechanical Reliability*, 2nd Ed. 1986, Macmillan, London.
- [2.65] Collins J.A., *Failure of Materials in Mechanical Design*, 1981, Wiley, NY.
- [2.66] Engelmaier W., *Reliable Surface Mount Solder Attachments Through Design & Manuf. Quality*, 1993, Rep. L21, ETH Zurich, Rel. Lab. (also *Proc. ETH/IEEE Workshop SMT*, 1992).
- [2.67] Freddi S., *Design of Experiment*, Course at the 15th Symp. Danubia-Adria, Bertinoro, 1998.
- [2.68] Hutchings F. et al. (Ed.), *Failure Analysis*, 1981, Am. Soc. Met., Metals Park OH.
- [2.69] Kececioglu D., *Reliability Eng. Handbook* (Vol. 1 & 2), 1991, Prentice, Englewood Cliffs NJ; - et al., "Combined-stress fatigue reliability analysis", *Proc. Ann. Rel. & Maint. Symp.*, 1998, pp. 202-08; - et al., "A unified approach to random fatigue reliability quantification under random loading", *Proc. Ann. Rel. & Maint. Symp.*, 1998, pp. 308-13.
- [2.70] Kutz M. (Ed.), *Mechanical Engineers' Handbook*, 1986, Wiley, NY.
- [2.71] Lewis E.E., "A load-capacity interference model for common-mode failures in 1-out-of-2: G systems", *IEEE Trans. Rel.*, 50(2001)1, pp. 47-51.
- [2.72] Manson S.S., *Thermal Stress and Low-Cycle Fatigue*, 1981, Krieger, Malabar FL.
- [2.73] Nelson J. et al., "Rel. models for mech. equip.", *Proc. Ann. Rel. & Maint. Symp.*, 1989, pp. 146-53.
- [2.74] NSWC-11: *HDBK of Reliability Prediction Procedures for Mechanical Equipment*, 2011, Naval Surface Warfare Center- Carderock Division, West Bethesda MA.
- [2.75] Padgett W.J., "A multiplicative damage model for strength of fibrous composite materials", *IEEE Trans. Rel.*, 47(1998)1, pp. 46-52.
- [2.76] Pozsgai P. et al., "SYSLEB: A Tool for the Calculation of the System Reliability from raw Failure Data", *Proc. Ann. Rel. & Maint. Symp.*, 2002, pp. 542-49.
- [2.77] RAC, NPS: *Mechanical Applications in Reliability Engineering*, 1993, Rome NY .
- see also [2.26, 2.27, 3.52, 3.70-3.93]

Failure (Fault) Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA)

- [2.80] Bednarz S. et al., "Efficient analysis for FMEA", *Proc. Ann. Rel. & Maint. Symp.*, 1988, pp. 416-21.
- [2.81] Bowles J.B., "The new SAE FMECA Std", *Proc. Ann. Rel. & Maint. Symp.*, 1998, pp. 48-53; - et al., "Software FMEA for small embedded control syst.", *Proc. Ann. Rel. & Maint. Symp.*, 2001, pp. 1-6.
- [2.82] Braband J., "Improving the risk priority number concept", *J. of System Safety*, Q2(2003), pp. 21-23.
- [2.83] Chrysler, Ford, GM, *Potential FMEA*, 2nd Ed. 1995 (also as SAE J-1739).
- [2.84] DIN 25419: *Störfallablaufanalyse*, 1977-79; 25424: *Fehlerbaumanalyse*, 1981; 25448: *Ausfall-effektanalyse*, 1980; 31000: *Allg. Leit. für das sicherheitsgerechte Gestalten tech. Erzeug.*, 1979.
- [2.85] Dugan J.B. et al., "Dynamic fault tree models for fault tolerant comp. syst.", *IEEE Trans. Rel.*, 41(1992), pp. 363-77 (see also *Rel. Eng. & Syst. Safety*, 39(1993), pp. 291-307); "Developing a low-cost high-quality software tool for dyn. fault-tree anal.", *IEEE Trans. Rel.*, 49(2000), pp. 49-59.
- [2.86] ESA ECSS-Q-30-02A: *Space product assurance, FMECA*, 2001.
- [2.87] Goddard P.L., "Software FMEA techniques", *Proc. Ann. Rel. & Maint. Symp.*, 2000, pp. 118-23.
- [2.88] Hall F.M. et al., "Hardware/Software FMECA", *Proc. Ann. Rel. & Maint. Symp.*, 1983, pp. 320-27.
- [2.89] IEC 60812 (2006): *Procedure for FMEA*; 61025(2006): *Fault Tree Analysis (FTA)*.
- [2.90] Jackson T., "Integrated sneak circuit analysis and FMEA", *Proc. Ann. Rel. & Maint. Symp.*, 1986, pp. 408-414.
- [2.91] Keene S.J., "Eng. application of failure data", *Proc. Ann. Rel. & Maint. Symp.*, 1971, pp. 104-09.

- [2.92] MIL-STD-1629A (1998): *Procedures for Performing a FMECA*.
- [2.93] Onodera K., "Effective technique of FMEA at each life-cycle", *Proc. Ann. Rel. & Maint. Symp.* 1997, pp. 50-56.
- [2.94] Picciolo G. et al., "Thermoelectrical power station rel. assessment", *Proc. PMAPS 2002*, pp. 347-53.
- [2.95] Price C.J. et al., "Identifying design glitches through automated design analysis", *Proc. Ann. Rel. & Maint. Symp.*, 1999, pp. 277-82.
- [2.96] RAC: *FMECA*, 1993; *FTA*, 1990; *WCCA* (Worst Case Circuit Anal.), 1992 (now RIAC, Utica NY).
- [2.97] Schneeweiss W., *The Fault Tree Method*, 1999, LiLoLe, Hagen.
- [2.98] Stamenkovic B. et al., "Failure modes, effects and criticality analysis: The basic concepts and applications", *Proc. Int. Summer Seminar*, Dubrovnik, 1987, pp. 21-25.
- see also [1.22, 3.58 (2013), 5.82, 5.75, 5.79, 3.58 (2013)]*

3 Qualification of Components and Assemblies

Selection Criteria and Qualification Tests for Components

- [3.1] Bajenescu T.I. et al., *Component Reliability for Electronic Systems*, 2010, Artech House, Norwood MA.
- [3.2] Birolini A., "Möglichkeiten und Grenzen der Qualifikation, Prüfung und Vorbehandlung von ICs", *QZ*, 27(1982)11, pp. 321-26; "Prüfung und Vorbehandlung von Bauelem. und bestück. Leiterplatten", *VDI/VDE Fachtagung*, Karlsruhe 1984, VDI Bericht Nr. 519, pp. 49-61; "Neue Ergebnisse aus der Qualif. grosser Halbleiterspeicher", *me*, 7(1993) 2, pp. 98-102; – et al., "Test and screening strategies for large memories", *1st European Test Conf.*, Paris: 1989, pp. 276-83.
- [3.3] Brambilla P. et al., "Rel. evaluation of plastic-packaged device for long life applications by THB test", *Microel. & Rel.*, 26(1986)2, pp. 365-84.
- [3.4] Diaz C. et al., "Electrical overstress & electrostatic discharge", *IEEE Trans. Rel.*, 44(1995)1, pp. 2-5.
- [3.5] ESA PSS 01-603: *ESA Preferred parts List*, 3rd Ed. 1995.
- [3.6] ETH Zurich Reliability Lab., *Reports Q2-Q12: Qualification Test for DRAMs 256Kx1, SRAMs 32Kx8, EPROMs 32Kx8, SRAMs 8Kx8, DRAMs 1Mx1, EEPROMs 8Kx8, SRAMs 128Kx8, DRAMs 4Mx1, EEPROMs 32Kx8, EPROMs 64Kx16, and FLASH-EPROMs 128Kx8*. 1988-92.
- [3.7] Gerling W., "Modern reliability assurance of integrated circuits". *Proc. ESREF'90*, Bari, pp. 1-12.
- [3.8] IEC 60068-1 to -2 (1983-2012): *Environmental Testing*; 60319 (1999): *Presentation and Spec. of Rel. Data for El. Comp.*; 60721-1 to -2 (1982-2012): *Classification of Envir. Cond.*; 60749-1 to -40 (2002-2012): *Semiconductor Devices - Mech. and Climatic Test Methods*; 61000-1 to -6 (1990-2012): *Electromag. Compatibility*; see also QC 001001 (2000): *Basic Rules of IEC Quality Assessment Syst. for Electron. Comp. (IECQ)*, QC 001002-1006, QC 200000, QC 210000.
- [3.9] IEEE, Special issues on: Reliability of Semiconductor Devices, *Proc. IEEE*, 62(1974)2; Micron and Submicron Circuit Engineering, *Proc. IEEE*, 71(1983)5; Integrated circuit technologies of the future, *Proc. IEEE*, 74(1986)12; VLSI Reliability, *Proc. IEEE*, 81(1993)5.
- [3.10] Jensen F., *Electronic Component Reliability*, 1995, Wiley, NY.
- [3.11] Lin H-Y. et al., "Efficient algorithm for space alloca. prob.", *IEEE Trans. Rel.*, 55(2006)2, pp. 369-78..
- [3.12] MIL-STD-883H (2010): *Test Methods and Procedures for Microelectronics*; see also -199, -202, -750, -810, -976, -M-38510, -S-19500.
- [3.13] Murari B. et al., *Smart Power ICs: Technologies and Applications*, 1996, Springer, Berlin.
- [3.14] Powell R.F., *Testing Active and Passive Electronic Components*, 1987, Dekker, NY.
- [3.15] RAC, *Parts Selection, Application and Control*, 1993; *Reliable Appl. of Components*, 1993; *Reliable Appl. of Microcircuits*, 1996; *Reliable Appl. of Hybrids*, 1993; *Reliable Appl. of Multichip Modules*, 1995, RAC, Rome NY (now RIAC, Utica NY).
- [3.16] Ratchev D., "Are NV-Mem. non-volatile?" *Proc. 1993 IEEE Workshop on Memory Test.*, pp. 102-06.
- [3.17] RIAC, *Reliability of Compound Semiconductor Analogue ICs*, 2006, RIAC, Utica NY.
- [3.18] Sawada K. et al., "An evaluation of I_{DDQ} versus conventional testing for CMOS sea-of-gate ICs", *Int. Test Conf.*, 1992, pp. 158-67.
- [3.19] Thomas R.W., "The US Department of Defense procurement strategy and the semiconductor industry in the 1990's", *Proc. 4th Int. Conf. Quality in El. Comp.*, Bordeaux 1989, pp. 1-3.
- [3.20] van de Goor A.J., *Testing Semiconductor Memories*, 1991, Wiley, NY.
- [3.21] Williams T.W. (Ed.), *VLSI - Testing*, 1986, North-Holland, Amsterdam.

- [3.22] Wolfgang E. et al., "Electron beam testing", *Proc. ESREF'90*, Bari, pp. 111-120.
 [3.23] Zinke O. et al., *Widerstände, Kondensatoren Spulen und ihre Werkstoffe*, 1982, Springer, Berlin.
see also [2.10, 5.1-5.20, 8.21-8.35]

Failure Mechanisms, Failure Analysis

- [3.30] Amerasekera E., Campbell D., *Failure Mechanisms in Semiconductor Devices*, 1987, Wiley, NY.
 [3.31] Barbottin G., et al. (Eds.), *Instabilities in Silicon Devices*, 1986, North-Holland, Amsterdam.
 [3.32] Bayle F. et al., "Temperature acceleration models in rel. predictions: Justification & improvements", *Proc. Ann. Rel. & Maint. Symp.*, 2010, 7 pp.
 [3.33] Black J.R., "Electromigration failure mode in Aluminum metallization for semiconductor devices", *Proc. IEEE*, 57(1969)9, pp. 1587-94.
 [3.34] Ciappa M., *Ausfallmech. integrierter Schaltungen*, 1991, Rep. F1 & F4, ETH Zurich, Rel. Lab.; - et al., "Rel. of laser-diode modules in temperature-uncontrolled env.", *Int. Rel. Phys. Symp.*, 1994, pp. 466-69; - et al., "Lifetime pred. of IGBT modules for traction appl.", *Proc. Int. Rel. Phys. Symp.*, 2000, pp. 210-16.
 [3.35] Chakravarthi AT. et al., "A comprehensive framework for predictive modeling of negative bias temperature instability", *Proc. Int. Rel. Phys. Symp.*, 2004, pp. 273-282.
 [3.36] Dantzig J.A. et al., "Solidification", *EPFL Press*, 2009, pp. 287-298, ISBN 978-2-940222-17-9.
 [3.37] Deal B.E. et al., "Characteristic of the surface-state charge of thermally oxidized silicon", *J. of Electrochem. Soc.*, 114(1967), pp. 266-274.
 [3.38] Dieci D. et al., "Breakdown and degradation issues and the choice of a safe load line for power HFET operation", *Proc. Int. Rel. Phys. Symp.*, 2000, pp. 258-63.
 [3.39] Fantini F., "Reliability and failure physics of integrated circuits", in *Dinemite II*, (Vol. IV), Interuniversitair Micro-Elektronica Centrum, 1986, Leuven, pp. 1-30.
 [3.40] Fung R.C.-Y. et al., "Latch-up model for the parasitic p-n-p-n path in bulk CMOS", *IEEE Trans. El. Devices*, 31(1984)1, pp. 113-20.
 [3.41] Ghidini G. et al., "Charge trapping mechanism under dynamic stress and their effect on failure time", *Proc. Int. Rel. Phys. Symp.*, 1999, pp. 88-92.
 [3.42] Gieser H.A. et al., "A CDM reproducible field degradation and its reliability aspects", *Proc. ESREF'93*, Bordeaux , 5pp., see also *Qual. & Rel. Eng. International*, 10(1994)4, pp. 341-45.
 [3.43] Glasstone S., Laidler K.J., Eyring H.E., *The Theory of Rate Processes*, 1941, McGraw-Hill, NY.
 [3.44] Herrmann M., *Charge Loss Modeling of EPROMs with ONO Interpoly Dielectric*, 1994, Ph.D. Thesis 10817, ETH Zurich; - et al., "Field and high- temperature dependence of the long-term charge loss in EPROMs", *J. Appl. Phys.*, 77 (1995)9, pp. 4522-40.
 [3.45] Howes M.J. et al. (Eds.), *Rel. and Degradation - Semiconductor Dev. & Circuits*, 1981, Wiley, NY.
 [3.46] Hu C. (Ed.), *Nonvolatile Semicond. Mem.: Tech., Design, Appl.*, 1991, IEEE Press, Piscataway NJ; -et al., "A unified gate oxide rel. model", *Proc. Int. Rel. Phys. Symp.*, 1999, pp. 47-51; "Exp. evidence for V-driven breakdown in ultra thin gate ox.", *Proc. Int. Rel. Phys. Symp.*, 2000, pp. 7-15.
 [3.47] Hu C.-K. et al., "Electromigr. of Cu/low dielectric const. interconnect", *Microel. Rel.*, 46(2006), pp. 213-31.
 [3.48] Jacob P., private commun. 2005/2009, peter.jacob@empa.ch; "Poly-si extensions and etching residues as a rel. risk" *Microsyst Technol.*, 15(2009)1, pp. 169-74; "Surface ESD in assembly fab mach. as a functional and rel. risk", *Microel. Rel.*, 48(2008), pp. 1608-12; - et al. "FIB voltage contrast localization & analysis of contac-via-chains", *Proc. SPIE, Edinburgh 1999*, pp. 273-79; "Electrostatic effects on semiconductor tools", *Microel. Rel.*, 44(2004), pp. 1787-92; "Electrostatic discharge directly to the chip surface, caused by autom. post-wafer processing", *Microel. Rel.*, 45(2005), pp. 1174-80; "Manuf.-robotics-induced damages on semicond. dies", *Proc. IPFA 2005*, pp. 307-12; "Unusual defects, generated by wafer sawing", *Microel. Rel.*, 48(2008), pp. 1253-57; "Reading distance degradation mechanism of near-field RFID devices", *Microel. Rel.*, 49(2009), pp. 1288-92.
 [3.49] JEDEC, *Failure Mechanism and Models for Semicond. Devices*, JEP 122G, 2011, JEDEC, Arlington, VA.
 [3.50] Lantz L., "Soft errors induced by α - particles", *IEEE Trans. Rel.*, 45 (1996)2, pp. 174-79.
 [3.51] Li E. et al., "Hot carrier effects in nMOSFETs in 0.1 μ m CMOS tech.", *Proc. Int. Rel. Phys. Symp.*, 1999, pp. 253-8; "Hot carrier ind. degr. in sub μ dev.", *Proc. Int. Rel. Phys. Symp.*, 2000, pp. 103-7.
 [3.52] Miner M.A., "Cumulative damage in fatigue", *J. of Appl. Mech.*, 12(1945)Sept., pp. A159-64.
 [3.53] Nakajiam H., "The discovery and acceptance of the Kirkendall effect: The result of a short research career", *JOM*, 49(1997)6, pp. 15-19.
 [3.54] Ohring M., *Reliability and Failure of Electronic Materials and Devices*, 1998, Academic Press, NY.

- [3.55] Pecht M.G. et al., *Guidebook for Managing Silicon Chip Reliability*, 1999, CRC Press, NY; et al, *Influence of Temperature on Microelectronics and System Reliability: A PoF Approach*, 2006, Lavoisier, Paris.
- [3.56] Peck D.S., "Comprehensive model for humidity testing correlation", *Proc. Int. Rel. Phys. Symp.*, 1986, pp. 44-50; - et al., "Highly accelerated stress Tutorial *Int. Rel. Phys. Symp.*", 1990, pp. 4.1-27.
- [3.57] Pierrat L., "Estimation de la prob. de déf. par interaction de 2 lois Weibull", *Rev. Stat. Appl.*, 1992, pp. 5-13; "La variabilité stat. de la température et son infl. sur la durée de vie", *Congrès IMAPS 05, Grenoble*; "La fiabilité des comp. de puissance", *inv. paper S1-4 Coll. EPF'06, Grenoble*.
- [3.58] RAC/RIAC, RIAC-FMD-2013: *Failure Mode / Mech. Distribution*, 2013; MFAT-1: *Microel. Failure Analysis Tech.*, 1981; MFAT-2: *GaAs Microcircuit Char. & Failure Anal. Techn.*, 1988, RAC, Rome NY, now RIAC, Utica NY.
- [3.59] Rajusman R., "Iddq testing for CMOS VLSI", *Proc. IEEE*, 88(2000)4, pp. 544-66.
- [3.60] Reiner J., "Latent gate oxide defects caused by CDM-ESD", *Proc. EOS/ESD Symp.*, 1995, pp. 6.5.1-11, also in *Jour. of Electrostatic*, 38(1996) pp. 131-57; *Latent Gate Oxide Damage Induced by Ultra fast Electrostatic Discharge*, 1995, Ph.D. Thesis 11212, ETH Zurich; - et al. "Impact of ESD-induced soft drain junction damage on CMOS product lifetime", *Microel. Rel.*, 40(2000), pp. 1619-28.
- [3.61] Reynolds F., "Thermally Accelerated Aging of Semic. Comp.", *Proc. IEEE*, 62(1974)2, pp. 212-22.
- [3.62] Rudra B., "Failure mech. models for conductive-filament formation", *IEEE Trans. Rel.*, 43(1994)3, pp.54-60.
- [3.63] Srinivasan G., "Modeling cosmic-ray-induced soft errors in IC's", *IBM J. R&D*, 40(1996)1, pp. 77-90.
- [3.64] Takeda E. et al., "An empirical model for devices degradation due to hot-carrier injection", *IEEE Electron Device Letters*, 1983, pp. 111-113.
- [3.65] Troutmann R.R., "Latch-up in CMOS technol.", *IEEE Circuits and Dev. Mag.*, (1987)5, pp. 15-21.
- [3.66] VITA, *ANSI/VITA 51.0-2008: Reliability Prediction*, 2008; *51.2-2011: Physic of Failure (PoF) Reliability Prediction*, 2011, Fountain Hills, AZ.
- [3.67] White M. et al., *Microelectronics Reliability: Physics-of-Failure Based Modeling and Lifetime Evaluation*, NASA WBS: 939904.01.11.10, JPL Publ. 08-5 2/08, 2008, Pasadena CA.

see also [1.19, 2.27 (TR), 2.61-2.77, 3.70-3.93]

Micro Connections and Packaging

- [3.70] ASM, *Packaging*, Vol. 1, 1989, ASM Int., Material park OH.
- [3.71] Bell.H. et al., *Reflow Technology: Fundamentals of Reflow Soldering*, 2009, Rehm Thermal Systems, D 89143, Blaubeuren, Germany
- [3.72] Barker D.B., Dasgupta A., Pecht M., "Printed-wiring-board solder-joint fatigue-life calculation under thermal and vibration loading", *Proc. Ann. Rel. & Maint. Symp.*, 1991, pp. 451-59.
- [3.73] Birolini A. et al., "Exp. Ergebnisse zur Q. & Z. der SMT mit Pitch 0.5 mm", *me*, (1995)5, pp. 28-33.
- [3.74] Darveause R. et al., "Constitutive relations for tin-based solder joints.", *IEEE Trans. Compon., Pack., and Manuf. Technol.*, 15 (1992) 6, pp. 1013-24.
- [3.75] Engelmaier, W., "Environmental stress screening and use environments - their impact on solder joint and plated-through-hole rel.", *Proc. Int. Electronics Pack. Conf.*, Marlborough MA, 1990, pp. 388-93.
- [3.76] ETH Zurich, Rel. Lab., *Reports P3-P18: Qualification Tests on 7 Telecom. Equipment*, 1989-91.
- [3.77] Fenech A. et al., "Determination of thermomechanical behavior of microel. packaging based on microstructural analysis", *Proc. ESREF*" 94, Glasgow, 1994, pp. 405-10.
- [3.78] Frear D.R. (Ed.), *The Mechanics of Solder Alloy Interconnections*, 1994, Van Nostrand Reinh, NY.
- [3.79] Grossmann G., *Zuv. von Weichlotstellen*, 1993, Rep. L29, ETH Zurich, Rel. Lab.; *Produktion und Prüfung von Testprints der SMT Fine Pitch*, 1996, Rep. K12, ETH Zurich, Rel. Lab.; "Metallurgical consid. for acc. testing of el. equip.", *IEEE Trans. Comp., Pack. & Manuf. Technol.*, 20(1997)2, pp. 213-18; "The deformation of Sn62Pb36Ag2 and its impl. on the design of thermal cycling for el. assemblies", *IEEE Trans. CMPT*, 22(1999)1, pp. 71-79; "Accelerated testing methodology for lead-free solder" in *Lead-Free Solder Interconnect Rel.*, ed. D. Shangguan, 2005, ASM Int., Ohio; - et al., "Proper. of thin layers of Sn62Pb36Ag2", *Proc. 1995 IEMT Symp.*, pp. 502-07; "Metallurgical consid. for accel. testing of el. equip.", *Proc. 1996 IEMT Symp.*, pp. 298-304; "Lifetime ass. of soft sold. joints on the base of the behav. of Sn62Pb36Ag2", *Proc. 1997 IEMT Symp.*, pp. 256-63; "Results of comp. rel. tests on lead-free solder alloys", *Proc 2002 ECTC Symp.*, 1232-37; Eds. *The ELFNET Book on Failure Mech., Testing Methods & Quality issues of Lead-Free Solder Interconnects*, 2011, Springer, Berlin.
- [3.80] Held M. et al., "Fast power cycling test for IGBT's in traction appl.", *Proc. PDES*, 1997, pp. 425-30.

- [3.81] Heiduschke K., "The logarithmic strain space description", *Int. J. Solids Structures*, 32 (1995), pp. 1047-62 and 33(1996) pp. 747-60; *Kontinuumsmech. und Finite Element Mod.* (URMEL), 1996, Report K11, ETH Zurich, Rel. Lab.; - et al., "Modeling fatigue cracks with spatial shape", *Proc. EuPac '94*, pp. 16-23; "Damage and micro-crack evolution in SMT joints", *Proc. EuPac '96*, pp. 112-15.
- [3.82] IEC 62137: *Test Methods for SM Boards of area array type package*, -1-1 to -1-5 (2007-09); *SM Solder Joints*, -3 (2011): *Guidance of Environmental & Endurance Tests Methods for Solder Joints*.
- [3.83] IEEE, Special issue on: Plastic Encapsulated Microcircuits, *IEEE Trans. Rel.*, 42(1993)4.
- [3.84] IPC-SM-785, *Guidelines for Accelerated Rel. Testing of Surface Mount Solder Attachments*, 1992; IPC/JEDEC J-STD-020C, *Moisture/Reflow Sensitivity Classif. of Nonhermetic Solid State SMD*, 2004.
- [3.85] Jacob P. et al., "Reliability Testing and Analysis of IGBT Power Semiconductor Modules", *Proc. ISTFA'94*, Los Angeles CA 1994, pp. 319-25.
- [3.86] Jud P. et al., "Local creep in SNAg3.8Cu0.7 lead-free solder", *J. Electr. Mater.*, 34(2005)9, pp. 1206-14.
- [3.87] Pecht M., (Ed.) *Handbook of Electronic Package Design*, 1991, Dekker, NY; - et al., "Are components still the major problem?", *IEEE Trans. Comp., Hybr. & Manuf. Technol.*, 15(1992), pp. 1160-64.
- [3.88] Philofsky E., "Design limits when using Au-Al bonds", *Proc. Int. Rel. Phys. Symp.*, 1986, pp. 114-19.
- [3.89] Reed J.R., *Risk Assessment of Printed Wiring Board Alternative Finishes*, 2000, Raytheon, Austin TX.
- [3.90] Shangguan D. (Ed.), *Lead-Free Solder Interconnect Reliability*, 2005, ASM International, Ohio.
- [3.91] Tullmin M. et al., "Corrosion of metallic materials", *IEEE Trans. Rel.*, 44 (1995)2, pp. 271-78.
- [3.92] Weber L., *Material- & Schädigungsmod. bei Pb-Zn-Ag-Lot*, 1996, Rep. K10, ETH Zurich, Rel. Lab.; *Creep-fatigue behavior of eutectic Sn62Pb36Ag2 solder*, 1997, Ph. D. Thesis 12251, ETH Zurich.
- [3.93] Wu W. et al., " dv/dt induced latching failure in IGBT's", *Proc. Int. Rel. Phys. Symp.*, 1994, pp. 420-24; "Investigation on the long term rel. of power IGBT modules", *Proc. ISPSD 95*, 1995, pp. 443-48.

see also [5.4, 5.18, 8.21-8.35]

4 Maintainability Analysis

- [4.0] Belzunce F. et al., "Comparison of expected failure times for several replacement policies", *IEEE Trans. Rel.*, 55(2006)4, pp. 400-05.
- [4.1] Berg M., "A proof of optimality for age replacement policies", *J. Appl. Prob.*, 13(1976), pp. 751-59; - et al., "Comparison of age, block & failure repl. policies", *IEEE Trans. Rel.*, 27(1978)1, pp. 25-29.
- [4.2] Birolini A., "Spare parts reservation of components subjected to wear-out or fatigue according to a Weibull disturb.", *Nuclear Eng. & Design*, 27(1974), pp. 293-98; "Basic stochastic models for a cost optim. spare parts provision", *Inv. Paper Ann. Conv. AICE 2000, Univ. Bocconi Milano*, pp. 1-16.
- [4.3] Blanchard B.S. et al., *Maintainability: Principles and Practices*, 1969, MacGraw-Hill, NY; *Logistics Engineering and Management*, 4th Ed., 1991, Prentice Hall, Englewood Cliffs, NJ; *Maintainability: A Key to Effective Serviceability and Maintenance Management*, 1995, Wiley, NY; *Systems Engineering and Analysis*, 3th Ed., 1998, Prentice Hall, Englewood Cliffs, NJ.
- [4.4] Bonivento C. et al., "A framework for reliability analysis of complex diagnostic systems", *Proc. 5th IFAC Symp. on Fault Detection, Supervision & Safety of tech. processes*, 2003, pp. 567-72.
- [4.5] Collett R.E. et al., "Integration of BIT effectiveness with FMECA", *Proc. Ann. Rel. & Maint. Symp.*, 1984, pp. 300-305.
- [4.6] Dersin P. et al., "Selecting test and maintenance strategies to achieve availability target with lowest life-cycle-cost", *Proc. Ann. Rel. & Maint. Symp.*, 2008, pp. 301-06.
- [4.7] Garnero M.A. et al., "Optimization of bearing-inspection intervals", *Proc. Ann. Rel. & Maint. Symp.*, 1998, pp. 332-38.
- [4.8] Glasser G.J., "The age replacement problem", *Technometrics*, 9(1967), pp. 83-91.
- [4.9] Hofstädt H. et al., "Qualitative testability analysis and hierarchical test pattern generation: A new approach to design for testability", *Proc. Int. Test. Conf.*, 1987, pp. 538-46.
- [4.10] Hughes G.F., et al., "Improved disk-driver failure warnings", *IEEE Trans. Rel.*, 51(2002)3, pp. 350-57.
- [4.11] IEC 60706 (2006): *Guide on Maintainability of Equipment*, -2 (2006): *Requirements*, -3 (2006): *Data Collection*, -5 (2007): *Testability*.
- [4.12] IEEE Special issues on: Maintainability, *Trans. Rel.*, 30(1981)3; Fault-tolerant computing, *Computer*, 17(1984)8, *Trans. Rel.*, 36(1987)2, *Trans. Comp.*, 39(1990)4 & 41(1992)5; Fault tolerance in VLSI, *Proc. of the IEEE*, 74(1986)5; Testing, *Trans. Ind. El.*, 36(1989)2; Software tools for hardware test., *Computer*, 22(1989)4; Fault-tolerant systems, *Computer*, 23(1990)7.

- [4.13] IEEE-STD 1149.1, .4, .7, .8 (2001-2012): *Test Access Part and Boundary-Scan Architecture*.
- [4.14] Kuo W. et al., *Maintenance Theory of Reliability*, 2005, Springer, London.
- [4.15] Lee K.W. et al., "A literature survey of the human reliability component in a man-machine system", *IEEE Trans. Rel.*, 37(1988), pp. 24-34.
- [4.16] Lee P.A. et al., *Fault Tolerance, Principles and Practice*, 2nd Ed. 1990, Springer, Berlin.
- [4.17] McCluskey E.J., *Logic Design Principles*, 1986, Prentice-Hall, Englewood Cliffs NJ.
- [4.18] MIL-HDBK-470A (1997, Not 2, 2012): *Designing and Developing Maintainable Products & Systems*, -472 (1966, Not 1, 1984): *Maintainability Prediction*, -2165 (1995): *Testability programs*; DoD-HDBK-791F (1988): *Main-tainability Design Techniques* - Metric.
- [4.19] Nakagawa T., *Maintenance Theory of Reliability*, 2005, Springer, London.
- [4.20] Pradhan D.K. (Ed.), *Fault-Tolerant Computing*, Vol.1 & 2, 1986, Prentice-Hall, Englewood Cliffs NJ.
- [4.21] RAC, MKIT: *Maintainability Toolkit*, 2000, RAC, Rome NY (now RIAC, Utica NY).
- [4.22] Redimbo G.R., "Reliability levels for fault-tolerant linear processing using real number correction", *IEE Proc. Comput. Dig. Tech.*, 143(1996)Nov., pp. 355-63.
- [4.23] Retterer B.L. et al., "Maintainability - historical perspective", *IEEE Trans. Rel.*, 33(1984)1, pp. 56-61.
- [4.24] Robach C. et al., "CATA: a c.-aided test anal. syst.", *IEEE Des. & Test Comp. Mag.*, (1984)5, pp. 68-79.
- [4.25] Savir J. et al., "Random pattern testab. of delay faults", *IEEE Trans. Comp.*, 37(1988)3, pp. 291-300.
- [4.26] Schagaev I. "Reliability of malfunction tolerance", *Proc. IMSCIT, 2008*, pp. 733-38; see also UK Patent GB 2448351 (21.09.2011) or <http://www.it-acis.co.uk/files/GB24483518.pdf>.
- [4.27] Simpson W.R. et al., *System Test- and Diagnosis*, 1995, Kluwer Acad. Press, Boston.
- [4.28] VDI 4003 B1.3: *Allg. Forderungen an ein Sicherungsprogramm: Instandhaltbarkeit*, 1983.
- [4.29] Wagner K.D. et al., "Pseudorandom testing", *IEEE Trans. Comp.*, 36(1987)3, pp. 332-43.
- [4.30] Wang H., "A survey of maintenance policies of deteriorating systems", *Europ. J. of Op. Res.*, 139(2002)3, pp. 469-89.
- [4.31] Williams T.W. et al., "Design for testability - a survey", *Proc. IEEE*, 71(1983)1, pp. 98-112; - Ed., *VLSI Testing* (Vol. 5 of Advances in CAD for VLSI), 1986, North Holland, Amsterdam.
- [4.32] Willimann B., *Optimale Auslegung Logistik kompl. Systeme*, 1993, Ph.D. Thesis 10313, ETH Zurich.
see also [5.21-5.32, 6.82, 6.86]

5 Design Guidelines for Reliability, Maintainability, and Software Quality

Reliability

- [5.0] AMCP 706-196, *Engineering Design HDBK: Design for Reliability*, 1976, US Army Materiel Command, Alexandria VA; see also 706-197,....-200.
- [5.1] Boxleitner W., "Electrostatic Discharge" in *Electronic Equip.*, 1989, IEEE Press, Piscataway NJ.
- [5.2] Catrysse J., "PCB & syst. design under EMC constr.", *Proc. 11th Int. Zurich EMC Symp.*, 1995, pp. 47-58.
- [5.3] Deutsch A., "Electrical characteristics of interconnections for high-performance systems", *Proc. IEEE*, 86(1998)2, pp. 315-55.
- [5.4] Gallo A.A. et al., "Popcorning: A failure mechanism in plastic-encapsulated microcircuits", *IEEE Trans. Rel.*, 44(1995)3, pp. 362-67.
- [5.5] Gardner J.R., "The appropriateness of plastic encapsulated microcircuits in a specific wooden-round application", *IEEE Trans. Rel.*, 45(1996)1, pp. 10-17.
- [5.6] Goedbloed J.J., *Electromagnetic Compatibility*, 1992, Prentice Hall, NY.
- [5.7] Haseloff E., *Was nicht im Datenblatt steht*, 1992, Appl.-Bericht EB 192, Texas Instruments, Freising; "Entwicklungsrichtlinien für schnelle Logikschaltungen und Systemen", *Proc. ETH/IEEE Conf. on Design Rules for Rel., EMC, Maint., Soft. Qual.*, 1993, ETH Zurich, Rel. Lab., pp. 5.1-17.
- [5.8] Hellström S., *ESD-The Scourge of Electronics*, 1998, Springer, Berlin.
- [5.9] Hirschi W., "EMV gerechte Auslegung elektron. Geräte", *Bull. SEV/VSE*, 83(1992)11, pp. 25-29.
- [5.10] *IEEE Trans. Rel.* Special issue on: Design for reliability, 40(1991)3 and 44(1995)2; Plastic encaps. microcircuits, 42(1993)4.
- [5.11] IEEE-STD 1100-2005: *IEEE Recom. Practice for Powering and Grounding Sensitive El. Equip.*
- [5.12] IPC, ANSI/IPC-SM-782: *Surface Mount Land Patterns (Config. and Design Rules)*, 1987.
- [5.13] Mannone P., "Careful design methods to prevent CMOS latch-up", *EDN*, Jan. 26, 1984, 6 pp.
- [5.14] MIL-HDBK-338B (1998): *Electronic Reliability Design Handbook*.
- [5.15] Pecht M.G. et al., "Thermal rel. manag. in PCB des.", *Proc. Ann. Rel. & Maint. Symp.*, 1987, pp.312-15.

- [5.16] RAC, SOAR-6: *ESD Control in the Manuf. Envir.*, 1986; TR-82-172: *Thermal Guide for Rel. Eng.*, 1982; VZAP: *ESD Susceptibility Data*, 1991, RAC, Rome NY (now RIAC, Utica NY).
- [5.17] Sergent J. et al., *Thermal Management Handbook*, 1998, McGraw-Hill, NY.
- [5.18] Solberg V., *Design Guidelines for Surface Mount and Fine Pitch Technol.*, 1996, McGraw-Hill, NY.
- [5.19] Vinson J.E. et al., "Electrostatic discharge in semiconductor devices Protection Techniques", *Proc. IEEE*, 88(2000)12, pp. 1878-900; - " - : An Overview", *Proc. IEEE*, 86(1998)2, pp. 399-418.
- [5.20] White D.R.J., *EMI Control in the Design of Printed Circuit Boards and Backplanes*, 1982, Interf. Control Tech., Gainesville VI.

see also [1.22, 2.11, 2.12, 2.14, 2.15, 3.1-3.93, 8.1-8.14]

Maintainability and Human Aspects

- [5.21] Abramovici M. et al., *Digital System Testing & Testable Design*, 1990, Computer Scient. Press, NY.
- [5.22] Bennetts R.G., *Design of Testable Logic Circuits*, 1984, Addison-Wesley, London.
- [5.23] Benso A. et al., "An on-line BISTRAM architecture with self-repair capability", *IEEE Trans. Rel.*, 51(2002), pp. 123-128.
- [5.24] DoD, AMCP-706-132: *Eng. Design Handbook - Maintenance Eng. Tech.*, 1975; -133: *Maintainability Eng. Theory & Practice*, 1975; DoD-HDBK-791 (AM): *Maintainability Design Tech.* - Metric, 1988.
- [5.25] Fuhrman C. et al., *Fault Coverage in Fault Tolerant Syst.*, Tech. Rep. 95/109, EPFL Lausanne, 1995.
- [5.26] Lala K.P., *Fault Tolerant & Fault Testable Hardware Design*, 1985, Prentice-Hall, Engl. Cliffs NJ.
- [5.27] Maunder C., *The Board Designer's Guide to Testable Logic Circuits*, 1992, Addison-Wesley, Reading MA; A universal framework for manag. Built-In Test, *Proc. Int. Test Conf.*, Paris 1995, 8 pp.
- [5.28] MIL-HDBK-470A (1997, Not2, 2012), *Designing and Developing Maintainable Products & Systems*, Vol. II: *Design Guidelines*; DoD-HDBK-791F (1988): *Maintainability Design Techniques* - Metric.
- [5.29] Richards D.W. et al., "Smart BIT - an approach to better system-level built-in test", *Proc. Ann. Rel. & Maint. Symp.*, 1987, pp. 31-34.
- [5.30] Robinson G. et al., "Interconnect testing of boards with partial boundary-scan", *Proc. Int. Test Conf.*, 1990, paper 27.3.
- [5.31] Sinanoglu O. et al., "Test power reduction through computationally efficient, decoupled scan chain modifications", *IEEE Trans. Rel.*, 54(2005)2, pp. 215-23.
- [5.32] Ye N., "The presentation of knowledge and state-information for system fault diagnosis", *IEEE Trans. Rel.*, 45(1996)4, pp. 638-45.

see also [4.5, 4.7, 4.9-4.13, 4.18, 4.21]

Software Quality

- [5.41] ACM Special issues on: Software Testing, *Commun. of the ACM*, 31(1988)6; Software Quality, *Commun. of the ACM*, 36(1993)11.
- [5.42] Aggarwal K.K. et al., "An integrated measure of software maintainability", *Proc. Ann. Rel. & Maint. Symp.*, 2002, pp. 235-41.
- [5.43] Avresky D. et al., "Fault injection for formal test. of fault tolerance", *IEEE Trans. Rel.*, 45(1996)3, pp. 443-55.
- [5.44] Braude E.J., (Ed.), *Software Engineering: Selected Readings*, 2000, IEEE Press, Piscataway NJ.
- [5.45] Brocklehurst S. et al., "Recalibrating soft. rel. models", *IEEE Trans. Soft. Eng.*, 16(1990)4, pp. 458-69.
- [5.46] BWB, *Software-Entwicklungsstandard der BWB - Vorgehensmodell*, 1991.
- [5.47] Chen M-H, et al., "Effect of testing techniques on software rel. estimates using a time domain model", *IEEE Trans. Rel.*, 44(1995)1, pp. 97-103.
- [5.48] Chillier R., "What is software failure?", *IEEE Trans. Rel.*, 45(1996)3, pp. 354-55.
- [5.49] Costa E.O., et al., al., "Exploring genetic programming and Boosting techniques to model software reliability", *IEEE Trans. Rel.*, 56(2007)3, pp. 422-34.
- [5.50] Deconick G. et al., "The EFTOS approach to dependability in embedded supercomputing", *IEEE Trans. Rel.*, 51(2002)1, pp. 76-90.
- [5.51] Deriennic H., et al., "Use of failure-intensity models in the software-validation phase for telecommunications", *IEEE Trans. Rel.*, 44(1995)4, pp. 658-65.
- [5.52] ESA PSS-05-04: *Guide to the Software Architect*, 1992; -05: *Detailed Design and Prod.*, 1992; -08: *Project Management*, 1994; -09: *Configuration Manag.*, 1992; -11: *Quality Assurance*, 1993.
- [5.53] Fakhre-Zakeri I. et al., "Mixture models for reliability of software with imperfect debugging", *IEEE Trans. Rel.*, 44(1995)1, pp. 104-13.

- [5.54] Fenton N. et al., *Software Reliability and Metrics*, 1991, Elsevier, London.
- [5.55] Garzia M. R., "Assessing software rel. from the customer's perspective", *Proc. ISAS 2006*, and in Kanoun K. et al. Ed., *Dependability Benchmarking for Computer Systems*, 2008, Wiley, NY.
- [5.56] Grady R., "Practical results from measur. soft. quality", *Commun. of the ACM*, 36(1993)11, pp. 62-68.
- [5.57] Herrmann D.S. et al., "The bridge between hardware, software, and system safety and reliability", *Proc. Ann. Rel. & Maint. Symp.*, 1999, pp. 396-402.
- [5.58] Hou R-H, et al., "Optimal release policy for hypergeometric distribution software-reliability growth model", *IEEE Trans. Rel.*, 45(1996)4, pp. 646-51.
- [5.59] Huang C-Y, et al., "Analysis of incorporating logistic testing-effort function into software reliability modeling", *IEEE Trans. Rel.*, 51(2002)3, pp. 261-70.
- [5.60] IEC 62628 (2012): *Guidance on Software Aspects of Dependability*.
- [5.61] IEEE-STD-828-2012: *Configuration Manag. in Systems and Software Eng.*, -1012-2012: *System and Software verification and Validation*, -1016-2009: *Software Design*, -1028-2008: *Software Review and Audits*; -1061-1968: *Software Quality Metrics*, -14102-2010: *Guidelines for the Evaluation and Selection of CASE Tools*; see also [A2.8] and Tab. A2.1.
- [5.62] ISO/IEC 90003:2004: *Guidelines for Appl. of ISO 9001:2000 to Computer Software*; 12207:2008: *Software Life-Cycle Processes*; 29119-1 to -5 (draft): *Software Testing*; see also Tab. A2.1.
- [5.63] Kline M.B., "Software and Hardware R&M - what are the differences?", *Proc. Ann. Rel. & Maint. Symp.*, 1980, pp. 179-84.
- [5.64] Kumar R. et al., "Neural-network techniques for software-quality evaluation", *Proc. Ann. Rel. & Maint. Symp.*, 1998, pp. 155-60.
- [5.65] Lanning D.L. et al., "Fault severity in models of fault-correction activity", "An empirical model of enhancement-induced defect activity in software", "The impact of software enhancement on software reliability", *IEEE Trans. Rel.*, 44(1995)4, pp. 666-82.
- [5.66] Le Traon Y. et al., "Efficient object-oriented integration and regression testing", *IEEE Trans. Rel.*, 49(2000)1, pp. 12-25.
- [5.67] Leveson N.G., "Software safety in computer-controlled systems", *Computer*, (1984)2, pp. 48-55; "Software safety: why, what, and how", *ACM Computing Surveys*, 18(1986)2, pp. 125-63.
- [5.68] Littlewood B. et al., "The risk of software". *Scient. Amer.*, 1992, pp. 38-43; "Validation of ultrahigh dependability for software-based syst", *Commun. of the ACM*, 36(1993)11, pp. 69-80; Littlewood B., "Evaluation of software reliability - achievements and limitations", *Proc. ETH/IEEE Int. Symp. on Rel. Eng. 2'000*, ETH Zurich, Rel. Lab., Oct. 17, 1996, 22 pp.
- [5.69] Lloyd C. et al., "Estimating the number of faults: Efficiency of removal, recapture, and seeding", *IEEE Trans. Rel.*, 48(1999)4, pp. 369-76.
- [5.70] Lyu M.R. Ed., *Handbook of Software Rel. Eng.*, 1995, IEEE Comp. Soc. Press, Piscataway NJ
- [5.71] Musa J.D., *Software Reliability Engineering*, 2004, Author House, Bloomington; "An overview of software rel. engineering" and "The operational profile", in Özekici S., Ed.: *Reliability and Maintenance of Complex Systems*, 1996, Springer, Berlin.
- [5.72] Parnas D.L. et al., "Evaluation of safety-critical software", *Commun. ACM*, 33(1990)6, pp. 636-48.
- [5.73] Pham H., *System Software Reliability*, 2007, Springer, London.
- [5.74] Pflieger S.L., "Measuring software reliability", *IEEE Spectrum*, Aug. 1992, pp. 56-60.
- [5.75] Reifer D.J., "Software Failure Modes and Effects Anal.", *IEEE Trans. Rel.*, 28(1979)3, pp. 247-49.
- [5.76] SAQ, 10300: *Software Qualität.s. & CASE*, 1995; 10301: *HDBK Beschaffung von Software*, 1996; 10302: *HDBK Audits im Soft.-Bereich*, 1996; 10303: *Grundlagen zum Umgang mit Soft. Probl.* 1997.
- [5.77] Schneidewind N.F., "Rel. modeling for safety-critical soft.", *IEEE Trans. Rel.*, 46(1997)1, pp. 88-98.
- [5.78] Singpurwalla N.D., "The failure rate of software: does it exist?", *IEEE Trans. Rel.*, 44(1995)3, pp. 463-69; - et al., "Assessing the rel. of software", in Özekici S., Ed.: *Rel. and Maint. of Complex Systems*, 1996, Springer, Berlin, pp. 345-367; - et al., *Statistical Methods in Rel. Eng.* 1999, Springer, NY.
- [5.79] Stankovic J.A., "A serious problem for next-generation system", *Computer*, 21(1988)10, pp. 10-19.
- [5.80] Teng X. et al., "A software-reliability growth model for n-version programming systems", *IEEE Trans. Rel.*, 51(2002)3, pp. 311-21; - et al., "Reliability modeling of hardware and software interactions, and its applications", *IEEE Trans. Rel.*, 55(2006)4, pp. 571-77.
- [5.81] USAF, "Air Force Weapon System Software Manag. Guidebook", 2008, SAF Acq. Center of Ex. Webseite.
- [5.82] Wallace D. et al., "An analysis of selected software safety Std.", *IEEE AES Mag.*, 1992, pp. 3-14.
- [5.83] Wei Y., "Do software reliability prediction models serve their intended purpose?", in *IEEE Rel. Soc. 2010 Tech. Rep.*; Improve the prediction accuracy of software rel. growth models, *IEEE Int. Symp. on Soft. Rel Eng. (ISSRE)*, 2010.

see also [1.13, 2.8, 6.23, A2.8]

6 Reliability and Availability of Repairable Equipment and Systems

- [6.0] Ajmone-Marsan M. et al., "A class of general stochastic Petri nets for performance ev. of multiproc. systems", *ACM Trans. Comp. Syst.*, 2(1984)2, pp. 93-122; *Performance Models of Multiprocessor Systems*, 1986, MIT Press; *Modeling with Generalized Stochastic Petri Nets*, 1995, Wiley, NY.
- [6.1] Ascher H., "Evaluation of repairable system rel. using the bad-as-old concept", *IEEE Trans. Rel.*, 17(1968)2, pp. 103-10; - et al., *Repairable Systems Reliability*, 1984, Dekker, NY (new Ed. in prep.).
- [6.2] Beaudry D., "Performance-related rel. meas. for comp. syst.", *IEEE Trans. Comp.*, 27(1978), pp. 540-7.
- [6.3] Beichelt F., et al., *Zuverlässigkeit & Instandhaltung - Math. Methoden*, 1983, Technik, Berlin; Beichelt F., *Zuverlässigkeits- und Instandhaltbarkeitstheorie*, 1993, Teubner, Stuttgart.
- [6.4] Billinton R. et al., *Reliability Evaluation of Power Systems*, 1996, Plenum Press, NY; *Reliability Assessment of Electric Power Systems using Monte Carlo Methods*, 1994, Plenum Press, NY.
- [6.5] Birolini A., "Comments on Renewal theoretic aspects of two-unit redundant systems", *IEEE Trans. Rel.*, 21(1972)2, pp. 122-23; "Generalization of the expressions for rel. and availability of rep. items", *Proc. 2. Int. Conf. on Struct. Mech. in Reactor Techn.*, Berlin: 1973, Vol. VI, pp. 1-16; "Some appl. of regenerative stochastic processes to reliability theory - part two: Reliability and availability of 2-item redundant systems", *IEEE Trans. Rel.*, 24(1975)5, pp. 336-40; *On the Use of Stochastic Processes in Modeling Reliability Problems* (Habil. Thesis ETH), 1985, Springer, Berlin (Lect. Notes Ec. & Math. Syst. Nr. 252); *Qualität & Zuverlässigkeit technischer Systeme*, 1985, 1988, 1991, 1997, Springer, Berlin.
- [6.6] Bobbio A., "System modeling with Petri nets" in Colombo G. et al. (eds.), *System Rel Assessment*, 1990, ECSC, EEC, EAEC, Brussels; "Stoch. reward models for performance & dependab. analysis", *J. of Commun.*, 43(1992)1, pp. 27-35.
- [6.7] Bondavalli A. et al., "Dependability modeling and evaluation of multiple-phased systems using DEEM", *IEEE Trans. Rel.*, 53(2004)4, pp. 509-22.
- [6.8] Choi, H. et al., "Markov regenerative stochastic Petri nets", *Performance Ev.*, 20(1994), pp. 337-57.
- [6.9] Ciardo G. et al., "A decomposition approach for stochastic reward net models", *Performance Eval.*, 18(1993)4, pp. 37-59.
- [6.10] Costes A. et al., "Reliability and availability models for maintained systems featuring hardware failures and design faults", *IEEE Trans. Comp.*, 27(1978)6, pp. 548-60.
- [6.11] Crow L.H., "A method for achieving an enhanced mission capability", *Proc. Ann. Rel. & Maint. Symp.*, 2002, pp. 153-57.
- [6.12] Dersin P. et al., "Mass transit system service quality: Trade-off analysis on reliability, maintainability and logistics", *Proc. Ann. Rel. & Maint. Symp.*, 1995, pp. 515-28; "
- [6.13] Dubi A., *Monte Carlo Applications in System Engineering*, 2000, Wiley, NY.
- [6.14] Endrenyi J., "Three state models in power system reliability evaluations", *IEEE Trans. Power Syst.*, 90(1971), pp. 1909-16; *Reliability Modeling in Power Systems*, 1978, Wiley, NY.
- [6.15] Finkelstein M., "Multiple availability on stoch. demand", *IEEE Trans. Rel.*, 48(1999)1, pp. 19-24; - et al., "Laplace-tr. & fast-repair approx. for mult. avail.", *IEEE Trans. Rel.*, 51(2002)2, pp. 168-76.
- [6.16] Fitzgerald K. et al., "Rel. model. & ass. of star-graph networks", *IEEE Trans. Rel.*, 51(2002)1, pp. 49-57.
- [6.17] Gaede K.W., *Zuverlässigkeit Mathematische Modelle*, 1977, Hanser, Munich.
- [6.18] Garriga G., "Repair proc. fundamentals & comput.", *Rep. EUR-5232e*, Nucl. Res. Center Ispra, 1974.
- [6.19] Gnedenko B.V. et al., *Mathematical Methods of Reliability Theory*, 1969, Academic, NY (1968, Akademie, Berlin); *Probabilistic Reliability Engineering*, 1995, Wiley, NY.
- [6.20] Guenzi G. et al., "Stochastic processes and reliability: Applications to repairable systems", *Atti Giornata AICE 1999, Univ. Bocconi Milano*, pp. 69-119; Guenzi G., private commun., 2002.
- [6.21] Hall J.D. et al., "Frequency and duration methods for power system reliability calculation", *IEEE Trans. Power Syst.*, 87(1968)9, pp. 1787-96, see also 88(1969)4, pp. 107-20.
- [6.22] IEEE-STD 493-2007: *IEEE Recomm. Practice for Design of Reliable Industrial & Com. Power Syst.*
- [6.23] Kanoun K. et al., "Fault-tolerant system dependability: Explicit modeling of hardware and software component-interactions", *IEEE Trans. Rel.*, 49(2000)4, pp. 363-75.
- [6.24] Kim K. et al., "Phased-mission system rel. under Markov env.", *IEEE Trans. Rel.*, 43(1994)2, pp. 301-09.
- [6.25] Kovalenko I. et al., "Uniform exponential bounds for the availability of a repairable system", in *Exploring Stochastic laws, Homage to V.S. Korolyuk*, 1995, VSP, Utrecht, pp. 233-42.
- [6.26] Kreimer J., "Effectiveness-analysis of real-time data acquisition and processing multichannel syst.", *IEEE Trans. Rel.*, 51(2002)1, pp. 91-99.
- [6.27] Kullstam A., "Availability, MTBF and MTTR for repairable M-out-of-N Systems", *IEEE Trans. Rel.*, 30(1981)4, pp. 393-94.
- [6.28] Lee K.V., "Stochastic model for random request availability", *IEEE Trans. Rel.*, 49(2000)1, pp. 80-84.

- [6.29] MacLaren M.D. et al., "Uniform random number generators", *J. ACM*, 12(1965), pp. 83-89.
- [6.30] Malhotra M. et al., "Power-hierarchy of dependability-model types", *IEEE Trans. Rel.*, 43(1994)3, pp. 493-502; "Dependability mod. using Petri-Nets", *IEEE Trans. Rel.*, 44(1995)3, pp. 428-40 (1996, p.272).
- [6.31] Metropolis N. et al., "The Monte Carlo method", *J. Amer. Stat. Assoc.*, 44(1949), pp. 335-41.
- [6.32] Obal D.W. et al., "Detecting and exploiting symmetry in discrete-state Markov models", *IEEE Trans. Rel.*, 56(2007)4, pp. 643-54.
- [6.33] Ou Y. et al., "Multi-phase reliability analysis for dynamic and static phases", *Proc. Ann. Rel. & Maint. Symp.*, 2002, pp. 404-10; "Modular solution of dynamic multi-phase systems", *IEEE Trans. Rel.*, 53(2004)4, pp. 499-508.
- [6.34] Pagès M.C., *System Reliability Evaluation and Prediction in Engineering*, 1986, Springer, Berlin.
- [6.35] Petri C.A., *Kommunikation mit Automaten*, Ph.D. thesis University of Bonn, 1962 (also as *Communication with Automata*, RADC TR-65-377, 1966).
- [6.36] Pullum L.L. et al., "Fault tree models for the analysis of complex computer-based systems", *Proc. Ann. Rel. & Maint. Symp.*, 1996, pp. 200-07.
- [6.37] Rai S. et al. (Ed.), *Advances in Distributed Systems Reliability and Distributed Computing Network Reliability*, 1990, IEEE Press, Piscataway NJ.
- [6.38] Ren Y. et al., "Design reliable systems using static & dynamic fault trees", *IEEE Trans. Rel.*, 47(1998)3, pp. 234-44.
- [6.39] Schneeweiss W., *Petri Nets for Rel. Modeling*, 1999, LiLoLe, Hagen; "Tutorial: Petri nets as a graphical description medium for many rel. scenarios", *IEEE Trans. Rel.*, 50(2001)2, pp. 159-64; *Petri Net Picture Book*, 2004, LiLoLe, Hagen; *The Modeling World of Rel. & Safety Eng.*, 2005, LiLoLe, Hagen; *Renewal Processes for Reliability Modeling*, 2009, LiLoLe, Hagen.
- [6.40] Shooman M., "Simplification of Markov models by state merging", *Proc. Ann. Rel. & Maint. Symp.*, 1987, pp. 159-64.
- [6.41] Smotherman M. et al., "A nonhomogeneous Markov model for phased-mission reliability analysis", *IEEE Trans. Rel.*, 38(1989)5, pp. 585-90.
- [6.42] Turconi G. et al., "A design tool for fault tolerant systems", *Proc. Ann. Rel. & Maint. Symp.*, 2000, pp. 317-26.
- [6.43] Ushakov I.A. et al., *Handbook of Reliability Engineering*, 1994, Wiley, NY.
- [6.44] Villemeur A., *Reliability, Availability, Maintainability & Safety Assessment*, Vol. 1, 1992, Wiley, NY.
- [6.45] Walzer M. et al., *The modeling world of reliability / safety engineering*, 2005, LiLoLe, Hagen.
- [6.46] Xing L., "Reliability analysis of phased-mission systems with imperfect fault coverage and common-cause failures", *IEEE Trans. Rel.*, 56(2007)1, pp. 58-68.
- [6.47] Yin L. et al., "Uncertainty analysis in rel. modeling", *Proc. Ann. Rel. & Maint. Symp.*, 2001, pp. 229-34; "Application of semi-Markov processes and CTMC to evaluation of UPS system availability", *Proc. Ann. Rel. & Maint. Symp.*, 2002, pp. 584-91.
- [6.48] Zheng Z. et al., "A study on a single-unit Markov repairable system with repair time omission", *IEEE Trans. Rel.*, 55(2006)2, pp. 182-88.
- [6.49] Zhihua T. et al., "BDD-based rel. analysis of phased-mission systems with multimode failures", *IEEE Trans. Rel.*, 55(2006)2, pp. 350-60.
- see also [2.1-2.20, 2.31-2.49, 2.85, A2.5 (61165), A7.2, A7.4, A7.10, A7.20, A7.26-A7.30]*

Networks Reliability & Availability

- [6.51] Albert R. et al., "Statistical mech. of complex networks", *Rev. Modern Physics*, 74(2002)1, pp. 47-97.
- [6.52] Aiello W. et al., "Augmented ring networks", *IEEE Trans. Par. & Distrib. Sys.*, 12(2001)6, pp. 598-609.
- [6.53] Bobbio A., "Struttura delle reti in un mondo interconnesso", *Mondo Dig.*, 20(2006)Dic, pp. 3-18; - et al., "Binary decision diagrams in network rel. analysis" *Proc. DCDS07, 2007*, pp. 57-62; "A tool for network rel. analysis", in *Int. Conf. on Computer Safety, Rel., and Security, SAFECOMP 2007*, Ed. Saglietti F. et al., 2007, Springer, Berlin, pp. 417-22; "Reliability and quality of services in weighted probabilistic networks using ADD", *Proc. Ann. Rel. & Maint. Symp.*, 2009, pp. 19-24.
- [6.54] Colbourn C.J., *The Combinatorics of Network Reliability*, 1987, Oxford Univ. Press; - et al., *Network Reliability a Computational Environment*, 1995, CRC Press, Boca Raton FL.
- [6.55] Frank H. et al., *Communication, Transmission, & Transp. Networks*, 1971, Addison-Wesley, Reading MA.
- [6.56] Jane C.C. et al., "A practical algorithm for computing multi-state two-terminal reliability", *IEEE Trans. Rel.*, 57(2008)2, pp. 295-302.

- [6.57] Kuo S.Y. et al., "Efficient and exact reliability evaluation for networks with imperfect vertices", *IEEE Trans. Rel.*, 56(2007)2, pp. 288-300.
- [6.58] Lee S.M. et al., "Sequential capacity determination of subnetworks in network performance analysis", *IEEE Trans. Rel.*, 53(2004)4, pp. 481-86.
- [6.59] Lin Y.-K., "Reliability of a stochastic-flow network with unreliable branches & nodes under budget constraints", *IEEE Trans. Rel.*, 53(2004)3, pp. 381-87.
- [6.60] Manzi E. et al., "Fishman's sampling plan for comp. network rel.", *IEEE Trans. Rel.*, 50(2001)1, pp. 41-6.
- [6.61] Moskowitz F., "Analysis of redundancy networks", *AIEE Trans. Comm. El.*, 35(1958), pp. 627-32.
- [6.62] Pan Y., "Fault tolerance in the block-shift network", *IEEE Trans. Rel.*, 50(2001)1, pp. 85-91.
- [6.63] Page L.B. et al., "Reliability polynomials and link importance in networks", *IEEE Trans. Rel.*, 43(1994)1, pp. 51-58; see also: Traldi L., "Commentary on", *IEEE Trans. Rel.*, 49(2000)3, p. 322.
- [6.64] Satisation S. et al., "An algorithm for lower reliability bounds of multistate two-terminal networks", *IEEE Trans. Rel.*, 55(2006)2, pp. 199-206.
- [6.65] Shooman M.L., *Reliability of Computer Systems and Networks*, 2002, Wiley, NY.
- [6.66] Shier D.R., *Network Reliability and Algebraic Structures*, 1991, Oxford Univ. Press, NY.
- [6.67] Tenenbaum A.S., *Computer Networks*, 3d Ed., 1996, Prentice-Hall, Englewood Cliffs NJ.
- [6.68] Tu H.Y. et al., "Families of optimal fault-tolerant multiple-bus networks", *IEEE Trans. Par. & Distrib. Sys.*, 12(2001)1, pp. 60-73.
- [6.69] Yeh W.C., "A simple heuristic algorithm for generating all minimal paths", *IEEE Trans. Rel.*, 56(2007)3, pp. 488-94.
- [6.70] Zhou L., *Availability Anal. & Optim. in Optical Transp. Networks*, 2007, Ph.D. Thesis 17191, ETH Zurich.

Human Reliability

- [6.71] Bell J. et al, *Review of Human Rel. Ass. Methods*, RR679, 2009, Health & Safety Exec. UK, www.hse.gov.uk.
- [6.72] Courdier S. et al, "Equipment failures: causes and consequences in endoscopic gynecologic surgery", *J. Minimally Invasive Gynecology*, 16(2009)1, pp. 28-33.
- [6.73] Dhillon B.S., Modeling human errors in repairable systems, *Proc. Ann. Rel. & Maint. Symp.*, 1989, pp. 418-424; *Human Reliability and Error in Transportation Systems*, 2007, Springer, London; *Human Reliability, Error, and Human Factors in Engineering Maintenance*, 2009, CRC Press, NY.
- [6.74] Dougherty E.M. et al, *Human Reliability Analysis*, 1988, Wiley, NY; "Human rel. analysis: where shouldst thou turn?", *Rel. Eng. & System Safety*, 29(1990), pp. 283-299.
- [6.75] Gertman D.L. et al, *The SPAR-H Human Rel. Analysis Method*, NUREG/CR-6883, 2005.
- [6.76] Hollnagel E., *Cognitive Reliability and Error Analysis Method: CREAM*, 1998, Elsevier, London; *The ETTO Principle - Efficiency - Thoroughness - Trade-Off*, 2009, Ashgate, London.
- [6.77] Kirwan B., *A Guide to Practical Human Reliability Assessment*, 1994, Taylor & Francis, London.
- [6.78] LaSala K.P., "Survey of industry human performance reliability practices", *IEEE Rel. Soc. Newsletter*, 36(1990)2, pp. 7-8; Reducing human performance-related risks with REHMS-D, *Proc. Ann. Rel. & Maint. Symp.*, 1999, pp. 288-92; *A Practical Guide to Developing Reliable Human-Machine Systems and Processes*, 2002, RAC, Rome NY (now RIAC, Utica NY).
- [6.79] Lee K.W. et al, "A literature search of the human rel. component in a man-machine system", *IEEE Trans. Rel.*, 37(1988)1, pp. 24-34.
- [6.80] Llory M., *L'accident de la centrale nucléaire de Three Mile Island*, 1999, l'Harmattan, Lyon.
- [6.81] Lydell B.O.Y., "Human rel. methodology: State of the art", *Rel. Eng. & Sys. Safety*, 36(1992), pp. 15-21.
- [6.82] MIL-STD 1472G (2012), *Human Eng.*; MIL-HDBK-759C (1998), *Human Eng. Design Guidelines*, see also DoD HFE TAG (2000): *Human Eng. Design Data Digest* (www.hfetag.com/).
- [6.83] Rasmussen N.C., *WASH 1400, The Reactor Safety Study*, 1975, US Nucl. Reg. Com.; *Methods of Hazard Anal. & Nucl. Safety Eng.*, 1981, MIT; see also Chang R. et al, *SOARCA, 2012*, US Nucl. Reg. Com.
- [6.84] Ribette P., private communication, 2011.
- [6.85] Salvendy G. (Ed.), *Handbook of Human Factors and Ergonomics*, 4th Ed., 2012, Wiley, NJ.
- [6.86] Sanders M.S. et al, *Human Factors in Engineering and Design*, 1987, McGraw-Hill, .NY.
- [6.87] Smith D.J., *The Safety Critical Handbook* 3th Ed., 2010, Elsevier, London.
- [6.88] Spurgin A.J., *Human Reliability Assessment: Theory & Practice*, 2010, CRC Press, NY.
- [6.89] Swain A.D. et al, *HDBK of Human Rel. An. with emp. on nucl. power plant appl.*, NUREG/CR-1278, 1983; Swain A.D., "Human rel. anal.: need, status, trends, limit.", *Rel. Eng. & Sys. Safety*, 29(1990), pp. 301-13.
- [6.90] Wickens C. et al, *An Intr. to Human Factors Eng.*, 2nd Ed., 2004, Pearson Ed. Inc., Upper Saddle River, NJ.

see also [1.3, 1.7, 1.9, 1.21, 1.23, 1.26, 1.28] and http://en.wikipedia.org/wiki/human_reliability

7 Statistical Quality Control and Reliability Tests

Statistical Quality Control

- [7.1] ANSI Z1.1 and Z1.2-1958: *Guide for Quality Control and Control Chart Method of Analyzing Data*, Z1.3-1959: *Control Chart Method of Controlling Quality During Production*.
- [7.2] Chandra M.J., *Statistical Quality Control, 2001*, CRC Press, NY.
- [7.3] IEC 60410 (1973): *Sampling Plans and Procedures for Inspection by Attributes*, see also MIL-STD-105, -414, -1235; DIN 40080, DGQ-SAQ-OeVQ 16-01, ISO 2859.
- [7.4] Sarkadi K. et al., *Mathematical Methods of Statistical Quality Control*, 1974, Academic Press, NY.
- [7.5] SAQ-DGQ-OeVQ, DGQ16-01: *Attributprüfung* 9th Ed. 1986; 16-26: *Meth. zur Ermittlung geeigneter AQL-Werte*. 4rd Ed. 1990; 16-31/-32/-33: *SPC 1/2/3 Stat. Prozesslenkung*, 1990.

Reliability Tests

- [7.10] Arrhenius S. "Über die Reaktionsgeschwindigkeit bei der Inversion von Rhorzucker durch Säuren", Z. Phys.-Ch., 1889, 23pp.
- [7.11] Ascher H.E. et al., "Spurious exponentiality observed when incorrectly fitting a distribution of nonstationary data", *IEEE Trans. Rel.*, 47(1998)4, pp. 451-59; Ascher H., "A set-of-numbers is not a data-set", *IEEE Trans. Rel.*, 48(1999)2, pp. 135-40; see also [6.1].
- [7.12] CEEES: *The Different Type of Tests and their Impact on Product Reliability*, Publ. N°9-2009, ISSN 1104-6341, Confederation of European Environmental Eng. Soc. (www.ceees.org/).
- [7.13] Chan V. et al., "A Failure-Time Model for Infant-Mortality and Wearout Failure Modes", *IEEE Trans. Rel.*, 48(1999)4, pp. 377-87.
- [7.14] Dersin P. et al., "Statistical estimation and demonstration of complex systems availability", *Proc. λμ 15 Conf.*, Lille, France, Oct. 2006, Section 6C, 6 pp.
- [7.15] Evans R.A., "Accelerated testing", *IEEE Trans. Rel.*, 26(1977)3, p. 241 and 40(1991)4, p. 491.
- [7.16] Glen A.G. et al., "Order statistics in goodness-of-fit test.", *IEEE Trans. Rel.*, 50(2001)2, pp. 209-13.
- [7.17] Gnedenko B.V. et al., *Statistical Reliability Engineering*, 1999, Wiley, NY.
- [7.18] Hu J.M. et al., "Rate of failure-mechanisms identification in accelerated testing", *Proc. Ann. Rel. & Maint. Symp.*, 1992, pp. 181-88.
- [7.19] IEC 60319 (1999): *Pres. and Spec. of Rel. Data for El. Comp.*; 60605: *Equip. Rel. Testing*, -2(1994): *Test Cycles*, -4(2001): *Estimation for λ*, -6(2007): *Goodness-of-fit for λ*; 60706: *Maintainability*, -2(2006): *Req.*, -3(2006): *Data Coll.*, -5(2007): *Testability*; 61070 (1991): *Availability Demonstration*; 61123 (1991): *Success Ratio* (supers. 60605-5); 61124 (2012): *λ Demonstration* (supers. 60605-7); 61163-1 &-2 (2006 & 1998): *Screening Assemblies & Comp.*; 61649 (2008): *Weibull Data*; 61650 (1997): *Comparison of two λ*; 61710 (2000): *Goodness-of-fit tests*; 62506 (2013): *Accelerated Tests*.
- [7.20] Khamis I.H. et al., "A new model for step-stress testing", *IEEE Trans. Rel.*, 47(1998)2, pp. 131-34.
- [7.21] Liao C.-M. et al., "Optimal design for step-stress accelerated degradation tests", *IEEE Trans. Rel.*, 55(2006)1, pp. 59-66.
- [7.22] Meeker W.Q. et al., "Pitfalls of accelerated testing", *IEEE Trans. Rel.*, 47(1998)2, pp. 114-18; "Accelerated degradation tests: Modeling and analysis", *Technometrics*, 40(1998)2, pp. 89-99.
- [7.23] MIL-HDBK-470A (1997, Not2, 2012), *Designing & Develop. Maintainable Products & Systems*, see also -HDBK-472 (1966, Not1, 1984); MIL-HDBK-781A (1996): *Rel. Test Methods, Plans, and Environments for Eng., Dev., Qualification & Prod.*, see also IEC 61124 (2012): *λ Demonstration* (supers. 60605-7).
- [7.24] Møltøft J., "Reliability engineering based on field information - the way ahead", *Qual. & Rel. Eng. Int.*, 10(1994)2, pp. 399-409.
- [7.25] Nelson W., *Accelerated Testing*, 1990, Wiley, NY; "A bibliography of accelerated test plans", *IEEE Trans. Rel.*, 54(2005)2, pp. 194-97.
- [7.26] Peck D.S. et al., *Accelerated Testing HDBK*, 1987, Techn. Ass., Portola Valley CA.
- [7.27] Shaked M. et al., "Nonparametric estimation and goodness-of-fit-testing of hypotheses for distributions in accelerated life testing", *IEEE Trans. Rel.*, 31(1982)1, pp. 69-74.
- [7.28] Teng S-L. et al., "A least-squares approach to analyzing life-stress relationship in step-stress accelerated life tests", *IEEE Trans. Rel.*, 51(2002)2, pp. 177-82.
- [7.29] Thomas E.F., "Reliability testing pitfalls", *Proc. Ann. Rel. & Maint. Symp.*, 1974, pp. 78-83.
- [7.30] Viertl R., *Statistical Methods in Accelerated Life Testing*, 1988, Vandenhoeck, Göttingen.
see also [A8.1 - A8.35]

Reliability Growth

- [7.31] Barlow R. et al., "Classical and Bayes approach to ESS- a comparison", *Proc. Ann. Rel. & Maint. Symp.*, 1990, pp. 81-84.
- [7.32] Benton A. et al., "Integrated reliability-growth testing", *Proc. Ann. Rel. & Maint. Symp.*, 1990, pp. 160-66.
- [7.33] Brinkmann R., *Modellierung des Zuverlässigkeitswachstums komplexer, reparierbarer Systeme*, 1997, Ph.D. Thesis 11903, ETH Zurich.
- [7.34] CEEES Publ. Nr 9: *Rel. for a Mature Product from Beginning of Useful Life*, 2009 (ISSN 1104-6341), Confederation of European Environmental Eng. Soc. (www.ceees.org/).
- [7.35] Crow L.H., "On tracking reliability growth", *Proc. Ann. Rel. & Maint. Symp.*, 1975, pp. 438-43; "Methods for assessing rel. growth potential", *Proc. Ann. Rel. & Maint. Symp.*, 1982, pp. 74-78; "Confidence interval procedures for the Weibull process with appl. to rel. growth", *Technometrics* 24(1982)1, pp. 67-72; "On the initial system rel.", *Proc. Ann. Rel. & Maint. Symp.*, 1986, pp. 115-19; "Evaluating the rel. of repairable systems", *Proc. Ann. Rel. & Maint. Symp.*, 1990, pp. 275-79; "Confidence intervals on the reliability of repairable systems", *Proc. Ann. Rel. & Maint. Symp.*, 1993, pp. 126-34; "The extended continuous evaluation rel. growth model", *Proc. Ann. Rel. & Maint. Symp.*, 2010, pp. 275-79; - et al., "Reliability growth estimation with missing data", *Proc. Ann. Rel. & Maint. Symp.*, 1988, pp. 248-53.
- [7.36] Duane J.T., "Learning curve approach to rel. monitoring", *IEEE Trans. Aerosp.*, (1964)2, pp. 563-66.
- [7.37] Evans R.A., "Assuming, of course that", *IEEE Trans. Rel.*, 46(1997)2, p. 161; "Whence come the data?", *IEEE Trans. Rel.*, 46(1997)3, p. 305.
- [7.38] Fries A. et al., "A survey of discrete rel.-growth models", *IEEE Trans. Rel.*, 45(1996)4, pp. 582-604.
- [7.39] IEC 61014 (2003): *Programs for Reliability Growth*; 61164 (2004): *Reliability Growth - Statistical Tests and Estimation Methods*.
- [7.40] IES, *Reliability Growth Processes and Management*, 1989.
- [7.41] Jämskeläinen P., "Rel. growth and Duane learning curves", *IEEE Trans. Rel.*, 31(1982)2, pp. 151-54.
- [7.42] Jayachandran T. et al., "A comparison of rel. growth models", *IEEE Trans. Rel.*, 25(1976)1, pp. 49-51.
- [7.43] Kasouf G. et al., "An integrated missile reliability growth program", *Proc. Ann. Rel. & Maint. Symp.*, 1984, pp. 465-70.
- [7.44] MIL-HDBK-189C (2011): *Reliability Growth Management*.
- [7.45] Rees R.A., "A data-set in not truth", *IEEE Trans. Rel.*, 46(1997)3, p. 306.
- [7.46] RIAC, *Achieving System Reliability Growth Through Robust Design and Test*, 2011, Utica, NY.
- [7.47] VDI 4009 B1.8: *Zuverlässigkeitswachstum bei Systemen*, 1985.
- [7.48] Wong K.L., "A new environmental stress screening theory for electronics", *Proc. Ann. Tech. Meeting IES*, 1989, pp. 218-24; "Demonstrating reliability and reliability growth with data from environmental stress screening", *Proc. Ann. Rel. & Maint. Symp.*, 1990, pp. 47-52.
- [7.49] Yamada S. et al, "Reliability growth models for hardware and software systems based on nonhomogeneous Poisson processes - a survey", *Microel. & Rel.*, 23(1983), pp. 91-112.

see also [5.58, 5.59, 5.68-5.71]

8 Quality and Reliability Assurance During the Production Phase

Production Processes

- [8.1] Desplas E.P., "Rel. in the manufacturing cycle", *Proc. Ann. Rel. & Maint. Symp.*, 1986, pp. 139-44.
- [8.2] DGQ 16-31/-32/-33: *SPC 1/2/3 Statistische Prozesslenkung*, 1990.
- [8.3] Ellis B.N., *Cleaning and Contamination of Electronics Components and Assemblies*, 1986, Electrochemical Publ., Ayr (Scotland).
- [8.4] Hnatek E. R., *Integrated Circuit Quality and Reliability*, 2nd Ed. 1999, Dekker, NY.
- [8.5] Grossmann G., "Contamination of various flux-cleaning combinations on SMT assemblies, *Soldering & SMT*, 22 (1996) Feb., pp. 16-21;
- [8.6] Lea C., *A Scientific Guide to SMT*, 1988, Electrochemical Publ., Ayr (Scotland).
- [8.7] Lenz E., *Automatisiertes Löten elektronischer Baugruppen*, 1985, Siemens, Munich.
- [8.8] Pawling J.F. (Ed.), *Surface Mounted Assemblies*, 1987, Electrochemical Publ., Ayr (Scotland).
- [8.9] Pecht M. et al., *Contamination of Electronic Assemblies*, 2002, CRC Press, NY.

- [8.10] Prasad R.P., *Surface Mount Technology*, 1989, Van Nostrand Reinhold, NY.
- [8.11] Shewhart W.A., "Quality control charts", *Bell Tech. J.*, 5(1926) pp. 593-603.
- [8.12] Stein R.E., *Re-Engineering the Manufacturing System*, 4th Printing 1996, Dekker, NY.
- [8.13] Vardaman J. (Ed.), *Surface Mount Technology: Recent Japanese Dev*, 1993, IEEE Press, Piscataway NJ.
- [8.14] Wassink R.J.K., *Soldering in Electronic*, 2nd Ed. 1989, Electrochemical Publ., Ayr (Scotland).

see also [3.48, 3..89, 3.82, 3.70-3.92]

Test and Screening Strategies

- [8.21] Bennetts R.G., *Introduction to Digital Board Testing*, 1981, Crane Russak, NY.
- [8.22] Birolini A., "Möglichkeiten und Grenzen der Qualifikation, Prüfung und Vorbeh. von ICs", *QZ*, 27(1982)11, pp. 321-326; "Prüfung und Vorbeh. von Bauelementen und Leiterplatten", *VDI-Bericht* Nr. 519, pp. 49-61 1984; "VLSI testing and screening", *Journal of Env. Sciences (IES)*, May/June 1989, pp. 42-48; "Matériels électroniques: stratégies de test et de déverminage", *La Revue des Lab. d'Essais*, 1989 pp. 18-21; – et al.. "Experimentelle Ergebnisse zur Qualität und Zuverlässigkeit der SMT mit Pitch 0.5 mm", *me* (1995) 5, pp. 28-33.
- [8.23] Bullock M., "Designing SMT boards for in-circuit testability", *Proc. Int. Test Conf.*, 1987, pp. 606-13.
- [8.24] De Cristoforo R., "Env. stress screening: lesson learned", *Proc. Ann. Rel. & Maint. Symp.*, 1984, pp.129-33.
- [8.25] Desplas E., "Reliability in the manuf. cycle", *Proc. Ann. Rel. & Maint. Symp.*, 1986, pp. 139-144.
- [8.26] Geniaux B. et al., *Déverminage des matériels électroniques*, 1986, ASTE, Paris; "Climatique et déverminage", *La Revue des Lab. d'Essais*, Sept. 1989, pp. 5-8.
- [8.27] IEC 61163: *Reliability Stress Screening - Part 1* (2006): *Repairable Assemblies*; - *Part 2* (1998): *Electronic Components*.
- [8.28] IES, *Environmental Stress Screening Guideline for Assemblies*, 1988; *Guidelines for Parts*, 1985; *Environmental Test Tailoring*, 1986; *Environmental Stress Screening*, 1989.
- [8.29] Kallis J.M. et al., "Stress screening of electronic modules: Investigation of effects of temp. rate-of-change", *Proc. Ann. Rel. & Maint. Symp.*, 1990, pp. 59-66.
- [8.30] Kim K. et al., "Some considerations on system burn-in", *IEEE Trans. Rel.*, 54(2005)2, pp. 207-14.
- [8.31] Kindig W. et al., "Vibration, random required", *Proc. Ann. Rel. & Maint. Symp.*, 1984, pp. 143-47.
- [8.32] MIL-HDBK-344A (2012): *Environmental Stress Screening of Electronic Equipment*, see also -HDBK-263 -, -2164, and -STD-810, -883.
- [8.33] Parker P. et al., "A study of failures identified during board level environmental stress testing", *IEEE Trans. Comp. and Manuf. Technol.*, 15(1992)3, pp. 1086-92.
- [8.34] Pynn C., *Strategies for Electronics Test*, 1986, McGraw-Hill, NY.
- [8.35] Wennberg S.R. et al., "Cost-effective vibration testing for automotive electronic", *Proc. Ann. Rel. & Maint. Symp.*, 1990, pp. 157-159.

see also [3.31-3.66, 3.70-3.93]

A1 Terms and Definitions

- [A1.1] EOQC (1976): *Glossary of Terms Used in Quality Control*.
- [A1.2] EN 13306 (2010): *Maintenance Terminology*.
- [A1.3] ESA, ECSS-P-001A (Rev. 1, 1997): *Space Product Assurance - Glossary of Terms*.
- [A1.4] IEC 60050-191 (2004, 2nd Ed. in press): *International Electrotechnical Vocabulary - Dependability*.
- [A1.5] IEEE-Std 15026-1-2011, see ISO/IEC 15026-1; IEEE/ISO/IEC 24765-2010: *System and Software Eng. - Vocabulary*.
- [A1.6] ISO 9000 (2005): *Quality Management Systems - Fundamentals & Vocabulary*.
- [A1.7] ISO/IEC 2382-14 (1997): *Infor. Technology Vocabulary: Rel., Maint., Availab.*; 15026-1 (2010, Cor 1 2012): *Systems & Soft. Eng. - Concepts & Vocabulary*; 29119-1 (draft): *Softwt. Testing - Concepts & Vocabulary*.
- [A1.8] MIL-STD-109B (1969): *Quality Assurance Terms and Definitions*; -280A (1969): *Def. of Item Levels and Related Terms*; -721C (1981): *Def. of Terms for Reliability & Maintainability*.
- [A1.9] Parr J.D. et al., "Standardization of reliability / maintainability / availability metrics for US AFSCN common user element", *Proc. Ann. Rel. & Maint. Symp.*, 1999, pp. 13-18.

A2 Quality and Reliability Standards (Customer Requirements, Guidelines)

- [A2.0] ANSI / GEIA-STD-0009 (2008): *Rel. Program Std. for Systems Design, Develop. and Manufacturing*, TechAmerica (see *ITEA*, 29(2008)3, pp. 254-62), see also *Implementation Guide*, JA1000/1 (2012).
- [A2.1] Bensi C., "Dependability Stds: An int. perspective", *Proc. Ann. Rel. & Maint. Symp.*, 1996, pp. 13-6.
- [A2.2] Bellcore TR-NWT-000418 (1997, Issue 4): *Generic Rel. Ass. Req. for Fiber Optic Transport Syst.*
- [A2.3] EN 50126 (1999): *Railway Applications - Spec. and Dem. of RAMS*; 9100-2003: *Quality Manag.*
- [A2.4] ESA ECSS-M-00 (2000): *Space Project Management*, see also -10 to -70; -Q-00 (1996): *Space Product Assurance*, see also -20 (QA), -30 (Dependability), -40 (Safety), -60 (El. Components), -70 (Materials & Processes), -80 (Software); -E-00 (1996): *Space Eng.*, -10 (System Eng.).
- [A2.5] FAA-HDBK-006A (2008): *RAM Handbook*, Fed. Aviation Administration, Washington.
- [A2.6] IEC 60068-1 to -2 (1983-2012): *Environm. Tests*; 60300: *Dependability Manag.*, -1 (2003): *System*, -2 (2004): *Guidelines*, -3-1 to -5, -10 to -12, -14 to -16 (1999-2011) *Appl. Guides*; 60319 (1999): *Spec. of Rel. Data for El. Comp.*; 60410 (1973) *Sampling plans by Attrib.*; 60447 (2004): *Man-Machine-Interf.*; 60605: *Eq. Rel. Test.*, -2 (1994) *Test Cycles*, -4 (2001) λ *Estim.*, -6 (2007) *Goodness-of-fit for λ* ; 60706: *Maintainability*, -2(2006) *Req.*, -3(2006) *Data Coll.*, -5(2007) *Testability*; 60721-1 to -2 (1982-2012): *Env. Cond.*; 60749-1 to -40 (2002-12): *Semicond. Tests*; 60812 (2006): *FMEA*; 61000 -1 to -6 (1990-2012): *EMC*; 61014 & 61164 (2003 & 2004): *Rel. Growth*; 61025 (2006): *FTA*; 61070 (1991): *Availability Dem.*; 61078 (2006): *Rel. Block Diagr.*; 61123 (1991): *Success Ratio* (sup. 60605-5); 61124 (2012): λ *Dem.* (sup. 60605-7); 61160 (2005): *Design Reviews*; 61163-1 & -2 (2006 & 1998): *Screening*; 61165 (2006): *Markov. Tech.*; 61508 -0 to -7 (2005-10): *Funct. Safety*; 61649 (2008): *Weibull Anal.*; 61650 (1997): *Comparison of two λ* ; 61703 (2001, new Ed. in prep.): *Math. expressions*; 61709 (2011): *Failure Rates Models*; 61710 (2000): *Goodness-of-fit tests*; 61882 (2001): *Hazard Studies*; 61907 (2009): *Comm. Networks Dep.*; 62010 (2005): *Maint. Manag.*; 62137-1 (2007-9), -3 (2011): *Tests for SM Boards*; 62198 (2001): *Project Risk Manag.*; 62239 (2012): *Proc. Manag. Avionics*; 62278 (2002), -3(2010): *Railway RAMS*; 62308 (2006): *Rel. Assess.*; TR 62380 (2004): *Rel. Data HDBK*; 62396 (2012): *Proc. Manag. for Avionics*; 62402 (2007): *Obsolescence Manag.*; 62429 (2007): *Screening*; 62502 (2010): *Event Trees*; 62506 (2013): *Accel. Tests*; 62508 (2010): *Human Aspects*; 62550 (in prep.): *Spare Parts*; 62551 (2012): *Petri Nets*; 62628 (2012): *Guidance on Software Aspects of Dependability*.
- [A2.7] IEEE-Std 493-2007: *Rec. Practice for Design of Reliable Ind. & Comm. Power Systems*; -1332-1998: *Standard Reliability Program*; -1413-2010: *Standard Framework for Rel. Prediction of Hardware*; -1413.1-2002: *Guide for Selecting and Using Rel. Predictions based on IEEE 1413*; -1624-2008: *Standard for Organizational Rel. Capability*; -1633-2008: *Recommended Practice on Software Rel.*
- [A2.8] IEEE-Stds in Soft. Eng.: Tab. A2.1 in particular 730-2002: *Quality Ass. Plan*, 828-2012: *Conf. Manag.*; -1012-2012: *System & Software Verif. & Valid.*; -1016-2009: *Software Design*, -1028-2008: *Software Reviews & Audits*; ..-15026, see ISO/IEC 15026; -1633-2008: *Recom. Practice on Software Rel.*
- [A2.9] ISO 9000 (2005): *Quality Management Systems (QMS) - Fund. & Vocabulary*; 9001 (2008/Cor 1:2009): *QMS - Requirements*; 9004 (2009): *QMS - Managing the Sustained Success of an Organization*; 10005 (2005): *QMS - Guidelines for Quality Plans*; 10006 (2003): *QMS - Guidelines for Quality Management in Projects*; 10007 (2003): *QMS - Guidelines for Configuration Manag.*; 10012 (2003): *Measurement Management Systems - Requirements*; 10013 (2001): *Guidelines for Quality Management System Documentation*; 10015 (1999): *QM - Guidelines for Training*; 12207 (2008): *Systems & Software Eng. - Software Life Cycle Process*, see also 90003, 14764, 15026, 15288, 15289, 15940, 16085, 16326, 18018, 24766, and IEC 62628; 14001 (2004/Cor 1:2009): *Environmental Manag. Systems - Req.*; 27005 (2011): *Security Techniques - Risk Management*; ISO/IEC/IEEE 29119-1 to -5 (draft): *Software Testing*.
- [A2.10] MIL-STD--781D, repl. by HDBK-781: *Rel. Testing*, -785B: *Rel. Progr.*, repl. by [A2.0], -810G (2008): *Env. Test Methods*, -882E (2012): *System Safety*, -883H (2010): *Test Proc. for Microel.*, -1472G (2012): *Human Eng.*, -1521B(1995): *Tech. Reviews*, -1629A (1998): *FMECA*, -1686 (1995): *ESD*; MIL-HDBK-189C (2011): *Rel. Growth*, -217G (draft, H planned): *Rel. Pred.*, -263B (1994): *ESD*, -338B (1998): *El. Rel. Des.*, -344A (2012): *ESS*; -454B (2007): *Gen. Guidelines for El. Eq.*, -470A (1997): *Maintainable. Sys.*, -472 (1966): *Maint. Pred.*, -759C (1998): *Human Eng.*, -781A (1996): *Rel. Test.*, -791 (1988): *Maint. Design*, -2164 (1986): *ESS*, -2165 (1995): *Testability*; MIL-Q-9858A: *Quality Req.* (repl. by ISO 9001), H-46855 (1990): *Human Eng.*, -S-19500 (1980): *Gen. Spec. Semicond.*; DoD Dir. 5134.01 (2005). NATO ARMP-1 (2008): *NATO Req. for Reliability and Maintainability* (see also AQAP-1-15).
- [A2.11] Miller J. et al., "Dependability Stds: International coop.", *Proc. Ann. Rel. & Maint. Symp.*, 1998, pp.26-9.
- [A2.12] NASA NHB 5300.4-1A, 1B, 2B, 1969-71; -STD-8729.1: *Planning, Dev., Manag. an Eff. RAM Prog.*, 1998.
- [A2.13] Rooney J.P., "IEC 61508: Opportunity for rel.", *Proc. Ann. Rel. & Maint. Symp.*, 2001, pp. 272-77.
- see also [5.61, A1.1-A1.9, A3.3] and Table A2.1

A3 Quality and Reliability Assurance Program

- [A3.1] AT&T (1990), *Reliability by Design: A Guide to Reliability Management*; see also [A2.2].
 - [A3.2] Carrubba E.R., Commercial vs. DoD rel. progr.", *Proc. Ann. Rel. & Maint. Symp.*, 1981, pp. 289-92.
 - [A3.3] DoD, *DoD Guide for Achieving Reliability, Availability and Maintainability, August 2005*; RIWG: *Report of Rel. Improvement Group*, Vol. 1 & 2, September 2008 (Office of the secretary of defense); *Sample Reliability Language for DoD Acquisition Contracts*, 2008, Washington.
 - [A3.4] IEEE-Std 730-2002: *IEEE Standard for Software Quality Assurance Plans*.
 - [A3.5] MIL-STD-785B (1998): *Rel. Progr. for Systems & Equip. Dev. & Production*, replaced by [A2.0].
 - [A3.6] NASA NHB 5300.4 -1A (1970): *Rel. Progr. Prov. for Aero. & Space System Contractors*.
- see also [1.2, 1.4, 1.8, 1.14., 1.15, 1.18, A1.1-9, A2.1-13, A.4.1-6, A.5.1-6]

A4 Design Reviews

- [A4.1] ASQC, *Configuration Management*, 1969.
- [A4.2] IEC 61160 (2005): *Formal Design Review*.
- [A4.3] IEEE Std 828-2012: *Configuration Management in Systems and Software Engineering*, 1028-2008: *Standard for Software Reviews and Audits*.
- [A4.4] MIL-STD-1521B (1985): *Technical Review and Audits for Systems, Equipment, and Comp. Programs*.
- [A4.5] Samaras T.T., *Fundamentals of Configuration Management*, 1971, Wiley, NY.
- [A4.6] VDI Bericht 192: *Konzeptionen und Verfahrensweisen für Entwurfsüberprüfungen*, 1973.

see also [1.4, 1.8, 1.14]

A5 Quality Data Reporting System

- [A5.1] ASQC, *A Rel. Guide to Failure Reporting, Analysis, and Corrective Action Systems*, 1977.
- [A5.2] Collins J.A. et al., "Helicopter failure modes and corrective actions", *Proc. Ann. Rel. & Maint. Symp.*, 1975, pp. 504-10.
- [A5.3] IEC 60300-3-2 (2004): *Dependability Manag. - Guide for the Collection of Dependability Data from Field*, see also 60706-3.
- [A5.4] MIL-STD-2155 (1985): *Failure Reporting, Analysis & Corrective Action System (FRACAS)*.
- [A5.5] NASA TND-5009 (1969): *An Introduction to Computer-Aided Reliability Data Analysis*.
- [A5.6] Thomas E., "Appl. of unified data base technol.", *Proc. Ann. Rel. & Maint. Symp.*, 1984, pp. 192- 96.

A6 Probability Theory

- [A6.1] Aitchison J. et al., *The Lognormal Distribution*, 1969, Univ. Press, Cambridge.
- [A6.2] Breiman L., *Probability*, 1968, Addison-Wesley, Reading MA.
- [A6.3] Bühlmann H. et al., *Einführung in die Theorie & Praxis der Entscheidung*, 1969, Springer, Berlin.
- [A6.4] Crow E.L. et al., *Lognormal Distributions - Theory and Applications*, 1988, Dekker, NY.
- [A6.5] Evans D.M., *Probability and its Applications for Engineers*, 1992, Dekker, Milwaukee.
- [A6.6] Feller W., *An Introduction to Probability Theory and its Applications*, Vol. I 2nd Ed. 1957, Vol. II 1966, Wiley, NY.
- [A6.7] Gnedenko B.W., *Theory of Probability*, 1967, Cheslea, NY; *Lehrbuch der Wahrscheinlichkeitsrechnung*, 3th Ed. 1962, Akademie, Berlin.
- [A6.8] Gumbel E.J., *Statistical Theory of Extreme Values and Some Practical Applications*, 1954, National Bureau of Standards, Washington.
- [A6.9] Johnson N.L. et al., *Distributions in Statistics*, Vol. 1 - 4, 1969 to 1972, Wiley, NY.
- [A6.10] Kolmogoroff A.N., *Grundbegriffe der Wahrscheinlichkeitsrechnung*, 1933, Springer, Berlin.

- [A6.11] Kuhn P.N., *Computational Probability*, 1980, Academic Press, NY.
- [A6.12] Laha R.G. et al., *Probability Theory*, 1979, Wiley, NY.
- [A6.13] Ochi M.K., *Applied Probability and Stochastic Processes*, 1990, Wiley, NY.
- [A6.14] Rao M.M., *Probability Theory with Applications*, 1984, Academic Press, Orlando.
- [A6.15] Roberts R.A., *An Introduction to Applied Probability*, 1992, Addison-Wesley, Reading MA.
- [A6.16] Rényi A., *Wahrscheinlichkeitsrechnung*, 2nd Ed. 1966, VEB Deut. Verlag der Wiss., Berlin.
- [A6.17] Shiriyayev A.N., *Probability*, 1984, Springer, NY.
- [A6.18] Stark H., et al., *Probability, Random Processes and Estimation Theory for Engineers*, 1986, Prentice Hall, Englewood Cliffs NJ.
- [A6.19] Trivedi K.S., *Probability and Statistics with Reliability, Queuing, and Computer Science Applications*, 2nd Ed. 2001, Wiley, NY.
- [A6.20] Weibull W., "A statistical distrib. function of wide applicability", *J. Appl. Mech.*, 1951, pp. 293-97.

A7 Stochastic Processes

- [A7.1] Asmussen S., *Applied Probability and Queues*, 1986, Wiley, Chichester.
- [A7.2] Birolini A., *Semi-Markoff und verwandte Prozesse: Erzeugung und Anwendungen auf Probleme der Zuverlässigkeits- und Übertragungstheorie*, Ph.D. Thesis 5375, ETH Zurich, 1974, also in *AGEN-Mitt.*, 18(1975), pp. 3-52 and part in "Some applications of regenerative stoch. processes to rel. theory - Part One & Two", *IEEE Trans. Rel.*, 23(1974)3, pp. 186-94 & 24(1975)5, pp. 336-40 and "Hardware simulation of semi-Markov & related proc.", *Math. & Comp. in Simul.*, 19(1977), pp. 75-97 & 183-91; *On the Use of Stoch. Processes in Modeling Rel. Problems*, 1985, Springer, Berlin (Lect. Notes Ec. & Math. Syst. 252); *Qualität und Zuverlässigkeit technischer Systeme*, 1985, 88,91, 97, Springer, Berlin.
- [A7.3] Cinlar E., *Introduction to Stochastic Processes*, 1975, Prentice Hall, Englewood Cliffs NJ.
- [A7.4] Cox D.R., "The analysis of non-markovian stoch. proc. by the inclusion of sup. variables", *Proc. Cambridge Phil. Soc.*, 51(1955), pp. 433-41; *Renewal Theory*, 1962, Methuen, London; - et al., *The Statistical Analysis of Series of Events*, 2nd Ed. 1968, Methuen, London.
- [A7.5] Csenki A., "Mission availability for rep. semi-Markov systems", *Statistics*, 26(1995), pp. 75-87.
- [A7.6] Cramér H., "Model building with the aid of stoch. proc.", *Technometrics*, 6 (1964), pp. 133-59; - et al., *Stationary and Related Stochastic Processes*, 1967, Wiley, NY.
- [A7.7] Downton F., "Stoc. models for successive failures", *Proc. 38th Sess. Int. Stat. Inst.*, 44(1971)1, pp. 667-94.
- [A7.8] Drenick R.F., "The failure law of complex equipment", *J. Soc. Ind. Appl. Math.*, 8(1960), pp. 680-90.
- [A7.9] Feller W., "On the integral eq. of renewal theory", *Ann. Math. Statistics*, 12(1941), pp. 243-67; "Fluctuation theory of recurrent events", *Trans. Amer. Math. Soc.* 67(1949), pp. 98-119; "On semi-Markov-proc.", *Proc. Nat. Acad. Scient. (USA)*, 51(1964), pp. 653-59; *An Introduction to Probability Theory and its Applications*, Vol. I 3th Ed. 1968, Vol. II 2nd Ed. 1966, Wiley, NY.
- [A7.10] Franken P. et al., "Reliability analysis of complex repairable systems by means of marked point processes", *J. Appl. Prob.*, 17(1980), pp. 154-67; - et al., "Reliability analysis of complex systems with repair", *EIK*, 20(1984), pp. 407-22.
- [A7.11] Franken P. et al., *Queues and Point Processes*, 1982, Wiley, NY.
- [A7.12] Gnedenko B.W. et al., (Ed.), *Handbuch der Bedienungstheorie*, vol. & II 1983, Akad., Berlin.
- [A7.13] Gnedenko B.W. et al., *Introduction to Queuing Theory*, 1989, Birkhäuser, Basel.
- [A7.14] Grigelionis B.I., "Limit theorems for sums of repair processes", *Cybernetics in the Serv. of Comm.*, 2(1964), pp. 316-41.
- [A7.15] Johnson N. L., "A proof of Wald's theorem on cumul. sums", *Ann. Math. Stat.*, 30(1959), pp. 1245-47.
- [A7.16] Karlin S. et al., "The differential equations of birth and death processes, and the Stieltjes moment problem", *Trans. Amer. Math. Soc.*, 86(1957), pp. 489-546; "The classification of birth and death processes", *Trans. Amer. Math. Soc.*, 85(1957), pp. 366-400; "Coincidence properties of birth and death processes", *Pacific J. Math.*, 9(1959), pp. 1109-40.
- [A7.17] Khintchine A.Y., *Mathematical Methods in the Theory of Queuing*, 1960, Griffin, London.
- [A7.18] Kovalenko I.N. et al., *Models of Random Processes*, 1996, CRC Press, NY.
- [A7.19] Lévy P., "Processus semi-markoviens", *Proc. Int. Congr. Math. Amsterdam*, 3(1954), pp. 416-26.
- [A7.20] Osaki S. et al., (Eds.), *Stochastic Models in Reliability Theory*, 1984, Springer, Berlin (Lect. Notes in Ec. and Math. Syst. Nr. 235).
- [A7.21] Parzen E., *Stochastic Processes*, 3rd Printing 1967, Holden-Day, San Francisco.

- [A7.22] Pavlov I.V., "The asymptotic distribution of the time until a semi-Markov process gets out of a kernel", *Eng. Cybernetics*, (1978)5, pp. 68-72.
- [A7.23] Pyke R., "Markov renewal processes: definitions and preliminary properties", *Annals Math. Statistics*, 32(1961), pp. 1231-42; "Markov renewal proc. with finitely many states", *Annals Math. Stat.*, 32(1961), pp. 1243-59; - et al., "Limit theorems for Markov renewal proc.", *Annals Math. Stat.*, 35(1964), pp. 1746-64; "The existence and uniqueness of stationary measures for Markov renewal proc.", *Annals Math. Stat.*, 37(1966), pp. 1439-62.
- [A7.24] Smith W.L., "Asymptotic renewal theorems", *Proc. Roy. Soc. Edinburgh*, 64(1954), pp. 9-48; "Regenerative stochastic processes, *Proc. Int. Congress Math. Amsterdam*, 3(1954), pp. 304-05; "Regenerative stoch. processes", *Proc. Roy. Soc. London*, Ser. A, 232(1955), pp. 6-31; "Renewal theory and its ramifications", *J. Roy. Stat. Soc.*, Ser. B, 20(1958), pp. 243-302; "Remarks on the paper: Regenerative stochastic processes", *Proc. Roy. Soc. London*, Ser. A, 256(1960), pp. 496-501.
- [A7.25] Snyder D.L. et al., *Random Point Processes in Time and Space*, 2nd Ed. 1991, Springer, Berlin.
- [A7.26] Solov'yev A.D., "The problem of optimal servicing", *Eng. Cybernetics*, 8(1970)5, pp. 859-68; "Asymptotic distribution of the moment of first crossing of a high level by a birth and death proc.", *Proc. sixth Berkeley Symp. Math. Stat. Prob.*, 3(1970), pp. 71-86; "Asymptotic behavior of the time of first occurrence of a rare event in a reg. process", *Eng. Cybernetics*, 9(1971)6, pp. 1038-48.
- [A7.27] Srinivasan S.K. et al., *Probabilistic Analysis of Redundant Systems*, 1980, Springer, Berlin (Lect. Notes Ec. & Math. Syst. 175); *Stochastic processes*, 2nd Ed. 1988, Tata McGraw-Hill, New Delhi.
- [A7.28] Störmer H., *Semi-Markoff-Prozesse mit endlich vielen Zuständen*, 1970, Springer, Berlin (Lect. Notes in Op. Res. and Math. Syst. Nr. 34).
- [A7.29] Takács L., "On a probability theorem arising in the theory of counters", *Proc. Camb. Phil. Soc.* 52(1956), pp. 488-98; "On certain sojourn time problems in the theory of stoch. proc.", *Acta Math. (Hungar)*, 8(1957), pp. 169-91; *Stochastic Processes, Problems and Solutions*, 4th Ed. 1968, Methuen, London.
- [A7.30] Thompson W.A., Jr., "On the foundations of reliability", *Technometrics*, 23(1981)1, pp. 1-13; *Point Processes Models with Applications to Safety and Reliability*, 1988, Chapman & Hall, N Y.

see also [2.34, 60-6.80]

A8 Mathematical Statistics

- [A8.1] Bain L. et al., *Statistical Analysis of Rel. and Life-Testing Models*, 2nd Ed. 1991, Dekker NY.
- [A8.2] Birnbaum Z.W., "Numerical tabulation of the distribution of Kolmogorov's statistic for finite sample size", *Annals Stat. Ass.*, 47(1952), pp. 425-41.
- [A8.3] Cain S.R., "Distinguishing between lognormal and Weibull distributions", *IEEE Trans. Rel.*, 51(2002)1, pp. 32-38.
- [A8.4] Cantelli F.P., "Considerazioni sulla legge uniforme dei grandi numeri e sulla generalizzazione di un fondamentale teorema del Sig. Paul Lévy", *Giornale Attuari*, 1933, pp. 327-38; "Sulla determinazione empirica delle leggi di probabilità", *Giorn. Attuari*, 1933, pp. 421-24.
- [A8.5] Chernoff H. et al., "The use of maximum Likelihood estimates in χ^2 goodness-of-fit", *Ann. Math. Stat.*, 25(1954), pp. 579-86.
- [A8.6] Clopper C.J. et al., "The use of confidence or fiducial limits illustrated in the case of the binomial", *Biometrika*, 26(1934), pp. 404-13.
- [A8.7] Cochran W.G., "The χ^2 tests of goodness of fit", *Ann. Math. Stat.*, 23(1952), pp. 315-45.
- [A8.8] Cramér H., *Mathematical Methods of Statistics*, 1946, 19th Printing 1999, Univ. Press, Princeton.
- [A8.9] d'Agostino R.B. et al., *Goodness-of-fit-Techniques*, 1986, Dekker, NY.
- [A8.10] Darling D., "Kolmogorov-Smirnov, Cramer-von Mises tests", *Ann. Math. Stat.*, 28(1957), pp. 823-38.
- [A8.11] Durbin J.: *Distribution Theory for Tests Based on the Sample Dis. Function*, SIAM Publ. No. 9, Philadelphia, 1973.
- [A8.12] Epstein B. et al., "Life testing", *J. Amer. Stat. Ass.*, 48(1953), pp. 486-502; "Truncated life tests in the exp. case", *Ann. Math. Stat.*, 25(1954), pp. 555-64; "Sequential life tests in the ex. case", *Ann. Math. Stat.*, 26(1955), pp. 82-93; "Test for the validity of the assumption that the underlying distribution of life is exponential" Part I & II, *Technometrics*, 2(1960), pp. 93-101 & 167-83; "Statistical life tests acceptance procedures", *Technometrics*, 2(1960), pp. 435-54; "The exact analysis of sequential life tests with particular application to AGREE plans", *Rel. & Maint. Conf.*, 1963, pp. 284-310.

- [A8.13] Feller W., "On the Kolmogorov-Smirnov limit theorems for empirical distributions", *Ann. Math. Stat.*, 19(1948), pp. 177-89.
- [A8.14] de Finetti B., "Sull'approssimazione empirica di una legge di probab.", *Giorn. Attuari*, 1933, pp. 415-20.
- [A8.15] Fisher R.A., "On the mathematical foundations of theoretical statistics", *Phil. Trans.*, A 222(1921), pp. 309-68; "The conditions under which χ^2 measures the discrepancy between observation and hypothesis", *J. Roy. Stat. Soc.*, 87(1924), pp. 442-50; "Theory of statistical estimation", *Proc. Cambridge Phil. Soc.*, 22(1925), pp. 700-25.
- [A8.16] Gliwienko V., "Sulla determinazione emp. delle leggi di probabilità", *Giorn. Attuari*, 1933, pp. 92-99.
- [A8.17] Gumbel E.J., *Statistical theory of extreme value and some practical applications*, Nat. Bureau of Standards, Appl. Math. Series 33, 1954; *Statistics of Extremes*, 1958, Columbia Univ. Press, NY.
- [A8.18] Hällgren B., "Availability compliance testing of systems with long mean time between failures", *Rel. Engineering*, 15(1986), pp. 83-94.
- [A8.19] Kalbfleisch J.D. et al., *Statistical Analysis of Failure Time Data*, 2. Ed. 2002, Wiley, NY.
- [A8.20] Kolmogoroff A.N., "Sulla determinazione empirica di una legge di distribuzione", *Giorn. Attuari*, 1933, pp. 83-91.
- [A8.21] Lawless J. F., *Statistical Models and Methods for Lifetime Data*, 1982, Wiley, NY.
- [A8.22] Lehmann E.L., *Testing Statistical Hypotheses*, 1959, Wiley, NY.
- [A8.23] Mann N.R. et al., *Methods for Statistical Analysis of Reliability and Life Data*, 1974, Wiley, NY.
- [A8.24] Mason R.L. al., *Statistical Design and Analysis of Experiments*, 2003, Wiley Inter., NY.
- [A8.25] Martz H.F. et al., *Bayesian Reliability Analysis*, 1982, Wiley, NY.
- [A8.26] Meeker W.Q. et al., *Statistical Methods for Reliability Data*, 1998, Wiley, NY.
- [A8.27] Miller L.H., "Table of % points of Kolmogorov statistics", *J. Amer. Stat. Ass.*, 51(1956), pp. 111-21.
- [A8.28] Pearson K., "On deviations from the probable in a correlated system of variables", *Phil. Magazine*, 50(1900), pp. 157-75.
- [A8.29] Rise J., "Compliance test plans for availability", *Proc. Ann. Rel. & Maint. Symp.*, 1979, pp. 368-73.
- [A8.30] Serfling R.J., *Approximation Theorems of Mathematical Statistics*, 1980, Wiley, NY.
- [A8.31] Smirnov N., "On the estimation of the discrepancy between empirical curves of distribution for two independent samples", *Bull. Math. Moscow Univ.*, 2(1939), fasc. 2.
- [A8.32] Stephens M., "On the half-sample method for goodness-of-fit", *J. Roy. Stat. Soc.*, B40(1978), pp. 64-70.
- [A8.33] Wald A., *Sequential Analysis* 1947, Wiley, NY; *Statistical Decision Functions*, 1950, Wiley, NY.

A9 Tables

- [A9.1] Abramowitz M. et al., (Eds.), *Handbook of Mathematical Functions*, 11th Ed. 1974, Dover, NY.
- [A9.2] Ciba-Geigy, *Wissenschaftliche Tabellen*, Vol. 3, 8th Ed. 1980, Ciba-Geigy, Basel.
- [A9.3] Fisher R.A. et al., *Statistical Tables for Biological, Agricultural and Medical Research*, 6th Ed. 1974, Longman, London.
- [A9.4] Jahnke-Emde-Lösch, *Tables of Higher Functions*, 7th Ed. 1966, Teubner, Stuttgart.
- [A9.5] Owen D.B., *Handbook of Statistical Tables*, 1962, Addison-Wesley, Reading MA.
- [A9.6] Pearson E.S. et al., *Biometrika Tables for Statisticians, Vol. 1*, 3rd Ed. 1966, University Press, Cambridge.

Index

(less relevant places (**not bold**) are often omitted,
bold italic refers to definitions or key places)

A priori / a posteriori probability **422, 533**

Absolute probability **481** → State probability

Absolutely continuous **424, 435**

Absorbing state **197, 198, 493, 494**

Accelerated test **35, 82, 86, 98-99, 101, 102, 329-34,**
335-36, 364, 374, 448, 558

Acceleration factor **36, 99, 101, 329-33**

Acceptable Quality Level (AQL) **86, 306-08, 552**

Acceptance line **305, 322-24, 550-51**

Acceptance probability curve

→ Operating characteristic curve

Acceptance test → Demonstration

Accessibility **8, 118, 157**

Accident prevention **9, 385**

Accumulated operating time → Cumulative op. time

Accumulated reward **271, 279, 501**

Acquisition cost **11, 13, 14, 379, 392**

Activation energy **37, 86, 97, 99, 103, 330, 331, 361**

Active redundancy **31, 43, 43-61, 62, 64, 68, 196, 201,**
213, 217, 232, 233, 364, 383

• with common cause failures **271-73**

Addition theorem **419, 421-22, 450**

Additional / supplementary states **193, 515**

Adjustment **118, 158**

Administrative delay **113, 375**

Advantage

- in-circuit test **362**
- redundancy (nonrepairable) **44**
- repair priority **222**
- repairable redundancy **202**
- 100% incoming inspection **358-59**
(see also Favored)

Aerospace **390**

Aftereffect → Without aftereffect

After-sale **8, 13**

Age replacement **134, 135-39**

Aging **6, 427** (see also Wear-out, As-bad-as-old)

Alarm / alarm circuitry **49, 255, 158, 249, 298**

Alarm deflection **255**

Alignment → Adjustment

Allocation (reliability) **67, 392, 394**

All-terminal **275-76**

Alternating renewal processes **176, 474-77, 478, 507, 510**

Alternative hypothesis (H_1) **302, 313, 320, 327, 334, 547**

Alternative investigation methods **280-94**

AMSAA model **352**

Anderson - Darling statistic **557**

Antistatic **94, 153** (see also Electrostatic Discharge)

AOQ / AOQL **303-04**

Aperture in shielded enclosure **149**

Approximate expressions **59, 124, 174, 186-87, 198-99,**
201-2, 206-07, 213, 215, 217, 226, 229-30, 232, 233,
243, 245, 247, 251, 279, 293-94, 452, 504, 516

Approximation for

- a distribution function **7, 193, 428, 447, 448, 451,**
452, 456-59, 469-71, 497, 509, 515
- a Laplace transform **186, 206**
- a $MTTF_S$, MUT_S **200, 232, 233, 279**
- a point availability **183, 186-87, 198, 201, 206,**
215, 232, 233, 294, 512
- a reliability function **199, 201, 278, 294**
- a repair function **114, 187, 206-07**
- a series-parallel structure **232, 233**
- an interval reliability **183, 200, 205, 278**

AQL → Acceptable Quality Level

Arbitrary failure and repair rates **171, 176-82, 188,**
193-95, 207-13

Arbitrary initial conditions (one item) **184-87**

Arbitrary repair rate **171, 183, 188, 192-95, 204-12,**
213, 218-19, 222-25, 249-50, 510-14

Arithmetic random variable **424, 428, 430, 438,**
450-54

Arrhenius model **36-37, 97, 102, 329-31, 361**

Arrival rate **516, 524** (see also Intensity)

Arrival / occurrence time **343, 353, 464, 517, 518**

As-bad-as-old **41, 138-39, 427, 519**

As-good-as-necessary **19**

As-good-as-new **5, 6, 8, 40-41, 61, 134, 171, 173, 178,**
239-40, 241, 316, 341, 374, 375, 378, 380, 381, 427

Assessed reliability **3**

(see also Demonstration, Estimation)

Assumptions **31, 39, 41, 43, 52, 170-71, 238-40, 260**

Assurance program / tasks

→ RAM / RAMS assurance program

Asymptotic behavior

- alternating renewal processes **477**
- correspondence with steady-state and stationary
472, 477, 498, 509
- Markov processes **496-98**
- one-item structure **185-87**
- regenerative processes **478-79, 514**
- renewal processes **469-71**
- semi-Markov processes **508-09**
(see also Stationary, Steady-state)

Asynchronous logic **155**

- Attainable intensity **354**
 Attributes (test by) **299**
 (see also Software quality)
 Audits **106, 357, 397**
 Availability **9, 374** → Point availability (PA)
 (see also Intrinsic, Joint, Mission, Operational,
 Overall, Technical, Work-mission availability)
 • approximate expressions **178, 183, 187**
 Availability estimation and demonstration **311-15,**
 545-46, 553-55
 Average availability (AA) **9, 178-79, 183, 188, 498**
 Average Outgoing Quality (AOQ) **303-04**
 Axioms of probability theory **416**
- B**ackdriving **362**
 Backward equation → Kolmogorov equation
 Backward recurrence time **468-69**
 Bad-as-old (BAO) → As-bad-as-old
 Bamboo structure **97**
 Baseline → Reference documentation
 Basic rules → Rules for
 Bathtub curve **6-7, 444**
 Bayes theorem **422, 436**
 Bayesian estimate / statistics **436, 533**
 BDD → Binary decision diagram
 Bernoulli distribution → Binomial distribution
 Bernoulli trials / model **449, 453, 455, 535, 538**
 Bernoulli variable **449, 453**
 Beta distribution **540, 546, 564**
 Biased **311, 317, 318, 529, 535, 537, 555**
 Bi-directional connection **31, 53, 275**
 Binary decision diagram (BDD) **53, 58, 76, 283-85**
 Binary process **56, 58, 61, 315, 515** (see also Indicator)
 Binomial distribution **44, 300-04, 310, 430-31, 449-51,**
 527, 535, 539-42, 549
 Binomial expansion **317**
 Birth and death process **131, 197, 214-17, 501-05**
 Birth processes → Birth and death process
 BIST → Built-in self-test
 BIT → Built-in test
 BITE → Built-in test equipment
 Bivariate distribution **436**
 Black model **97, 333**
 Blackwell theorem **470**
 Block replacement **134, 135-39, 241**
 Bonding **93, 95, 100, 103, 104**
 Boolean function / method **57-61, 275, 280**
 Boolean variable **58, 315** (see also Indicator)
 Bottom-up **72, 78, 163, 164, 166, 286, 377**
 Boundary-scan **155**
 Boundary sliding **109, 363**
 Bounds **59, 61, 187, 215, 229, 240, 260, 264, 265, 280,**
 293-94 (see also Interval estimation)
- Branching processes **521**
 Breakdown **96-97, 102, 106, 145, 149, 150**
 Bridge structure **31, 53-54**
 Bridging **90**
 Built in **1, 2, 8, 16, 115, 144, 259**
 Built-in self-test (BIST) **156**
 Built-in test (BIT) **66, 116-17, 156, 249, 252**
 Built-in test equipment (BITE) **116-17, 156**
 Burn-in **6-7, 89, 101, 109, 360, 361, 364, 374**
 (see also Dynamic burn-in, Static burn-in)
 Bypass **158, 294, 295**
- Calibration **358**
 Capability **13, 152, 374, 386, 405**
 Capacitors (use & limits) **100, 145, 146, 148, 151, 573**
 Captured **188**
 Care **342, 345, 350, 363**
 CASE **164**
 Case-by-case **35, 81, 138, 139, 174, 220, 238, 240,**
 249, 259, 266, 274, 277, 289, 294, 334, 363, 510
 Cataleptic failure **4, 6**
 Cauchy distribution **563**
 Cause-to-effects-analysis / chart **15, 22, 66, 72-80,**
 160, 165, 351, 377, 378
 Causes for
 - common cause failures **271**
 - hardware defects / failures **95, 103, 106-07, 109-11,**
 271, 351, 362-63, 376, 377, 385, 411
 - software defects **162-65**
 - weaknesses **162-65, 351**
- CCF → Common cause failure
 CDM → Charged device model
 Censoring **318, 320, 346-49, 353, 354, 518, 526, 537**
 Central limit theorems **126, 456, 457-59, 471, 528**
 Central moments **433**
 Centralized logistic support **125-29, 130**
 Ceramic capacitor **145, 148, 151, 153, 573**
 Cerdip **147**
 Certification **388**
 Change **7, 165, 351, 357, 402**
 Chapman-Kolmogorov equations **482**
 Characteristic function **561, 567**
 Characterization (electrical) **89, 90, 91-93, 108**
 Charge spreading **103**
 Charged device model (CDM) **94**
 Chebyshev inequality **315, 433, 455, 456, 534**
 Check list **77, 79, 120, 393-97, 394-404, 405-09**
 Check strategy **21, 249, 250, 253, 255, 256, 257, 258**
 Chi-square (χ^2) distribution **430-31, 445, 562**
 - relation to exponential, normal, Poisson
 distribution **445, 562**
- Chi-square (χ^2) test **338-40, 344, 557-60**
 Claim **15, 382** (see also Product liability)

- Classical probability **417**
- Clock **149, 151, 155, 156**
- Close cooperation → Cooperation
- Clustering of states **229, 293**
- CMOS terminals **150**
- Coating **147**
- Coefficient of variation **128, 433**
- Coffin-Manson **109, 333**
- Cognitive **295**
- Coherent system **57, 58, 59, 61**
- Cold redundancy → Standby redundancy
- Combination of
- methods / tools **76-78, 282**
 - stresses **82, 111, 333, 334**
- Commercial program **290**
- Common cause
- events **286**
 - failures **42, 45, 66, 72, 79, 245, 255, 271-74, 277, 286, 383, 406** (see also Single-point failures)
- Common ground point **148**
- Common mode currents **149**
- Common mode failures **72, 271, 277**
- Comparative studies / comparisons **14-15, 26, 31, 38, 44, 47-48, 78, 116, 119, 130, 133, 202, 206, 207, 217-18, 227-28, 232, 233, 237, 272-73, 366, 467-68, 572-76**
- Compatibility **148, 154, 162, 402, 408**
- Complementary event / complement of events **414**
- Complete Gamma function **443, 444, 566**
- Completeness **162**
- Complex structure / system **31, 52, 53-61, 64-66, 68-69, 238, 239-76, 277-79, 280-92, 293-94**
- Complexity factor **67**
- Components & materials (basic considerations) **407**
- Components properties **572-75** (see also Design guidelines and Technological properties / limits)
- Composite hypotheses **547**
- Composite shmoo-plot **91**
- Compound failure rate **332**
- Compound processes → Cumulative processes
- Compression → Time compression
- Computer-aided reliability prediction **35, 289-92**
- Conclusions **174**
- Concurrent engineering **11, 16, 19, 375, 379, 383, 398**
- Condition for
- Markov processes **462, 482, 487**
 - memoryless property **427, 442, 482**
 - Poisson processes **472**
 - regenerative processes **478**
 - renewal processes **463-64**
 - semi-Markov processes **462, 505, 510**
 - semi-regenerative processes **462, 478, 514**
- Conditional density / distribution function **436, 507, 517**
- Conditional mean / expected value **426, 437**
- Conditional failure rate **378, 426**
- Conditional probability **418-19, 426, 466, 480, 482, 506**
- Conditional reliability function **40, 426**
- Conductive-filament **333**
- Confidence ellipse **300-301, 540-541**
- Confidence interval **301, 312, 319, 538, 539-46**
- Confidence level **86, 300, 318, 538, 546**
- Confidence limits **538**
- availability $PA=AA$ **311-12, 545-46**
 - failure rate λ **318-20, 542-45**
 - failure rate at system level λ_S **320**
 - one sided **302, 312, 319, 538**
 - parameters of a lognormal distribution **327**
 - unknown probability p **300-02, 538-42**
in particular **301, 312, 319, 538**
- Configuration **375** (see also Documentation)
- Configuration accounting **396, 402**
- Configuration auditing **396, 401-02**
(see also Design reviews)
- Configuration control **165, 396, 402**
- Configuration identification **396, 401**
- Configuration management **13, 15, 16, 18, 21, 160, 164, 165, 357, 358, 375, 396, 401-03**
- Conformal coating → Coating
- Congruential relation **291**
- Conjunctive normal form **59**
- Connections **157**
- Connector **145, 150, 151, 153, 156, 157**
- Consecutive k -out-of- n systems **45**
- Consequence → Failure effect, Fault effect
- Consistency checks **76**
- Consistency condition **461**
- Consistency (software) **162**
- Consistent estimates **456, 533, 534**
- Constant acceleration test **361**
- Constant failure rate λ
- as necessary condition **6, 40, 171, 179, 259-66, 378, 316-25, 332, 380, 427, 472, 487, 482-505**
 - concept **6, 316, 441-42, 427**
 - estimation **317, 318-20, 535, 542-44**
 - demonstration **320-25**
 - investigations with **6, 35, 40, 61-64, 183, 187, 188, 201, 217, 232, 233, 296-98, 378, 426-27, 441-42, 472-73, 482-505**
- Constant repair rate μ **183, 188, 201, 217, 226, 232, 233, 381, 482-505**
- Consumer risk β **303, 306, 313, 314, 321, 323, 548, 554** (see also Type II error)
- Contamination **85, 93, 98**
- Continuity test **88**
- Continuous from the right **423-34, 526-27**
- Continuous param. Markov chain → Markov process
- Continuous random variable **424-5, 430-1, 435-6, 441-8**

- Contract 387, 394 (see also System specifications)
- Controllability 155
- Convergence almost sure \rightarrow Conv. with probability 1
- Convergence in probability 455
- Convergence quickness 127, 186-87, 198, 301, 307, 312, 319, 325, 416, 528, 544, 552
- $PA(t) \rightarrow PA$ 183, 186-87, 198
 - $R_S(t) \rightarrow e^{-\lambda_S t}$ 199
- Convergence with probability one 455
- Convolution 438-39, 475, 485, 567
- Cooling 84, 145-47, 150, 153, 351
- Cooperation 10, 19, 20, 21, 92, 238, 280, 387-90, 394-97
- Corrective actions 16, 22, 72, 73, 77, 80, 104-05, 160, 358, 383, 404, 412
(see also Quality data reporting system)
- Corrective maintenance 8, 112-13, 118, 120, 375
(see also Repair)
- Correlation coefficient 437, 447, 462-63
- Correlation diagram 78
- Correspondence \rightarrow Equivalence
- Corrosion 6, 83, 85, 98-100, 102, 103, 147, 333
- Cost / cost equations 12, 14, 67, 135-43, 367-71, 450, 498
- Cost effectiveness 11, 13, 16, 309, 375, 379
- Cost optimization 11-15, 16, 67, 120, 134-43, 143, 242, 364-71, 375, 379, 386, 392, 398, 450, 498, 522
- Cost rate / cost per unit time 12-14, 139-40
- Count function / process ($v(t)$) 5, 464, 472, 516, 522
- Coupler 268 (see also Switch)
- Coupling 91, 97, 148, 151
- Covariance matrix 437
- Coverage 117, 249 \rightarrow Incomplete coverage, Test cov.
- Cracks 85, 93, 102, 104, 106, 108-11, 153
- Cramér - von Mises test 344, 556
- Creep deformation 108-09
- Critical
- application 253
 - decision 294
 - design review (CDR) 107, 403, 408-09
 - operating states 277
- Criticality 72-73, 160, 165, 168
- Criticality grid / criticality matrix 72-73
- Cumulated states 270, 499
- Cumulative damage 333, 522
- Cumulative distribution function \rightarrow Distribution funct.
- Cumulative operating time 316, 317, 318-20, 321, 332
- Random cumulative operating time 537
- Cumulative processes 521-23
- Customer documentation \rightarrow User documentation
- Customer requirements / needs 19, 387-90, 391-93, 394
- Customer risk \rightarrow Consumer risk
- Cut sets \rightarrow Minimal cut sets
- Cut sets / cuts theorem 497, 500
- Cutting of states 229, 237, 293
- Cycle (regenerative process) 291, 477, 478-79, 514
- Cycles to failure 333
- Damage 85, 94, 100, 102, 104, 106, 107, 152, 333, 334, 351, 357, 359, 362**
- Damage evolution / accumulation 109, 333
- Damp test \rightarrow Humidity test
- Data
- analysis 341-56, 569-71
 - collection 21, 22, 23, 383, 410-12
 - retention 89, 97-98
- DC parameter 88, 92
- Death process 61-64
(see also Birth and death process)
- Debug test 166
- Debugging 160, 166
- Decentralized logistic support 129-30, 134
- Decoupling device 32, 66, 148, 151 (see also Elements with more than one failure mechanism / mode)
- Decreasing failure rate 6-7, 242, 337-38, 442, 444
(see also Strictly increasing / decreasing failure rate)
- Decreasing intensity 6-7, 345, 348-49
- Defect 1, 4, 6-7, 72, 159, 162-66, 351, 364-65, 376, 377, 378, 381, 384, 400
(see also Dynamic defect, Nonconformity)
- causes / examples 95, 102, 106-07, 110, 152-53, 162-64, 351, 358-59, 362-63, 365-66
 - detection \rightarrow Fault detection
 - elimination (software) 166
 - prevention hardware 66, 79, 120, 144-54, 154-59, 357-58, 391-09
 - prevention software 159-65, 167
- Defect freedom (reliability for software) 162, 166
- Defect tolerant (software) 159-60, 162, 164
- Defective probability 12, 86, 299-308, 359, 362-63, 365-66, 367-72, 548
- Deferred cost 12, 14, 364, 366-71, 389
- Definition of probability 416-17
- Definitions and terms 2-15, 162, 373-86
- Deformation mechanisms / energy 109, 363
- Degradation 4, 7, 66, 92, 96, 101, 112, 392
(see also Graceful degradation)
- Degree of freedom 430, 445, 557, 559, 562-64
- De Moivre - Laplace theorem 456, 540
- Demonstration
- availability 313-15, 393, 553-55
 - defective (or unknown) probability p 302-08, 309-10, 548-52 (in particular 305, 323)
 - constant failure rate λ or $MTBF = 1 / \lambda$ 320-25, 392-93 (in particular 305, 323)
 - $MTTR$ 327-29, 393

- De Morgan's laws **414**
- Dendrites **95, 100**
- Density **424, 430, 435**
- Density rate 426 → Failure rate
- Dependability **9, 11, 13, 374, 376, 388, 389, 501**
- Derating **33, 79, 82, 84, 86, 144-45, 376**
- Design FMEA / FMECA **72, 78, 377**
- Design guidelines **13, 25-27, 66, 77, 79, 84, 396, 399**
- components / assemblies **150-53**
 - cooling **145-47**
 - derating **37, 144-45**
 - EMC / ESD **148-49**
 - ergonomic / human / safety aspects **158-59**
 - maintainability **154-159**
 - moisture **147**
 - package form / type **147**
 - reliability **144-54**
 - software quality **159-68**
 - temperature **37, 145-47**
 - testability **155-57**
- (see also Rules)
- Design reviews **13, 16, 21, 26, 27, 77, 79, 107, 120, 160, 164, 165, 365, 376, 396, 401-02, 403, 405-09**
- Design rules → Rules
- Destructive analysis / test **92, 104, 105, 334**
- Detection → Fault detection
- Deterministic → Defect, Systematic failure
- Device under test (DUT) **88**
- Dew point **104**
- Diagnosis **113, 115, 116, 120, 249**
- (see also Fault localization)
- Diagram of transitions
- probabilities **61, 190, 197, 203, 215, 221, 235, 487, 488-90, 491, 493, 494, 501, 503**
 - rates **204, 238, 246, 247, 251, 253-58, 261, 263, 267, 272-73, 277, 288**
 - states **194, 208, 222, 252, 511, 512, 513**
- Die-attach **93, 361**
- Dielectric breakdown → Time dielectric breakdown
- Difference between → Distinction between
- Different elements **44, 202-03, 232, 233**
- Difference equations **62-63, 197, 492**
- Different required functions **29, 259**
- Differential equations (method of) **63, 197-99, 491-94**
- Directed connection / arc **31, 55, 275, 287**
- Discrete random variable **424, 429, 430, 449-54**
- Discrimination ratio **303, 322**
- Disjunctive normal form **59**
- Dislocation climbing **109, 363**
- Dispersion → Variance
- Disposal **13, 19, 379**
- Distinction between
- active and standby redundancy **43, 62-64, 201, 207**
 - arrival times and interarrival times **464, 517**
 - deterministic and random failure / faults **351**
 - failure and defect **3-4, 117, 351, 376, 377, 378**
 - Markov and semi-Markov process **462, 505**
 - renewal and regeneration point **464, 475, 478, 514**
 - reliability and availability **9, 170, 374, 384, 492, 493**
 - reliability and interval reliability **40, 179, 493, 494**
 - reliability and safety **9, 384, 385**
 - repairable and nonrepairable **202**
 - software and hardware quality assurance **161**
 - time and failure censoring **320, 537, 542-44**
 - time-homogeneous and stationary **462-63**
 - $\lambda(t)$ and $f(t)$ **7, 425-26**
 - $\lambda(t)$ and $h(t)$, $m(t)$ **7, 352, 378, 466-67**
 - $\lambda(t)$ and $z_S(t)$ **7, 378, 524**
 - *MTBF* and *MTTF* **39-40, 380**
 - MUT_S and $\sum P_i MTTF_{Si}$ **500**
 - $P_{ij}(\delta t)$ and $Q_{ij}(\delta t)$ **487**
 - P_i and P_i **497, 509, 510, 514**
 - t_1^*, t_2^*, \dots and t_1, t_2, \dots **341, 353, 517**
 - $\tau_1^*, \tau_2^*, \dots$ and τ_1, τ_2, \dots **341, 517**
- Distributed / meshed systems / structures **52, 275-76**
- Distribution function **423, 430-31, 434, 441-54**
- with random parameter **428**
- Distribution law **423, 434, 481, 483**
- Documentation **7, 15, 19, 118, 161, 162, 163-64, 400-03**
- Does not close → No connection
- Does not open → Stuck at state
- Dominant failure mechanism / rate **38, 257, 332**
- Dormant state **33, 36, 145**
- Double one-sided sampling plan **307-08**
- Down / down state (d, \bar{U}) **277-78, 474-75, 491, 508**
- Down time **123-24, 140, 181, 242, 270, 314-15, 522**
- (see also System mean down time (MDT_S))
- Drift **71, 76, 79, 83, 100, 101, 147, 151, 572-75**
- Drivers **151**
- Drying material **147**
- Duane model **352-54**
- Duration (sojourn, stay) → Stay time
- Duty cycle **38, 67, 290, 392**
- Dwell time **98, 108, 109, 361, 363**
- Dynamic burn-in **101, 109, 361** (see also Burn-in)
- Dynamic defect **3-4, 159, 355, 376, 384, 385, 400**
- Dynamic fault tree / gate **76, 281-82**
- Dynamic gate **76, 281**
- Dynamic parameter **88, 150, 358**
- Dynamic stress **69, 149**
- Early failures **4, 6-7, 35, 101, 109, 333, 337-38, 345, 350, 351, 355, 359, 364, 374, 376, 377, 428, 467-68**
- Early failures period **6-7, 337-38, 345, 350, 351, 355**
- EBIC (electron beam induced current) **104, 105**
- Ecological / Ecologically acceptable **10, 391, 392**

- EDF → Empirical distribution function
- Edges 275
- EDX spectrometry 104, 105
- Effect → Failure effect, Fault effect, Error effect
- Effectiveness → Cost effectiveness
- Efficiency (software) 162
- Efficient estimates 533, 534
- Electrical characterization 90, 91-93, 108
- Electrical overstress 96, 153, 365
- Electrical test
 - assemblies 362-63
 - components 88-92
- Electrolysis 147
- Electromagnetic compatibility (EMC) 79, 82, 84, 108, 144, 148-49, 351, 405
- Electromigration 6, 89, 95, 97, 103, 106, 333
- Electron beam induced current (EBIC) 104
- Electron beam tester 91, 104
- Electronic assemblies
 - accelerated test 332
 - design guidelines 151-53
 - qualification test 107-11
 - testing and screening 362-64
- Electrostatic Discharge (ESD) 89, 94, 102, 104, 106-07, 108, 144, 148-49, 153, 357
- Elementary event 414
- Elementary renewal theorem 469
- Elements of a quality assurance system 13, 21
- Elements which appear more than once in an RBD 29-30, 31, 32, 53, 54, 56, 68, 275-76, 284, 285, 289
- Embedded
 - Markov chain 252, 291, 478, 480, 485, 486, 497, 505, 508, 509, 510, 514
 - renewal process 176, 210-11, 462, 474-75, 478-79, 506, 514
 - semi-Markov proc. 171, 204, 223, 462, 510, 511-13
- Embedded software 160, 164
- EMC → Electromagnetic compatibility
- Emergency situation 158, 294
- Emission (EMC) 148
- Emission microscopy (EMMI) 104
- Empirical
 - distribution function 334-39, 526-32
 - evaluation of data 336-39, 443, 525-32, 569-71
 - failure rate 4-5
 - mean / variance / moments 4, 325, 326, 528-29
 - methods, 525-32
 - moments / quantiles 325-26, 528-29
 - reliability function 4-5
- Empty set 414
- Environmental
 - conditions/stress 28, 33, 36, 79, 82-4, 154, 379, 406
 - stress screening → ESS
- Environmental and special tests
 - assemblies 108-09
 - components 89, 92-100
- Equations for Markov & semi-Markov models 172-73
- Equivalence between asymptotic, stationary, steady-state 171, 187-88, 472, 477, 479, 498, 509, 514
- Equivalent events 414
- Ergodic distribution 482, 497
- Ergonomics 120, 158-59, 294, 395, 407, 409
- Erlang distribution 193, 312, 314, 445, 546, 554
- Error / mistake 3, 6, 72, 76, 78, 95, 158-59, 160, 163-64, 294-98, 351, 376, 377, 378 (see also Human)
- Error correcting code 66, 160, 164
- Error effect 294-95
- ESD → Electrostatic discharge
- ESS 6, 351, 363, 376, 384 (see also Screening)
- Estimate → Empirical and Parameter estimation
- Estimated reliability 3
- Estimation (statistical)
 - availability 311-12, 315, 545-46
 - failure rate λ or $MTBF = 1 / \lambda$ (T fixed) 316-20, 535, 537, 542-43 (in particular 319)
 - failure rate λ (k fixed) 317, 537, 543-44
 - HPP / Poisson distribution 536, 542
 - $MTTR$ 325-27
 - NHPP 353-54, 520
 - point / interval (basic theory) 533-46
 - probability p , R , $PA=AA$ 300-02, 309-10, 535, 538-42, 545-46 (in particular 301, 309, 312)
- ETA → Event tree analysis
- Euler integral 566
- Events / field of events 413-16
- Event tree analysis (ETA) 76, 286, 295
- Evolution of a Markov / semi-Markov process 485-86, 510
- Examples of real systems 30, 32, 68, 235, 267, 275, 276
- Exchangeability 118, 157
- Expanding a 2-out-of-3 to a 1-out-of-3 redundancy 49
- Expected percentage of performance 271, 501
- Expected percentage of time in a state 173, 498, 507, 514
- Expected value 429, 431, 436 → Mean
- Exponential distribution 6, 40, 126, 174, 238-40, 279, 378, 427, 430-31, 441-42 (see also Constant λ)
- External cause/event/influence 10, 76, 78, 271, 281, 286
- External initialization 155
- Extreme value distributions 443
- Extrinsic 3-4, 86, 377, 411
- Eyring model 99, 102, 333
- Factorial 566
- Fail-safe 1, 9, 66, 72, 158, 164, 480
- Failure 1, 3-4, 6-7, 377, 378, 385 (see also Fault)

- Failure analysis **87, 89, 95, 101, 102-05**
 Failure cause **3-4, 10, 73, 95, 105, 106-7, 110, 377, 411**
 Failure censoring → Censoring
 Failure collection → Fault collection
 Failure coverage → Incomplete coverage
 Failure detection → Fault detection
 Failure effect → Fault effect
 Failure-free operating time **39, 425** → Failure-free time
 Failure-free time **3-6, 39-40, 175, 238-40, 378, 425, 442**
 Failure frequency → System failure frequency
 Failure hypothesis **69-70**
 failure intensity $z(t)$ **5, 7, 279, 350, 377, 466, 521, 523**
 • at system level $z_G(t)$ **521**
 Failure localization → Fault localization
 Failure mechanism **4, 37, 38, 64, 96-100, 102, 103, 108, 109, 111, 333-34, 342, 358-63, 377, 428**
 • analysis / modeling **39, 99, 102-03, 329-34, 356**
 Failure mode **3, 27, 42, 62, 64, 66, 101, 277, 377, 411**
 • examples **51, 64-65, 100, 249, 266-67, 572-76**
 • distribution **100, 572-76**
 • investigation **64-65, 72-78, 243-47, 257-58, 266-69**
 Failure modes analysis → FMEA / FMECA
 Failure propagation → Secondary failures
 Failure rate λ , $\lambda(t)$, $\lambda(x)$ **4-7, 32-38, 39, 101, 109, 344, 378, 425-28, 431, 441, 442, 444, 453, 466, 516, 524**
 • analyses **25-67**
 • confidence limits **319, 320**
 • estimation **318-20, 535, 537, 542-44**
 • demonstration **320-25** (in particular **323**)
 • distinction to → Distinction between
 • handbooks **35-36**
 • models / modeling **35-37, 38, 99, 329-33, 334**
 • of a series system **31, 42**
 • of mixed distributions **41, 428**
 • temperature dependence **3, 34-35, 37, 329-34**
 • values **36, 38, 50, 329, 392, 572-75**
 (see also Conditional failure rate)
 Failure recognition → Fault detection
 Failure severity **72-73**
 Failure tolerant → Fault tolerant reconfigurable system
 Failures with constant failure rate λ **6-7, 35**
 False alarm **66, 239, 249, 255**
 Fatigue **83, 98, 101, 103, 333, 443** (see also Wear-out)
 Fault **4, 72-73, 78, 165, 377, 378**
 Fault collection **20, 21, 357, 410-12**
 Fault coverage **249** → Incomplete coverage
 Fault criteria **408** (see also Fault effect)
 Fault detection **79, 88, 90, 102, 105, 113, 116, 117-18, 120, 154-59, 166, 240, 249, 274, 358-72, 405-09**
 Fault effect / consequence **4, 10, 72-80, 87, 101, 240, 294-95, 377, 385, 407, 409, 411** (see also Error effect, ETA, FMEA / FMECA, FTA, Negligible)
 Fault localization **112, 113, 116, 117, 154, 249-55, 362**
 Fault models / modeling **90-91, 243-58, 266-74, 356**
 Fault modes and effects analysis → FMEA
 Fault review board **411, 412**
 Fault sensing device **73**
 Fault tolerant structures / reconfigurable systems
 16, 49, 64-65, 66, 101, 159, 160, 164-65, 240, 259-72, 275-76, 498-501
 Fault tree / Fault tree analysis **66, 76, 78, 280-85, 378**
 Fault tree structure function **283-85**
 Favored (can be) **306, 324**
 Feasibility / feasibility check **11, 19, 77, 121, 161, 376, 401, 403, 405, 406**
 Feedback **22, 86, 87, 104, 150, 156, 160, 161**
 Fiber optic **157**
 Field data **35, 36, 37, 51, 341-50, 410**
 Field data change service **117**
 Field of events **413-16**
 Field operation **82, 83**
 Figures → Numerical values,
 Final value theorem **567**
 Fine leak test **361-62**
 Finite element analysis **69**
 Firing rule **287**
 First delivery **372**
 First-in / first-out **153, 226, 235, 239, 259, 263, 290, 488**
 First production item **400**
 Fishbone diagram → Ishikawa diagram
 Fisher / *F*-distribution **312-14, 451, 534, 540, 545-46, 553-55, 559, 564-65**
 FIT (Failures in time) **36**
 Fit of models **102**
 Fitness for use **11, 382** → Quality
 Fix replacement **134-35, 136, 138**
 Fixed length test → Simple two-sided test
 Flaw **73, 95, 106-11, 351, 376**
 (see also Error / Mistake)
 Flexibility (software) **162**
 Flow of failures / events **168, 316, 318, 352, 520**
 FMEA/FMECA **27, 42, 66, 69, 72-73, 74, 78, 79, 117, 120, 156, 160, 244, 259, 266, 274, 277, 377, 384, 394**
 Force of mortality **378, 426** → Failure rate
 Formation → Motivation and training
 Forward equation → Kolmogorov equation
 Forward recurrence time **182, 185, 187, 468-69, 470, 473, 476** (see also Rest waiting time)
 FRACAS → Quality data reporting system
 Fractile → Quantile
 Fraction of defective items → Defective probability
 Frequency / duration **266, 270-71, 278, 498-501, 509-10**
 Frequency of failures / repairs $f_{udS} = f_{duS}$ **266, 270-71, 278-79, 498-500, 509-10**
 Frequency of states occurrence **465, 476, 497, 509, 510**
 FTA → Fault Tree Analysis

- Function of a random variable *428, 429, 448*
 Functional block diagram *29, 30, 32, 68, 244, 267, 282*
 Functional test *88, 90-92*
- Gain** → Improvement
- Gamma distribution *126, 187, 330, 430-31, 444-45*
 Gamma function *444, 566* → Complete, Incomplete G. f.
 Gate review → Design review
 Gaussian distribution → Normal distribution
 General reliability data *341-56*
 Generalized cut sets theorem *497, 502*
 Generalized Eyring model *333*
 Generating function → Moment generating function
 Generation of nonhomogeneous Poisson proc. *520*
 Generator for stochastic jump processes *291-92*
 Genuine acceleration *329*
 Geometric distribution *292, 430-31, 453*
 Geometric probability *417*
 Glass transition temperature *85*
 Glassivation → Passivation
 Glitches *151*
 Glivenko-Cantelli theorem *527*
 Go / no go decision *158, 412*
 Gold-plated pins *94, 153*
 Gold wires *100*
 Good-as-new → As-good-as-new
 Goodness-of-fit tests *334-40, 344, 354, 555-60*
 Graceful degradation *66, 259, 277*
 Gradual failure *4*
 Grain boundary sliding *109, 363*
 Graphical evaluation / approach *335, 336, 339, 345, 350, 529-32*
 Grigelionis theorem *521*
 Gross leak *361-62*
 Ground *148-49, 150, 151, 152, 157*
 Ground tracks *151*
 Guard rings *149, 151*
 Guidelines → Design guidelines
- Halogen-free** *153*
- HALT → Highly accelerated life test
 Handbooks *21, 35, 36, 584, 600*
 Handling *85, 94*
 HASL → Hot air solder leveling
 HASS → Highly accelerated stress screening
 HAST → Highly accelerated stress test
 Hazard rate *5, 378, 426* → Failure rate
 Hazards / hazard rate *5, 378*
 HBM → Human body model
 HCMOS *149*
 Hermetic enclosure *147, 153*
 Hermetic package *85, 104, 147, 359-62*
 Heuristic methods *52-57, 341-50, 467*
- Hidden defect *14, 107, 117, 154, 156, 377*
 Hidden failures / faults *8, 66, 79, 112, 116, 117, 120, 154, 156, 240, 249-56, 377, 381*
 High temperature storage *89, 98, 359, 360*
 Higher-order moments *432, 433, 529*
 Highly accelerated life test (HALT) *334*
 Highly accelerated stress screening (HASS) *358*
 Highly accelerated stress tests (HAST) *98, 99, 334*
 Historical development *16, 17, 85*
 Homogeneous → Time-homogeneous
 Homogeneous Poisson process → Poisson process
 Hot air solder leveling *153*
 Hot carriers *89, 96, 102, 103*
 Hot redundancy → Active redundancy
 HPP → Homogeneous Poisson process
 Human aspects / factors *2, 3, 9, 10, 27, 73, 76, 120, 154, 158-59, 164-65, 294-98, 374, 384, 385, 395, 407, 409*
 Human body model (HBM) *94*
 Human errors *10, 119, 158-59, 164, 294-95*
 Human reliability *174, 294-98*,
 (see also Risk management)
 Humidity tests *89, 98-100* (see also HAST, Moisture)
 Hypergeometric distribution *430-31, 454*
 Hypotheses
 - failure *69*
 - statistical *302, 314, 320-21, 547, 548-50*
- Idempotency** *414*
- IE → Totally independent elements
 Imperfect switching → Switch
 Impossible event *414* (see also Empty set \emptyset)
 Improvement through
 - preventive maintenance *240-42, 243, 250*
 - redundancy *40, 47, 48, 202, 227, 228*
 - repair *202, 227, 228*
- Impulse $\delta(t)$ *568*
 In steady state → Stationary
 In-circuit test *362*
 In-process tests *396*
 Inclusion / Exclusion *422*
 Incoming inspection *21, 90, 150, 358, 362, 365, 366-71*
 Incomplete coverage *116-17, 249-56, 280*
 Incomplete Gamma function *444, 566*
 Increasing failure rate *6-7, 134-40, 241, 242, 442*
 (see also Strictly increasing / decreasing failure rate)
 Increasing intensity *345-48*
 Independent (see also Totally independent)
 - elements *31, 52, 171, 232, 233, 239, 280*
 - events *419, 421*
 - increments *343, 356, 461-62, 473, 516, 520, 524*
 - random variables *435, 437, 438, 438-40, 445, 447, 456, 460, 486, 525, 526, 533, 547*
 - stress / strength *70-71*

- Indicator **56, 58, 61, 315** (see also Binary process)
- Indices **3, 39, 169, 173, 175, 238, 491**
- Indirect plug connectors **120, 157**
- Induced failure / failure mechanism **83, 333**
- Inductive / capacitive coupling **91, 148, 151**
- Industrial applications (environment) **36, 37, 38, 145**
- Influence of
- common cause failures / events → Common cause
 - failure mode **243-58, 266-69**
 - number of repair crews **141, 217-18**
 - preventive maintenance **134-40, 240-43**
 - repair priority **141**
 - repair time distribution **114-15, 133-34, 206-07**
 - series element **225, 227-28, 297**
 - travel time **203-04, 512**
- Information feedback **22, 104, 382-83, 412**
- Infrared thermography (IRT) **104, 152**
- Inherent → Intrinsic
- Initial conditions / distribution **63, 184-85, 187, 197-99, 215, 471, 477, 481, 482-83, 497, 507, 508-09**
- Initial value theorem **567**
- Initiating event **286**
- Input / output pins / driver **150, 151** (see also CMOS)
- Inserted components **84, 108, 110, 111, 152**
- Inspection (quality) **20, 21, 365-66, 367-71, 372, 383**
- Instantaneous availability → Point availability
- Instantaneous failure rate **425** → Failure rate
- Instantaneous reward rate → Reward rate
- Integral equations (method of) **172, 178, 192, 200-01, 204-05, 208-12, 218-19, 223-24, 495-96**
- Integral Laplace theorem **456, 540**
- Integrated circuits (ICs) **34-38, 84-85, 87-101, 147, 150, 153, 332, 358, 359-62, 365-66, 575**
- Integrity **162, 289, 410**
- Intensity
- failure intensity **7, 344, 350, 365, 366, 377, 378, 500, 521, 524,**
 - of a point process **524**
 - of a Poisson process **316, 317, 342, 343, 345-49, 352, 353-56, 473, 503, 516, 517-19**
- Interactions **66, 160, 163, 164-65**
- Interarrival times **5, 6, 40, 41, 113, 175, 316, 341, 345, 349-50, 378, 380, 381, 426, 464, 467, 517, 524**
- Interchangeability **8** (see also Obsolescence)
- Interface
- hardware **66, 78, 79, 82, 118, 144, 151**
 - hardware / software **351**
 - software **161, 163, 164, 408**
 - Si/SiO₂, Al/Si **96, 97**
- Interference **351, 405**
- Intermetallic compound / layer **100, 103, 108, 153**
- Intermittent operation **85, 147**
- Internal visual inspection **89, 93, 104**
- Intersection of events **414**
- Interval estimate (λ) at system level **320**
- Interval estimation **300-02, 311-12, 315, 318-20, 327, 354, 538, 539-46** (in particular **301, 312, 319**)
- failure rate λ **318-20, 542-44**
 - human **296, 297, 298**
 - number of trials **459**
 - number of observations **452, 457, 542**
 - point availability **311-12, 545-46**
 - unknown probability p **300-02, 309, 538-42**
- Interval reliability **40, 172-73, 179, 183, 184, 188, 195, 200, 201, 205, 213, 216, 278, 476, 494**
- Intrinsic **3, 9, 86, 144, 377, 411**
- Intrinsic (inherent) availability **9, 13**
- Inverse function **291, 428**
- Inverse power law **333**
- Ion migration **103**
- Irreducible Markov chain / process **481-82, 497, 508-09, 514**
- IRT → Infrared thermography
- Ishikawa diagram **76-77, 78**
- ISO 9000: 2020 family **11, 388-89**
- Item **2, 379**
- Joint availability **181-82, 183, 184, 188, 315**
- Joint density / distribution **434-35, 517, 519**
- Joint distribution function **434**
- Jump processes **482, 484, 495, 505-06, 514**
- Junction temperature **33, 79, 145-47, 150, 331**
- Just-in-time **153**
- k -out-of- n : F **45**
- k -out-of- n : G → k -out-of- n redundancy
- k -out-of- n consecutive → Consecutive
- k -out-of- n redundancy **31, 44, 61-64, 130-34, 213-16, 217, 218-19, 232, 233, 489, 501-03, 511, 513**
- k -terminal **275**
- Kepner-Tregoe **76, 78**
- Key item method **52-53, 54-56, 60, 68-69, 275-76, 284**
- Key renewal theorem **185, 186, 470, 477, 479**
- Kindness (test pattern) **91**
- Kirkendall voids **100**
- Kolmogorov backward / forward equations **484**
- Kolmogorov-Smirnov test **334-39, 344, 354, 520, 556, 558-59, 565** (theorem **529-30**)
- Koroilyuk theorem **515**
- k th moment / k th central moment **432-33**
- Lack in the diagnosis **249**
- Lagrange multiplier **67**
- Laplace test **346, 348**
- Laplace transform **63, 196-97, 567-68, 439, 444, 496**
- Large complex repairable systems **293-94**

- Large series-parallel repairable structures 226-37
- Last repairable unit → Line replaceable unit
- Last replaceable unit → Line replaceable unit
- Latch-up 89, 96, 103, 150, 153
- Latent damage → Damage, Potential rel. problem
- Latent failure → Damage, Hidden failures
- Latent fault time → Undetected fault time
- Law of large numbers 455-56
- Lead-free solder 108, 109, 111, 152, 363
- Leadless 152
- Leak test → Seal test
- Learning process / phase 150, 309, 351-52, 358
- Level I, II, III → Normal test
- Liability → Product liability
- Life cycle cost (LCC) 11, 13, 16, 112, 375, 379, 386, 391, 392, 399
- Life-cycle phases 19 (hardware), 161 (software)
- Lifetime 341, 379, 386
- Lightly loaded redundancy → Warm redundancy
- Like new → As-good-as-new
- Likelihood function → Maximum likelihood function
- Limit of models 102, 520
- Limit theorems of probability theory 454-60
- Limited useful life (components) 146, 150-51, 573-74
- Limiting distribution / state probability 478, 497, 502, 509, 514 (see also Asymptotic)
- Lindeberg conditions 457
- Line repairable unit → Line replaceable unit
- Line replaceable unit (LRU) 115, 119, 125, 154, 385
- Link → Edge
- Liquid crystals 104
- List of preferred parts (LPP) → Qualified part list
- Load capability 33
- Load sharing 43, 52, 62, 61, 62-64, 171, 197, 202, 214, 480, 501
- Localization → Fault localization
- Logarithmic Poisson model 355
- Logistic delay 113, 375, 381
- Logistic support 8, 13, 115, 119, 125, 129, 154, 170, 171, 242, 501, 379, 397
- Lognormal distribution 37, 114, 193, 207, 330, 325-29, 339, 430-31, 447-48, 569
- Lognormal probability chart 339, 569
- Long-term behavior / stability 86, 101
- Loss of image 364
- Loss of performance 259, 270
- Lot tolerance percent defective (LTPD) 306-07, 552
- Lower confidence limit → Confidence limits
- Lower bound ($PA(t)$, $R(t)$) 59, 187, 260, 262, 264, 315 (see also Interval estimation)
- Lowest replaceable unit → Line replaceable unit
- LRU → Line replaceable unit
- LTPD → Lot tolerance percent defective
- Machine model (MM) 94
- Macro-structures (MS) 174, 199, 229, 233, 234, 237, 269
- Maintainability 1, 8, 9, 13, 113-15, 162, 379, 388-90
 - analysis 72, 121-125, 394-95, 399
 - engineering 13
 - estimation / demonstration 325-29, 393
 - guidelines 154-59
 - program 390
 - software 162
- Maintenance 8, 113
 - concept 8, 112, 115, 116-20
 - cost 134-43, 522
 - levels 119-20
 - strategy 35, 134-41, 240-48, 257-58, 265-66, 427
- Majority redundancy 31, 49, 66, 158, 164, 217, 218-19, 222-25, 233, 249, 253, 295
- Man-machine 16, 120, 159, 407 (see also Ergonomics)
- Mandatory for (see also Condition for, Model validity)
 - accelerated tests 329
 - common cause failures 274
 - component's selection 84-86
 - elements appearing more than once in a rel. block diagram 29-30, 31, 32, 56, 69
 - fail-safe behavior 72
 - fault tolerant systems 66
 - general data analysis 342
 - human reliability 158-59, 295
 - incomplete coverage 249, 253, 255
 - Markov process 171, 487, 506
 - Memoryless 40, 427, 442
 - MTBF and related interarrival times 6, 40, 341, 380
 - $MTTF_{Si}$ 40-41
 - Poisson processes (HPP and NHPP) 520
 - reconfiguration 266
 - redundancy 27, 42, 66, 72, 79, 240, 250, 255, 275
 - regenerative processes 171, 478
 - reliability growth 353
 - reliability improvement 27, 78 (see also Design guidelines, Design reviews)
 - repairable systems 240, 524
 - risk management 11
 - short-term tests (HALT, HAST, step-stress) 329, 334 (see also Model validity / verification)
 - semiconductor devices 150
 - semi-Markov processes 510
 - semi-regenerative processes 171, 514
 - SMT 109, 363
 - software quality / quality assurance 159, 166
 - test hardware and software 166
- Manufacturability 401
- Manufacturing process 106-11, 152-53, 357-72, 400
- Manufacturing quality 16, 20, 86, 357-72
- Margin voltage 98

- Marginal density / distribution function **435, 517**
- Market / market needs **19, 375, 383, 388, 391, 394, 398, 403, 405, 406, 409** (see also Time to market)
- Marked point processes **515**
- Marking **287**
- Markov chain **480-82** (see also Embedded M. c.)
- Markov model **61-64, 129-34, 141, 167, 171, 172-73, 189-91, 196-204, 214-18, 220-21, 225-26, 230-37, 245-48, 251-74, 277-79, 294, 482-505**
- Markov processes with a finite number of states
 - basic characteristics **462, 482-487, 496-501, 510**
 - process evolution **485-86**
 - simulation **291-93**
- Markov property **482** (see also Memoryless)
- Markov renewal processes **505**
- Markov sequence **520**
- Markov theorem **497**
- Match / Matching **149, 151**
- Mathematical statistics **525, 526-60**
- Maximum (τ_{\max}) **440**
- Maximum acceptable $p, \overline{PA}, \lambda, MTBF$ **302, 313, 321, 392**
- Maximum likelihood function / method **300, 311, 315, 318, 326, 341, 344, 353-54, 534, 535-37, 559**
- MDT \rightarrow Mean down time
- Mean (expected value) **6, 39-40, 277-79, 429, 431, 432, 436, 438, 522-23, 528-29**
 - accumulated reward **271, 279, 501**
 - down / up time **124, 200, 237, 242, 270, 278-79, 499-500, 509**
 - expected failures per year **270, 392**
 - instantaneous reward rate **271, 279, 501**
 - logistic delay (MLD) **242**
 - number of failures / repairs **270, 278-79, 499-500**
 - operating time between failures **MTBF 6, 40, 316, 380**
 - acceptance test **392-93**
 - estimation / demonstration **316-25**
 - sojourn time in Z_i **251, 507, 510, 514** (see also Stay)
 - survival failure-free time **426**
 - time between consec. occurrence of Z_i **509, 514**
 - time to failure (MTTF, $MTTF_{Si}$) **6, 39, 41, 63, 172-73, 176, 201, 217, 227-28, 232, 233, 277, 278, 380, 496, 508**
 - time to preventive maintenance (MTTPM) **8, 113, 121, 125, 381**
 - time to repair (MTTR) **8, 9, 113, 121-24, 381, 474**
 - acceptance test **393**
 - estimation / demonstration **325-29**
 - time to restoration \rightarrow Mean time to repair
 - time to system failure \rightarrow Mean time to failure
 - undetected (latent) fault time τ_{UFT} **251, 427**
 - up time (MUT) \rightarrow Mean down / up time
- Mean value function **343, 350, 352, 355, 516, 524**
 - at system level **520**
- Mean value theorem **479**
- Mechanical fatigue **333** (see also Fatigue, Coffin)
- Mechanical keying / fixing **152, 155, 157**
- Mechanical reliability **68-71, 73**
- Mechanical stress **169-71, 83, 98**
- Mechanism \rightarrow Failure mechanism
- Median **114, 434**
- Memories 90-91, 95, 97-98, **151**
- Memoryless **7, 278, 342, 427, 431, 462, 507, 516, 524**
- Memoryless property **7, 35, 40, 62, 179, 183, 241, 317, 378, 427, 442, 453, 462, 473, 482, 486, 487, 500, 516**
- Meniscograph method **94**
- Merging \rightarrow State merging
- Meshed \rightarrow Distributed
- Metal migration **100, 103** (see also Electromigration)
- Metallization **97, 103**
- Metallographic investigation **95, 104, 107, 108-10**
- Method of
 - Boolean function **57-61**
 - differential equations **63, 173, 197-99, 491-94**
 - integral eqs **172, 200-01, 204-05, 495-96, 508**
 - key item **52-53, 54-56, 60, 68-69, 275-76, 284**
- Metrics (software quality) **160**
- Microcracks \rightarrow Cracks
- Microsections **95, 104, 105, 107, 108, 110**
- Microvoids **108, 109**
- Miner's hypothesis **333, 334**
- Minimal cut sets **59, 60, 76, 275, 281, 283**
- Minimal operating state \rightarrow Critical operating states
- Minimal path sets **58, 60, 76, 275, 281, 283**
- Minimal repair **138-39, 427**
- Minimum (τ_{\min}) **440**
- Minimum acceptable $p, \overline{PA}, \lambda, MTBF$ **302, 313, 321, 392**
- Mishandling \rightarrow Misuse
- Misleading probability **295**
- Mission availability **180**
- Mission profile **3, 28, 38, 68, 69, 79, 238, 379, 392, 408**
- Mission reliability **260** \rightarrow Reliability (R)
- Mistake \rightarrow Error
- Misuse **102, 103, 179, 271, 384**
- Mitigate **72, 73, 76, 286, 377** (see also Check strategy)
 - incomplete coverage **255**
- Mixed distribution function **424**
- Mixture of distributions **7, 41, 338, 428**
- MLD \rightarrow Mean logistic delay
- MM \rightarrow Machine model
- Modal value **113-14, 434**
- Mode \rightarrow Failure mode
- Model validity / verification **102, 109, 117, 168, 238-40, 249, 252, 277, 280, 295, 329, 331, 332-34, 341-42, 344, 353, 356, 510, 520** (see also Assumptions, Mandatory)

- Modeling early failures / wear-out period 7, 337, 355, 428, 443, 444, 467-68
- Models for cost optimization → Cost optimization
- Models for failure rates / mechanisms 35-38, 94, 96-100, 102, 103, 109, 329-34, 428
- Models for faults → Fault models
- Modification 162, 163, 165, 351, 357, 402
- Modified renewal process 464
- Module / Modular
- hardware 118, 120, 154-55
 - software 161-63, 164, 166
- Moisture 85, 93, 98-99, 147
- Moment generating function 522, 567
- Monotone / Monotony 57
- Monotonic trend (test for) 345-50
- Monte Carlo simulation 280, 290-92, 294, 448, 457, 520
- More than one failure mechanism / mode → Multiple
- More than one repair crew 217-18, 232, 488, 489, 503-504 (see also Totally independent elements)
- More than 2 states → Multiple failure modes / mech.
- Motivation / training / training level 18, 24, 115, 119, 154, 159, 294, 397, 407
- MP → Markov process
- MS → Macro-structures
- MTBF* → Mean operating time between failures
- MTBUR* (mean time between unsched. removals) 381
- MTTF* → Mean time to failure
- MTTPM* → Mean time to preventive maintenance
- MTTR* → Mean time to repair / restoration
- Multi-states → More than 2 states
- Multidimensional random variable → Random vector
- Multifunction system → Phased-mission system
- Multilayer 97, 110, 148, 154
- Multimodal 434
- Multinomial distribution 340, 451, 559, 560
- Multiple failure modes / mechanisms 37, 64-65, 66, 76, 248, 255, 257-58, 266-69, 275, 332, 342, 363, 428
- Multiple fault / consequences 76, 274, 378
- Multiple one-sided sampling plans 307-08
- Multiplication theorem 420-21
- Multi point ground 149
- MUT* → Mean up time
- Mutually exclusive events 57, 178, 181, 244, 414, 415, 416, 419, 420, 422, 468
- Mutually independent . 419, 435 → Independent
- MUX 155, 156
- N** self configuring programming (NSCP) 66, 164
- n*-dimensional distribution function 434, 460 (see also Random vector)
- N-modular redundancy 49
- N-version programming (NVP / NVS) 49, 66, 164
- NBTI (negative bias temperature instability) 103
- Negligible
- alarm circuitry 298
 - common cause failure 273-74
 - human error 296, 297, 298
 - incomplete coverage 253, 255, 256
 - imperfect switching 245, 246, 247, 248, 257
 - series element to a redundancy 46-48, 221, 225, 226
- Network reliability 275-76
- New-better-than-used 427
- New-worse-than-used 427
- NHPP → Nonhomogeneous Poisson process
- No aging 427 (see also Constant failure rate)
- No connection 245, 257-58, 266-69
- No FF (no further failures at system down) 170, 174, 229, 233, 235, 239, 489, 490
- No start at call 252 (see also Refuse to start)
- Nodes 275
- Non-irreducible Markov chain 497
- Non-markovian 277
- Non-parametric 529
- Nonelectronic components 35
- Nonconformity 376, 381
- Nondestructive analysis 102, 105
- Nonhermetic packages 85, 89, 98 (see also Plastic)
- Nonhomogeneous Poisson processes (NHPP) 138-39, 168, 342, 343-49, 352-56, 473, 516-20
- tests 343-49, 520
- Nonregenerative stochastic processes 170, 171, 193, 207, 219, 478, 515-24
- Nonrepairable item (up to system failure) 5-6, 39-57, 61-71, 243-44, 275-76, 283-85
- Normal distribution 37, 70-71, 126, 128, 142, 328, 330, 430-31, 446-47, 456-59, 471, 518, 528, 561, 571
- Normal probability chart 571
- Normal process 463
- Normal / reduced / tightened test 306
- Not regeneration state 208, 218, 511-13
- Null hypothesis (H_0) 302, 313, 320, 327, 547-48
- Number of observations 457, 458, 542
- Number of states 56, 65, 221, 226, 235, 490
- Number of trials 291, 457
- Numerical
- computation 289-92
 - examples (some few important) 50-51, 70, 207, 237, 264, 269, 270, 310, 332, 335, 338, 457-59, 467, 558
 - test conditions 83, 89, 94, 98, 99-100, 108-09, 359-62, 363
 - values for derating 145
 - values for failure modes 100
 - values for failure rates 7, 36-38, 50-51, 392, 572-75
 - values for defective probability 359, 362-63

- OBIC (optical beam induced current) 104, 105
Object oriented programming 164
Observability 155
Obsolescence 8, 118, 143, 150, 379, 400
OC → Operating characteristic curve
Occurrence frequency 286
Occurrence rate 271, 274
Occurrence time → Arrival time
On line / without interruption 112, 124, 125, 170, 171, 196, 239, 240
One-item structure 39-41, 175-89, 240-43
One-out-of-2-tworedundancy 43-44, 196-213, 232, 233, 243-58, 271-74, 296-98, 488, 492-94, 511-12 (in particular 196-99, 201, 213, 232, 233, 488, 492-94)
One regeneration state 196, 171, 207, 208, 478
One repair crew → Only one repair crew
One-sided confidence interval 302, 312, 319, 320, 538
One-sided sampling plan (for p) 306-08, 551-52
One-sided tests to demonstration λ or $MTBF = 1 / \lambda$ 324-25
One-step transition probability 506
Only one repair crew
 all models of Chapter 6 except pp. 217-18, 231, 232, 276, 280-85, 294, 488-89, 503, 515
Operating characteristic curve 303-04, 307, 322, 324, 325, 329, 549-50, 552
Operating (field) conditions 3, 7, 28, 33, 79, 84, 99, 102, 376, 394, 406
Operating console 149, 159
Operation monitoring 116, 156, 249
Operational availability 13, 242
Operational profile 28
Optical beam induced current (OBIC) 104
Optimal derating 33, 145
Optimization 67, 112, 120, 143, 364, 375, 386
 • cost 12-15, 67, 120, 137-40, 142-43, 358, 366-71
 • preventive maintenance period 137-38, 139, 140, 241-43, 250-51
 • reliability allocation 67
 • steady-state availability 143
Optoelectronic / Optocoupler 145, 146, 151
Order statistic 343, 345-47, 354, 518, 519, 526, 536
Order(ed) observations / sample 334, 335, 343, 345, 346, 347, 354, 518, 519, 526, 528, 558
Ordinary renewal process 292, 464
Organization (company structure) 20, 388
Outcoming event 286
Outgoing quality (AOQ) 303-04, 367
Overall availability 9, 139-40, 242
Overstress / overload 33, 103, 153, 351, 359
Oxidation 98
Oxide / oxide breakdown 96-97, 102, 103, 106-7, 333
Package / Packaging 84-85, 100, 104, 146-47, 333 (see also Hermetic, Plastic)
Pairwise independent 419
Parallel model 31, 43-45, 61-64, 196-201, 213-19, 232, 233, 243-59, 271-74, 488-89, 492-94, 501-03, 511-13
Parallel redundancy → Active redundancy
Parameter estimation 300-02, 309, 311-12, 315, 316-20, 325-27, 353-54, 533-46 (in particular 301, 312, 319, 533, 538)
Pareto 76, 78
Part count method 51
Part stress method 27, 33-38, 50-51 (see also 69-71)
Partition(ing) 29, 38, 58, 90, 115, 118, 154, 158, 160, 164, 166
Partitioning cumulative op. time 316, 317, 323, 393
Passivation / Passivation test 85, 89, 93, 100, 104-6, 147
Path 55, 58, 166
Path set → Minimal path sets
Pattern sensitivity 91, 93
PCB → Populated printed circuit board
Pearson / Pearson theorem 539, 557
Percentage point 434
Performability / Performance 270, 374 → Capability
Performance effectiveness → Reward
Performance parameters / test 84, 86, 108, 406 (see also Characterization)
Petri nets 287-88
Phased-mission systems 28, 30, 38, 259-66, 379
Physical models 38, 333
Physics of failures 38, 333 (see also Failure mech.)
Piecewise definition 424, 567
Pilot production 19, 351, 357, 374, 376, 384
Pinholes 93
Pitch 85, 109, 152, 363
Plastic / Plastic packages 83-85, 98-100, 147, 152
Plug-in / plug-out 116, 157
PoF → Physics of failures
Point availability ($PA_{S_i}(t)$, $PA_S = AA_S$) 9, 170, 374
 • computation 9, 61, 172-73, 177, 183, 184, 185, 188, 195, 197-98, 201, 209, 213, 217, 233, 278, 515-16
 • definition 9, 173, 177, 374, 476, 492, 498, 508
 • demonstration 313-14, 315, 553-54
 • estimation 311-12, 315, 545-46
 • with preventive maintenance 242
Point estimate at system level (λ) 320
Point estimation 300, 311, 317, 318, 325-26, 354, 533-37, 542, 546
Point processes 168, 341, 464, 515, 523-24
Poisson approximation 10, 304, 322, 451, 452
Poisson distribution 305, 317, 430-31, 451-52, 536
Poisson's integral 446, 448, 566

Poisson processes

- homogeneous (HPP) 7, 35, 142, 316, 317-18, 341-42, 345-49, 350, 378, 380, 467, 472-73, 516-20, 522-24
- nonhomogeneous (NHPP) 168, 343-56, 516-20
- simulation 520

Populated printed circuit board (PCB) 23, 84, 85, 90, 94, 107-11, 116, 149, 151-53, 157, 358, 362-66

Portability (software) 162

Possible causes

- common cause failures 66, 271
- defects / latent failures 106-07, 108-10, 148, 162-63
- single point failures 66

Potential reliability problem 95, 106-07, 110

(see also Damage, Weaknesses)

Power devices 96, 98, 150, 151, 152

Power Law / Power Law process 333, 352

Power of a (statistical) test 548, 556

Power supply 83, 96, 108, 148, 151, 152, 155, 157

Power-up / power-down 150, 151

ppm 359, 446

Practical aspects for *MTBF* / *MTTR* demonstration 392-93

Predicted maintainability 121-25

Predicted reliability 3, 25-27, 50-51, 35-38, 28-71, 169-294, 394-95

Preferred part list (PPL) → Qualified part list (QPL)

Preheating 153

Preliminary design reviews 403, 406-08

→ Design reviews

Preliminary / rough analyses 51, 392, 394

Premature wear-out 333

Pressure cooker → HAST

Preventive actions / measures 16, 22, 72-79, 120, 144-66, 357-58, 363, 393-404, 405-09

Preventive maintenance 8, 112-13, 134-40, 240-43, 249-51, 381-82, 427

Primary failure 4

Printed circuit board → Populated printed circuit board

Printed wiring board → Populated printed circuit board

Priority /priority list 160, 164, 400, 408

Probability 415-18

Probability chart 335, 336-37, 339, 443, 531-32, 569-71

Probability density → Density

Probability plot paper → Probability chart

Problems for homework 576-81

Procedure for (see also Rule for)

- analysis of binary decision diagrams (BDD) 283
- analysis of complex rep. systems 277-79, 293-94
- analysis of mechanical systems 69-70
- analysis of phased mission systems 262
- binary decision diagrams 283
- chi-square test 338-40, 557-58
- cost optimization 12-15
- cost optimization at incoming inspections 364-72

• demonstration of

availability ($PA=AA$) 313-15, 553-55
MTTR 327-329, 393

probability p 302-08, 309-10, 548-52
 λ or $MTBF = 1 / \lambda$ 305, 315, 320-25
(in particular 305, 314, 323)

• double one-sided sampling plan 307-08

• electrical test of compl. ICs 88-90, 90-93

• environmental test

assemblies (PCBs) 108-09
ICs 92-100

• ESD test 94

• estimation of

availability ($PA=AA$) 311-12, 545-46
MTTR 325-27

parameters 353-54, 533-46

probability p 300-02, 309, 535, 538-42

λ or $MTBF = 1 / \lambda$ 318-20, 535, 537, 542-45
in particular 301, 312, 319

• event trees 286

• failure analysis 105

• first delivery 372

• FMEA / FMECA 72-73, 74-75

• frequency / duration 278-79, 498-501

• graphical estimation of $F(t)$ 334-39, 529-32

(see also 349-50, 351-56, 467, 555-57, 569-71)

• goodness-of-fit tests

Anderson-Darling / Cramér - von Mises 556-57

Kolmogorov-Smirnov 334-9, 344, 354, 556, 558-9

χ^2 test 338-40, 557-60

• Laplace test 346, 348

• maintenance 161

• mechanical system's analysis 67-68, 69

• modeling complex rep. systems 277-79, 293-94

• phased-mission systems investigation 262

• qualification test

assemblies 108-09

complex ICs 87, 89

first delivery 372

• quality assurance 17-20, 21-24, 387-90, 391-412

• quality cost optim. at incoming inspection 364-72

• RAMS assurance 17-20, 21-24, 387-90, 391-412

• reliability allocation 67

• reliability engineering 13, 393-95

• reliability prediction 2-3, 25-28, 52, 67-69, 238-40, 277-79, 294, 394-95 (see also 28-51, 53-67)

• reliability test

accelerated tests 330, 332, 333

statistical aspects 309-25, 334-56, 525-60
(in particular 305, 314, 319, 323)

technical aspects 101, 109, 359-64

• screening of

assemblies 363-64

- components **359-62**
- sequential test **305-06, 322-24, 550-51**
- simple one-sided test plan **306-07, 324-25, 551-52**
- simple two-sided test plan **302-05, 320-23, 549-50**
- software development & test **162-65 & 166-67**
- test and screening **87-111, 358-71**
 - in particular **89, 360, 367-71**
- transition probabilities (determination of) **172-73, 485-86, 506-07, 511-13** (see e. g. **200-01, 204-05**)
- transition rates (determination of) **172-73, 485-87,** (see e. g. **197, 203, 215, 235, 246, 258, 267, 273**)
- trend tests **346-49**
- Process FMEA / FMECA **72, 78**
- Process reliability **3**
- Processes with independent increments **343-50, 351-56, 461-62, 473, 516-20, 524**
- Processes with stationary increments **463, 473, 516**
- Procurement **357, 402**
- Producer risk α **86, 303, 306, 313, 314, 321, 323, 548, 554** (see also Type I error)
- Product assurance **16, 382, 389, 390**
- Product liability **10, 15, 376, 381, 382, 402**
- Production
 - documentation **401**
 - FMEA / FMECA → Process FMEA / FMECA
 - flaw **85, 106, 107, 108, 110**
 - procedures **357, 396**
 - process **6, 21, 87, 98, 106, 107, 110, 357-58, 364-66, 376-77, 382, 387, 390, 396, 400**
 - related rel. problems **95, 106-07, 110**
- Program / erase cycles **97, 360**
- Program for quality & rel. assurance **17-19, 391, 393-409**
- Project documentation **401**
- Project management **17-24, 159-68, 398**
- Project manager **398, 401, 412**
- Project quality & reliability assurance manager **401**
- Propagation (of events) **286**
- Protection against
 - common cause failures **66, 274**
 - damage **362**
 - ESD / EMC **94, 148-50**
 - damage **362**
 - incomplete coverage **249, 253**
 - single point failures **66**
 - shorts / opens **32, 64-65, 94**
 (see also Design guidelines and Rules)
- Prototype **18, 19, 87, 107, 334, 351, 365, 396, 397, 399, 402, 403, 406, 408-09**
- Pseudo redundancy **42, 383**
- Pseudorandom number **291-92**
- PSG **93, 99** (see also Passivation)
- Pull-up / pull-down resistor **149, 150, 152, 156**
- Purple plague **100, 103**
- Quad redundancy **65, 66, 101**
- Quadratic statistics **344, 556**
- Qualification tests **18, 87, 107, 351, 365, 396, 402, 403**
 - assemblies **107-11**
 - components **89, 87-107**
 - prototypes **351, 396**
- Qualified part list (QPL) **87, 150, 395, 400, 407**
- Quality **11, 16, 382**
- Quality and reliability (RAMS) assurance program **16, 17-18, 24, 387-90, 393-412**
- Quality and reliability requirements **387-90, 391-93**
- Quality and reliability standards **387-90**
- Quality assurance **11, 13, 16, 17-24, 358, 376, 382, 394-97, 398-412** (see also Design guidelines)
- Quality assurance department **19, 20**
- Quality assurance / management system **21, 382, 388**
- Quality attributes for software **160, 162**
- Quality control / test **13, 16, 21, 383, 396**
 - statistical aspect **299-308**
- Quality cost **367, 397** (see also Cost optimization)
- Quality data reporting system **21-23, 365, 383, 397, 404, 410-12**
- Quality factor π_Q **36-37**
- Quality growth (software) **166-68**
- Quality handbook **21, 397**
- Quality management **16, 20, 21, 24, 382, 383, 388** (see also Quality assurance, TQM)
- Quality of design **16**
- Quality of manufacturing **16, 21, 86, 357-58**
- Quality metric for software **160**
- Quality tests **13, 21, 383, 398, 402, 404**
- Quantile **128, 434, 562-65**
- Quick test **116**
- RAM / RAMS assurance program
 - Quality and reliability assurance program
- RAM / RAMS engineering → Reliability eng.
- Random cumulative operating time **537**
- Random duration (phased-mission systems) **261, 265**
- Random numbers → Pseudorandom numbers
- Random sample → Sample
- Random variable **423-25**
- Random vector **434-38, 460-63**
- Random vibrations **83, 108, 109, 111**
- Rare event **10, 288, 292**
- RBD → Reliability block diagram
- Reachability tree **287-88**
- Realization (time schedule / simulation) of a stochastic process **176, 208-09, 219, 250, 292-93, 461, 464, 475, 506, 511-14**
- Realization of RAMS requirements
 - Quality and reliability assurance program
- Reason for → Causes for

- Recognition → Failure detection
- Reconfiguration **66, 118, 164, 238, 500-01**
- failure censored **266-69**
 - time censored (phased-mission system) **259-66**
 - with reward and frequency / duration **270-71**
- Recrystallization **109**
- Recurrence time **181, 182, 185, 468-69, 476, 517**
- Recurrence time limit theorem **470**
- Recycling **10, 19, 379**
- Redesign **8, 87, 351, 359**
- Reduced test → Normal / reduced / tightened test
- Reduction (diagram of transition rates) **277, 293**
- Redundancy **31, 42-49, 51, 53-61, 65, 68, 101, 227-28, 232-33, 235, 244, 250, 259, 267, 275-76, 284, 383**
(see also Active, One-out-of-2, k -out-of- n , Standby, Warm redundancy)
- for software **42, 49, 159, 164**
 - practical example **30, 32, 49, 51, 65, 235, 244, 267, 282**
 - realization **42-43, 49, 51, 65, 66, 101**
- Reference documentation **403, 408**
- Reference failure rates **36, 38, 572-75**
- Reflow soldering **153**
- Refuse to start **246**
- Regeneration point **170, 176, 178, 208, 464, 475, 478, 495, 506, 514** (see also Renewal point, Distinction)
- Regeneration state **208, 223, 462, 478, 506, 511-13**
- Regenerative processes **171, 462, 478-479, 514** (see also Markov, Semi-Markov, Semi-regenerative processes)
- Rejection line **305, 322-24, 550**
- Relation between (see also Distinction between)
- distribution functions **445, 452, 562, 563, 564**
 - stationary and asymptotic & steady-state **472, 477, 479, 498, 509**
 - stochastic processes **171, 505**
 - P_i and \mathcal{P}_i **497, 510, 514**
- Relative frequency **300-02, 415-18, 455, 526, 535, 540-42**
- Relative humidity **98-99, 147, 153**
- Relaxation **109**
- Release procedure **87, 402**
- Reliability **2-3, 13, 39, 170, 184, 199, 384**
(see also Assessed, Estimated, Predicted)
- allocation / optimization **67, 392, 394**
 - analysis **13, 16, 25-79, 144-53, 169-294, 394-95, 399**
(in particular **25-27, 31, 172-73, 201, 233, 277-79**)
 - as selection criterion **86**
 - assurance → Quality & rel. assurance program
 - block diagram (RBD) **28-32, 68, 238, 384**
(see **238-80** if the RBD doesn't exist)
 - block diagram with repetition of at least 1 element
→ Same element(s) in reliability block diagrams
 - demonstration → Reliability tests
 - engineering **13, 16**
 - estimation → Reliability tests
 - function **3, 39, 58, 63, 69-71, 172-73, 174, 176, 184, 190, 199, 384, 425, 426, 493, 495, 508**
with preventive maintenance **241-43**
(see also Conditional rel. function, Rel. analysis)
 - growth **309, 351-56, 384** (see also 166-68)
 - guidelines **144-53**
 - human → Human reliability
 - improvement **26-27, 144-53, 154-68, 391-409**
 - long term behavior (components) **86**
 - mechanical → Mechanical reliability
 - optimization **67**
 - prediction → Procedure for
computer aided **289-92**
 - tests
physical **35, 89, 101, 109-11**
statistical (estimation & demonstration)
as failure rate (λ or $R(t)=e^{-\lambda t}$) **309-25**
for a fixed mission (R) **309-10**
(see also Procedure for reliability tests)
 - weaknesses **77, 80, 309**
 - with preventive maintenance **241-43**
- Remote control / diagnostic / maintenance **117-18, 120**
- Renewal density **344, 465, 466, 475, 516**
(see also Frequency)
- Renewal density theorem **470**
- Renewal equation **466**
- Renewal function **465**
- Renewal point **135, 208, 241, 292, 464, 474, 475, 524**
(see also Regeneration point **478**)
- Renewal points frequency → Renewal density
- Renewal processes **126, 134, 136, 171, 292, 342, 350, 463-64, 465-73, 478, 520-21**
- embedded **210, 474-75, 478, 506, 514**
 - simulation **291-92**
- Repair **8, 113, 170-71, 351, 375, 381**
- frequency → System repair frequency
 - priority **141, 220-21, 233, 235, 239, 242, 246, 258, 267, 272, 277, 488, 490**
(see also Maintenance strategy)
 - rate **115, 177-78, 183, 201, 204-05, 213, 232, 233**
(see also Approximation for a repair function)
 - strategy → Maintenance strategy
 - time **8, 113-15, 115-20, 121-24, 325-29, 381**
- Repairability **113** → Corrective maintenance
- Repairable items / systems **5-6, 40, 169-298**
- Repairable spare parts **130-34** (see also Spare parts)
- Repairable versus nonrepairable **40, 202, 378, 380, 383, 426**
- Replaceability **157**
- Replacement policy **134, 135-40** (see also Centralized and Decentralized logistic support)
- Report / information status → Status test

- Reproducibility **16, 79, 401, 408, 409**
 Requalification **2, 87**
 Required function **3, 28, 29, 239, 259, 379, 385, 392**
 Requirements → Quality and reliability requirements,
 Reserve contacts **157**
 Reserve / reserve state **42-43, 62, 170, 196, 207, 249**
 Residual failure-free time → Survival failure-free time
 Rest waiting time **343, 517**
 (see also Waiting time paradox)
 Restart anew **178, 462, 464, 478**
 Restoration **8, 112, 113, 171, 375** → Repair
 Restoration frequency → System repair frequency
 Restoration time **113** → Repair time
 Results (tables / graphs) **31, 44, 48-49, 111, 127, 141, 172-73, 183, 188, 195, 201, 213, 217, 227-28, 232, 233, 237, 241, 248, 256, 264, 269, 301, 303, 305, 312, 314, 319, 322, 325, 329, 323, 324, 331, 336, 337, 339, 430-31, 468, 473, 532, 544, 550, 551, 552**
 (see also Numerical examples)
 Reusability (software) **162**
 Reuse **10, 116, 119, 130**
 Reverse bias **98-99, 360**
 Reward **238, 266-67, 270-71, 279, 498, 500-01**
 Reward rate **271, 279, 501**
 Rework **108, 153, 363**
 Rise time **88, 94, 148, 149**
 Risk **9-11, 67, 72, 150, 295, 369, 385, 391, 395, 406**
 - acceptance **10**
 - analysis / management **10, 11, 286, 294, 389**
 - assessment **294**
 - awareness / perception **11**
 - development / production **11, 387, 391, 406**
 - priority number concept **10**
 - statistical **300, 303, 306, 322, 324, 525**
 - technology **67, 150**
 (see also Confidence level γ , Consumer risk β ,
 Producer risk α , Type I error α , Type II error β)
 Robustness (software) **162** → Defect tolerant
 ROCOF **524**
 Rough analysis **51, 350, 392, 394, 437**
 Rule for (see also Procedures for)
 - check at failure **249, 250, 253, 255, 256**
 (see also Check strategy)
 - common cause failures **274**
 - convergence of $PA(t)$ to PA **183, 186-87, 198**
 - convergence of $R_S(t)$ to $e^{-\lambda_S t}$ **197**
 - critical decisions / failures **72, 73, 76, 158, 294, 295**
 - data analysis **342**
 - derating **33, 145**
 - firing **287**
 - FMEA / FMECA **72**
 - imperfect switching **245, 247, 257**
 - incomplete coverage **249, 253, 255**
 - junction temperature **37, 146, 150**
 - Markov processes **487, 510**
 - partition of cumulative op. time **317, 323, 393**
 - phased-mission systems **262**
 - power-up / power-down **150, 152**
 - quality and reliability (RAMS) assurance **19**
 - redundancies **46, 226, 250, 254, 257**
 - reliability allocation **67**
 - semi-Markov processes **505, 510**
 - series / parallel structures **46, 226**
 - software defect models **167-68**
 - software quality assurance **159-66, 167**
 - use of ICs in plastic packages **85, 147**
 (see also Condition, Design guidelines,
 Mandatory, Procedure for)
 Run-in **363, 374**
 Run test **166**
 Safety **1, 9-10, 13, 15, 66, 158, 259, 385, 390, 395, 402, 407**
 - analysis / assurance / improvement **9-10, 66, 72-80, 158-59, 294-98, 385, 395, 399**
 - engineering **13**
 - factor **69**
 Same element(s) in the reliability block diagrams **30, 31, 32, 54-6, 57, 58, 60, 68-9, 275-6, 284, 285, 290**
 Same stress **71**
 Sample **299, 526**
 Sample path **461**
 Sample space (Ω) **413-14**
 Sample without replacement **454**
 Sampling tests / plans ($p, R, PA, \lambda, MTBF=1/\lambda, MTTF$)
299-329, 334-49, 367-71, 533-46, 548-60
 Scale parameter **442**
 Scan path **156-57**
 Scanning electron microscope **95, 104, 105, 107**
 Schmitt-trigger **92, 148**
 Scrambling table **91**
 Screening
 - assemblies **79, 351, 363-64** (see also ESS)
 - components **79, 359-62**
 (see also Testing / screening, Technological charact.)
 Screening strategy → Strategy
 Seal test **361-62**
 Second source **79, 81, 87, 150, 407**
 Secondary failure **4, 66, 73, 274, 411, 522**
 Selection criteria for
 - electronic components **81-86, 150, 395, 400, 572-5**
 - materials **395, 400**
 - special manufacturing processes **400**
 SEM → Scanning electron microscope
 Semidestructive analyses / tests **104, 105, 334**

- Semi-Markov processes **167, 171, 172, 193-95, 462, 474-77, 484, 486, 505-10**
- simulation **291-92**
- Semi-Markov process embedded → Semi-regenerative process, Embedded semi-Markov process
- Semi-Markov transition probability **171, 172, 192-94, 200, 223, 252, 292, 296-98, 485-86, 506-07, 511, 512, 513**
- Semi-regenerative processes **170, 171, 204-07, 218-19, 222-25, 240, 462, 478, 510-13, 514**
- Sequential test **305-06, 322-24, 550-51**
- Series element **46-48, 66, 72, 220, 221, 225, 226-28**
- Series model / structure / system **31, 41-42, 121-23, 189-95, 342, 428, 442, 443, 520**
- Series - parallel model / structure / system **31, 45-49, 124, 141, 220-37, 284, 285, 289, 490**
- (in particular **31, 47, 227, 233**, see also **71** for stress-strength)
- Series production **19, 351, 357, 374, 376, 384**
- Serviceability **113** → Preventive maintenance
- Services reliability **3**
- Set operations **414**
- Shannon decomposition / expansion/tree **53, 58, 283-5**
- Shape of the
- failure rate **7, 337-38, 444**
 - repair time density / distribution **114, 174, 206-07**
 - renewal function **467-68** (see also **524**)
- Shape parameter **442**
- Shewhart cycles **76**
- Shield / shielded enclosure **149**
- Shmoo plot **91, 93**
- Shock **83**
- Short-term test **334** (see also HALT, HASS, HAST)
- Silicon nitride glassivation → Passivation
- Silver plated pins **94**
- Simple hypotheses **547**
- Simple one-sided sampling plan **306-07, 551-52**
- Simple one-sided test **324-25**
- Simple structure **28, 31 (1-6), 39-51, 175-237**
- Simple two-sided sampling plan **302-04, 549-50**
- Simple two-sided test **320-23**
- Simplicity (software) **162**
- Simulation → Monte Carlo
- Single-point failure **42, 66, 79, 407**
- Single-point ground **148**
- Six- σ approach **446**
- Skill **144, 158, 159, 163**
- Sleeping state → Dormant state
- SMD / SMT **84, 109-11, 152-53, 363**
- test & screening **109**
- SMP → Semi-Markov process
- Sneak analyses **76, 79, 399**
- Soft error **89, 97**
- Software
- attributes **160, 162** → Software quality attributes
 - causes for defects **162-63, 271**
 - common faults / failures **271, 274**
 - configuration management **160, 164, 165, 400, 408**
 - defects **117, 154, 159-60, 162-66, 351, 355**
 - defect modeling **166-68, 400**
 - defect prevention **162-65**
 - defect tolerant **159, 401, 408**
 - design reviews **160, 161, 164, 165, 400, 408**
 - development procedure **160-65**
 - documentation **161, 162, 163, 164**
 - embedded **160, 164**
 - error correcting codes **164**
 - errors at start ($t=0$) **168, 356**
 - failure rate **166**
 - FMEA / FMECA **72-73, 160**
 - interaction **163, 164-65**
 - interface **161, 163, 164, 408**
 - life-cycle phases **160, 161, 400, 408**
 - metrics **160, 162**
 - object oriented **164**
 - packages **188**
 - quality **13, 21, 160, 162, 384**
 - quality assurance **13, 16, 17, 21, 159-68, 400, 408**
(see also Design guidelines)
 - quality attributes **160, 162, 400, 408**
 - quality growth **166-68, 351-56, 408**
 - redundancy **66, 164**
 - reliability (defect freedom) → Software quality
 - specifications **161, 163, 164**
 - standards **160, 165, 166, 389, 390**
 - test strategy **401, 408** (see also Software testing)
 - testing / validation **163, 164, 166**
 - time / space domain **159, 160, 164**
 - Validation **161, 163, 166**
- Sojourn time → Stay time
- Solder joint **108-11, 152-53, 333, 362-63**
- Solder-stop pads **152**
- Solderability test **89, 94**
- Soldering temperature profile **84-85, 153**
- Spare parts provisioning **116, 118, 125-34, 142**
- Special diodes **150**
- Special manufacturing processes **152, 400**
- Special tools **116, 120, 157**
- Specifications **3, 18, 19, 161, 163, 164, 387, 394, 398, 402, 403, 408-09**
- Specified $p, \overline{PA}, \lambda, MTBF$ **302, 313, 321, 392**
- Standard deviation **433**
- Standard industrial environment **36, 37**
- Standard normal distribution **126, 430-31, 446, 456-59, 471, 561, 534, 540, 571**
- Standardization **117, 120, 154, 159, 167, 387, 408**

- Standardized random variable *433, 446*
- Standards *35-36, 38, 78, 143, 160, 162, 165, 306, 387-90*
- Standby redundancy *43, 62-63, 201, 212, 213, 217, 218, 243-45, 383, 440* (see also Active and Warm red.)
- Standby time *242*
- State clustering → State space reduction
- State merging → State space reduction
- State probability *62, 172-73, 197, 481, 483, 491, 497-98, 508-09*
- numerical values *237, 269*
- State space *460-63*
- State space extension *193-95, 487, 515*
- State space method *56-57, 65*
- State space reduction *229, 277, 293*
- State transition diagram → Diagram of transitions
- Static burn-in *361* (see also Burn-in)
- Static fault tree *76, 281, 282, 283, 285*
- Stationary / steady-state (see also Asymptotic behav.)
- alternating renewal process *187-89, 476-77*
 - behavior at system level *278*
 - distribution *481, 497, 508-10*
 - increments (time-homogeneous) *463, 472, 473*
 - initial distribution *481, 497, 508-10*
 - Markov chain *481*
 - Markov process *172-73, 496-98, 510*
 - one-item structure *187-89, 311-15*
 - point process *523*
 - processes *462-63*
 - regenerative process *479*
 - renewal process *471-72*
 - semi-Markov process *172-17, 508-10*
- Statistical decision *526*
- Statistical equilibrium → Steady-state → Stationary
- Statistical error → Statistical risk
- Statistical hypothesis *547-48*
- Statistical maintainability tests *325-29*
- Statistical process control *299*
- Statistical quality control *16, 299-308*
- Statistical reliability tests *309-24, 334-56, 525-60*
- Statistical risk *525* (see also α , β , β_1 , β_2 , γ)
- Stochastically independent *419, 435* → Independent
- Statistics → Mathematical statistics
- Status / status test *116, 119, 249*
- Stay time (sojourn time) *170, 171, 173, 260, 271, 277, 292, 480, 486, 487, 491, 501, 505, 507, 508, 510, 514*
- Steady-state → Stationary / steady-state
- Steady-state properties of Markov proc. *496-501, 510*
- Step-stress tests *334*
- Stiffness *109, 363*
- Stirling's formula *341, 566*
- Stochastic demand *181*
- Stochastic evolving network *276*
- Stochastic matrix *480, 482*
- Stochastic mean value theorem *479*
- Stochastic Petri net *287*
- Stochastic processes *61-4, 169, 171, 172-3, 460, 460-524*
- Stochastically independent *419, 435* → Independent
- Storage / transportation *153*
- Strategy
- cost optimization *143, 364-71, 450*
 - incoming inspection *366-72*
 - maintenance *35, 125, 134-41, 240-43*
 - spare parts provisioning *125-34*
 - test *21, 120, 166, 359, 364-66, 368-69, 372, 383, 395*
 - test & screening *21, 120, 363, 364-72, 383, 395*
- (see also Check strategy, Cost)
- Stress factor *33, 86, 144-45, 150-51, 376*
- (see also Derating)
- Stress-strength method *69-71, 76*
- Strict liability → Product liability
- Strict sense stationary *462*
- Strictly increasing / decreasing failure rate *137, 138, 139, 241, 242, 426, 442, 444*
- Strong law of large numbers *456, 527*
- Strongly consistent *533*
- Structure function *58, 59, 283, 285*
- (see also Fault tree structure function)
- Stuck-at-state *245-47, 248, 257-58, 266-69*
- Stuck-at-zero / at-one *90*
- Student distribution (*t*-distribution) *563*
- Subcontractor *399, 402* (see also Supplier)
- Successful path method *55-56*
- Successive approximation *304*
- Sudden failure *4, 411*
- Sufficient statistic/estim. *300, 318, 346-49, 533, 534-36*
- Sum of
- Homog. Poisson processes *10, 122, 317-8, 473, 521*
 - Nonhomogeneous Poisson proc. *473, 518, 521*
 - Point processes *524*
 - Random variables *438-40, 445, 447, 455, 464-65*
 - Renewal processes *520-21*
- Superconform / superuniform *558*
- Superimposed processes → Sum of
- Superposition → Sum of
- Supplementary / additional states *193-95, 515*
- Supplementary variables *193-94, 515*
- Supplier *15, 105, 357, 358, 372, 395, 407*
- Suppressor diodes *148, 149*
- Sure event *414* (see also Sample space Ω)
- Surface mount devices / technique → SMD / SMT
- Survival failure-free time *426*
- Survival function *426* → Reliability function
- Susceptibility *148* → EMC
- Sustainable development *10, 379, 392, 407*
- Switch *46, 47, 48, 49, 149, 220-25, 226, 227-28, 243-47, 249-55, 257-58, 266-69, 282-85, 289*

- Switching phenomena **148, 149**
- Symmetry condition **461**
- Symptom → Failure mode
- Synonyms used in this book
- *failure-free time* for *failure-free operating time* **425**
 - *independent* for *totally* (mutually, statistically, stochastically) *independent* **419, 435**
 - *mean* for *expected value* **525**
 - *reliability function* for *survival function* **425**
 - *repair* for *restoration* **420**
 - *sample* for *random sample* **525**
 - *stationary* for *asymptotic and steady-state* **169, 472, 477, 498, 509**
- System **2, 3, 29, 31, 39, 169-71, 172-73, 175, 277-79, 293-94, 385**
- confidence limits (on λ) **320**
 - design review **403, 405-6** (see also Design review)
 - down time → Down time, Mean down time
 - effectiveness → Cost effectiveness
 - failure frequency (f_{inS}) **270, 278, 499-500**
 - failure intensity **279, 500, 524**
 - function → Structure function
 - mean down time (MDT_S) **270, 278-79, 499-500**
 - mean time to failure referred to state Z_i ($MTTF_{S_i}$) **41, 173** → Mean time to failure
 - mean up time (MUT_S) **270, 278-79, 499-500**
 - reconfiguration → Reconfiguration
 - repair frequency (f_{inS}) **270, 279, 500**
 - restoration frequency → System repair frequency
 - specifications **387, 398-9** (see also Specifications)
 - status **159** (see also Status)
 - up time → Up time, Mean up time
 - without redundancy → Series model
- Systematic failure **1, 3-4, 6-7, 115, 351, 364, 365, 374, 376, 377, 378, 382, 384, 385**
- Systems engineering **11, 16, 17, 379, 386, 388**
- Systems with complex structure **31, 52, 52-66, 68, 238-79, 293-94**
- Systems with hardware and software **168**
- Systems with more than 2 states or one failure mode → More than two states or one failure mode
- Tailoring **17, 364, 377, 391, 393, 394, 398**
- Tasks / task assignment **17-20, 295, 393-97**
- Tchebycheff → Chebyshev
- t -distribution → Student's distribution
- Team work **10, 72, 78, 375**
- Technical availability **242** → Overall availability
- Technical delay **113, 375, 381**
- Technical safety → Safety
- Technical system **4** → System
- Technological characterization
- assemblies **107-11**
 - components **89, 87-107**
 - prototypes **351, 396**
- Technological properties / limits **10, 32, 38, 84-85, 86, 92, 96-100, 108, 147-53, 329, 334, 351, 363, 572-75**
- Temperature dependence **3, 34-35, 37, 329-34**
- Test (statistical)
- unknown availability **313-15, 553-55**
 - unknown distribution function **334-40, 555-60**
 - unknown *MTTR* **327-29, 393**
 - unknown probability **302-08, 309-10, 548-52**
 - unknown λ or *MTBF* = $1 / \lambda$ **320-25, 392-93**
 - statistical hypotheses (basic theory) **547-60** (in particular **305, 314, 323, 328**)
- Test (technical)
- assemblies **108, 362-63**
 - components **88-92, 358-59**
- Test & screening procedure → Procedure for screening
- Test and screening strategy → Strategy
- Test by attributes / by variables **299**
- Test conditions **83, 89, 93-101, 108-09, 359-62, 363**
- Test coverage **90, 91, 117, 156** (see also Incomplete cov.)
- Test modi **156**
- Test pattern **90-93**
- Test plan **303, 305, 313, 314, 321, 323, 328, 549, 550, 551-52, 554**
- Test point **152, 156**
- Test power → Power of a test
- Test procedure → Procedure for test and screening
- Test stimuli **157**
- Test strategy → Strategy
- Test structure **97**
- Test time partitioning → Partitioning
- Test vector **88**
- Testability **79, 116-17, 150, 152, 155-57, 401**
- software **162, 164, 166**
- Testing → Test
- TDDB → Time-dependent dielectric breakdown
- Theorem
- addition **419, 422**
 - Bayes **422, 436**
 - Blackwell **470**
 - central limit **126, 456, 457-59, 471**
 - cut sets / cuts **497 / 500**
 - De Moivre - Laplace **456, 540**
 - Elementary renewal **469**
 - Final value / Initial value **567**
 - Fréchet **422**
 - Fubini **179**
 - Generalized cut sets **497, 502**
 - Glivenko-Cantelli **527**
 - Grigelionis **521**
 - Initial value **567**
 - Integral Laplace **456, 540**

- Key renewal **185, 186, 470, 477, 479**
- Kolmogorov **529**
- Korolyuk **515**
- Limit theorems of probability theory **454-56, 457-60**
- Markov **497**
- Mean value **479**
- Multiplication **420-21**
- Pearson **539, 557**
- Recurrence time limit **470**
- Renewal density **470**
- Stochastic mean value **479**
- Tightened elementary renewal **469**
- Total probability **422**
- Thermal cycles **89, 95, 98, 108, 109, 111, 359-61, 363**
- Thermal design concept / management **146**
- Thermal resistance **84, 85, 146-47**
- Thermal stress **150**
- Thermomechanical stress **147, 152**
- Three parameter Weibull distribution **443, 531-32**
- Three states **64-65, 152**
- Tightened elementary renewal theorem **469**
- Tightened test → Normal / reduced / tightened test
- Time censored reconfiguration → Phased-mission sys.
- Time censoring → Censoring
- Time compression **333**
- Time consuming **174, 226, 240, 289, 515, 516**
- Time-dependent dielectric breakdown **89, 96-97, 103**
- Time domain **159, 164**
- Time-homogeneous
 - Markov chains **480**
 - Markov processes **171, 172-73, 462, 482-505**
 - Poisson processes **472**
 - processes **463**
- Time redundancy **42, 164, 383**
- Time schedule (diagram) **176, 182, 208, 209, 219, 238, 250, 464, 475, 511, 512, 513**
- Time to market **11, 19, 388, 391, 406** (see also Market)
- Timing diagram / problems **151, 163**
- Top-down **76, 78, 163, 164, 378**
- Top event **76, 78, 280-81, 283, 286**
- Tort liability → Product liability
- Total additivity **416**
- Total down time **124, 181, 522** (see also *MDT*)
- Total expectation **437**
- Total operating time → Total up time
- Total probability **52, 70, 177, 422, 469, 481, 483, 495**
- Total probability theorem **422**
- Total quality management (TQM) **16, 17, 18, 19, 20, 21, 376, 386, 388, 391**
- Total up time **180, 181, 500, 522** (see also *MUT*)
- Totally exclusive events → Mutually exclusive events
- Totally independent elements **52, 61, 217-18, 226, 229, 231, 232, 237, 275-76, 280-85, 293, 294, 515**
- Totally independent **419, 435** → Independent
- Traceability **390, 402**
- Training → Motivation / training / training level
(see also Motivation & training, Skill)
- Transformation of
 - random variables **291, 428, 448**
 - stochastic processes **345-46, 515, 518-19**
- Transient phenomena **144, 148, 150**
- Transition diagram → Diagram of transitions
- Transition probability **172-73, 197, 199, 480, 482, 492, 493, 495, 507** (see also Diagram of)
- Transition rate **287, 483, 485** (see also Diagram of)
- Transportation / storage **153**
- Travel time **203-04, 512**
- Trend test **345-50**
- Triplet **413, 423**
- True reliability **26**
- Truncated distribution / random variable **71, 135, 136, 140, 291, 292, 428, 568**
(see also **71** for stress-strength)
- Truth table **88, 90, 92**
- Twisted pairs **149**
- Two chamber oven **98, 361**
- Two dimensional random vector **436**
- Two failure mechanisms **332, 342, 363, 428**
(see also Multiple failure modes / mechanisms)
- Two failure modes **64-65, 66, 255, 257-58, 266-69**
(see also Multiple failure modes / mechanisms)
- Two-sided confidence interval → Confidence interval
- Two-sided test / sampling plan
 - availability $PA=AA$ **313-14, 553-55**
 - const. failure rate λ or $MTBF = 1 / \lambda$ **320-24**
 - unknown probability p **302-06, 549-51**;
(in particular **305, 314, 323**)
- Two step action **158, 294, 295**
- Type I (time) / II (failure) censoring → Censoring
- Type I / II error (α / β) **303-08, 313-14, 321-25, 327-29, 334-40, 346-49, 547-48, 549-60**
(see also Producer risk, Consumer risk)
- Ultrasonic cleaning **153**
- Unavailability **61, 237, 309, 311-15, 545-46, 553-55**
- Unbiased **300, 311, 318, 528, 529, 533-37, 555**
- Uncertainty (mech. rel.) **71**
- Unconditional
 - expected value (mean) **437**
 - probability **344, 426, 466, 474, 516, 524**
 - stay time **507**
- Uncovered latent failures **134**
- Understandability / readability (software) **164**
- Undetected failure / fault time τ_{UFT} **249, 251, 427**
- Uniform distribution **345, 346, 448, 449**

Uniformly distributed

- random numbers 291, 292
- random variables 345, 346, 449

Unify methods / models / data 35, 38, 161, 169, 170-71

Uninterruptible power supply (UPS) 230-37

Union of events 414

Unit step function $u(t)$ 567, 568

Unknown probability 291, 299-308, 309-10, 311-15, 315, 459, 535, 538-42, 549-52, 545-46, 553-55
(see also Defective probability)

Unload redundancy → Standby redundancy

Unused logic inputs 150

Up / up states (u, U) 57, 278, 474-75, 491, 508

Up time 181, 278-79, 499-500, 522

(see also System mean up time (MUT_S))

Upper bound 59, 187, 240, 260, 280, 281, 294

Upper confidence limit → Confidence limits

Usability 162, 289, 410

Use of $R(t_1, t_2)$ 40, 179, 384

Useful life 13, 35, 39, 81, 85, 119, 125, 177, 380, 386
(for components 146, 150, 151, 573, 574)

User / User doc. 15, 117, 118, 154, 156, 159, 397, 401

Validation (software) 161, 163, 166

Validity → Model validity

Value Analysis 386, 401

Value Engineering 386, 401

Variable resistor 100, 145, 151, 572

Variable (test by) 299

Variance 431, 432-33, 438, 523, 528

Vibrations 82, 83, 108, 109, 111, 333, 363

Viscoplastic deformation 109

Visual inspection 89, 93, 102, 104

Voids 93, 100, 108, 109, 110

Voltage bias /reverse bias 98, 99, 100, 360

Voltage stress 333

Voter 49, 222, 282, 285

Wafer 97, 106, 153

Waiting redundancy → Warm redundancy

Waiting time → Stay time

Waiting time paradox 470

Warm redundancy 43, 62, 196-200, 201, 213, 217, 245-48, 258, 383 (see also Active red., Standby red.)

Warranty 16, 21, 364, 383

Wash / Washing liquid 153

Wave matching 151

Weak law of large numbers 455

Weaknesses analysis 6, 26-27, 68, 69, 72-80, 309, 405-09 (see also 87-111, 144-68, 351-56, 367, 410-12, Design reviews, Rules)

Wear-out / wear-out failures 6-7, 8, 35, 98, 240, 333, 336, 337, 342, 345, 350, 351, 377, 428, 443, 467-68

Wear-out period 6, 336, 345, 350, 355

Weibull distribution 126-28, 335-38, 342, 430-31, 440, 442-43, 531-32, 535-38, 570

Weibull probability chart 335-38, 443, 531-32, 570

Weibull process 352

Weighted sum 7, 12, 14, 41, 337-38, 368-71, 428
(see also Cost /cost equations, Mixture)

Whisker growth 153

Wide sense stationary 463

Wire wrap 157

Without aftereffect 342, 343, 356, 462, 473, 480, 516, 517, 520, 523

Without interruption → On line

Without redundancy → Series model

Work-mission availability 142, 180-81, 522

Worst case analysis 76, 79, 151, 394, 406

X-ray inspection 102

Zener diodes 145, 149, 150

Zero defects 86

Zero hypothesis → Null hypothesis H_0

1-out-of-2 → One-out-of-two

1-out-of-2: G → One-out-of-two

6- σ approach 446

85/85 test → Humidity test

α particles 103

α ; β (producer/type I risk; consumer/type II) 547-48

β_1, β_2, γ ($\gamma=1-\beta_1-\beta_2$ = confidence level) 538

λ (constant (time independent) failure rate) 6, 171, 378, 426-27 (see also Constant failure rate, Repairable versus nonrepairable)

μ (constant (time independent) repair rate) 115, 171
(see also λ)

χ^2 (Chi-square) 562

$\eta_n = \tau_n^* - \tau_{n-1}^*$ (interarrival times) 517

$o(\delta t)$ (Landau notation) 483

$i = \sqrt{-1}$ 561, 567

Π circuit 576

S_0 (indices for state Z_0 entered at $t=0$) 52, 172-73

t_1, t_2, \dots (realizations of τ) 4-5, 526-27, 336, 339

t_1^*, t_2^*, \dots (arbitrary points on the time axis) 346-50, 517-20

τ (failure -free time) 425

τ' (repair time) 113

τ_{\min}, τ_{\max} 440

$\hat{}$ is used for an estimated (or empirical) value 299, 528